КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.1021
УДК 004.056.5

Балацька Валерія Сергіївна
доктор філософії,
старший викладач кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0002-6262-6792
v.balatska@ldubgd.edu.ua

Івануса Андрій Іванович
кандидат технічних наук, доцент,
начальник кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0001-9141-8039
a.ivanusa@ldubgd.edu.ua

Пановик Уляна Петрівна
кандидат технічних наук, доцент,
доцент кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0002-9663-4328
u.panovyk@ldubgd.edu.ua

МЕТОД ІНТЕГРАЦІЇ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СТАНДАРТІВ ТА ПРОТОКОЛІВ У ПРОЦЕС ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ОРГАНІЗАЦІЇ

Анотація. У статті розглянуто проблему розриву між задекларованими політиками інформаційної безпеки, вимогами стандартів та протоколів, а також фактичним функціонуванням інформаційної інфраструктури в організаціях. На практиці елементи КСЗІ часто створюються формально, без врахування реальних ризиків, характеристик мережевих протоколів та відповідності міжнародним і національним стандартам безпеки. У результаті політики інформаційної безпеки не узгоджуються з параметрами технічних засобів, що призводить до фрагментації системи захисту та зниження її загальної ефективності. Додатковою проблемою є використання застарілих або небезпечних протоколів, які продовжують функціонувати через відсутність системного контролю відповідності вимогам стандартів. Запропоновано метод інтеграції політик інформаційної безпеки, вимог стандартів (ISO/IEC 27001:2022, NIST SP 800-53, НД ТЗІ України) та наборів безпечних протоколів (TLS 1.3, SSHv2, DNSSEC, IPSec) у процес побудови комплексної системи захисту інформації. Метод складається з чотирьох етапів: аналіз активів і протоколів, формування та формалізація політик безпеки, встановлення відповідності стандартам та побудова інтегрованої архітектури КСЗІ на основі отриманих результатів. Для кількісної оцінки узгодженості елементів КСЗІ розроблено алгоритм оцінювання відповідності (compliance scoring), який дозволяє об’єктивно визначати рівень відповідності інформаційної інфраструктури вимогам нормативних документів і політик. Експериментальна перевірка методу у тестовому середовищі показала збільшення відповідності стандартам із 52 % до 92 %, усунення застарілих або небезпечних протоколів (FTP, SMB1, HTTP), а також підвищення ефективності формування параметрів КСЗІ завдяки автоматизованій прив’язці політик до технічних механізмів безпеки. Отримані результати підтверджують доцільність використання методу під час побудови та модернізації КСЗІ організацій різних типів. Метою роботи є розроблення методу інтеграції політик інформаційної безпеки, стандартів та протоколів у процес формування комплексної системи захисту інформації в організації.

Ключові слова: комплексна система захисту інформації; КСЗІ; політика інформаційної безпеки; управління інформаційною безпекою; моделювання КСЗІ; стандарти інформаційної безпеки; НД ТЗІ; ISO/IEC 27001; NIST SP 800-53; мережеві протоколи безпеки; TLS 1.3; SSHv2; DNSSEC; IPSec; оцінювання відповідності.

ВСТУП

В умовах цифрової трансформації організацій та зростання обсягів критично важливої інформації питання побудови ефективної системи захисту інформації набуває особливого значення. Діяльність державних органів, суб'єктів господарювання, установ освіти та об'єктів критичної інфраструктури дедалі більше залежить від стабільності роботи інформаційних систем, а будь-які порушення конфіденційності, цілісності чи доступності можуть мати суттєві негативні наслідки. Це визначає потребу у впровадженні комплексних, узгоджених, нормативно вивірених механізмів захисту. Одним із таких інструментів в Україні є комплексна система захисту інформації (КСЗІ), що регулюється НД ТЗІ та визначає вимоги до організаційних, технічних, криптографічних і програмно-апаратних засобів [1].

Попри існування нормативної бази, практика демонструє, що побудова КСЗІ у значній кількості організацій здійснюється без системного підходу до інтеграції політик, стандартів і технічних засобів захисту. Часто політики інформаційної безпеки мають рамковий характер, а їхні вимоги не узгоджуються з фактичними налаштуваннями мережевої інфраструктури, рівнем ризиків та застосовуваними протоколами. Наприклад, у документації можуть бути задекларовані вимоги щодо використання TLS 1.3 або SSHv2, тоді як у реальному середовищі продовжують функціонувати застарілі або небезпечні протоколи, такі як FTP, Telnet, SMBv1 або HTTP без шифрування [2]. Це створює ситуацію, коли декларативний рівень безпеки не відповідає реальному, що прямо суперечить вимогам НД ТЗІ щодо цілісності та адекватності КСЗІ.

Особливої уваги потребує питання відповідності міжнародним і національним стандартам. Сучасні організації дедалі частіше повинні відповідати вимогам ISO/IEC 27001:2022, NIST SP 800-53, рекомендаціям НБУ, ДССЗЗІ України та іншим документам, які визначають конкретні вимоги до управління інформаційною безпекою, криптографічного захисту, управління доступом, моніторингу, журналювання та реагування на інциденти. Водночас відсутність єдиного методу, що інтегрує ці стандарти з політиками та протоколами в рамках КСЗІ, ускладнює забезпечення відповідності та підтримку актуального рівня безпеки.

Проблематика також охоплює сферу управління ризиками. Більшість КСЗІ формуються без ґрунтовного ризик-орієнтованого аналізу, що призводить до неефективного розподілу ресурсів і впровадження заходів, які не вирішують найкритичніших загроз. За відсутності інтегрованої моделі, що поєднує ризики, політики та технічні засоби, окремі компоненти системи безпеки залишаються ізольованими й не забезпечують комплексного захисту.

Додатковою проблемою є неузгодженість між рівнями управління безпекою. Політики інформаційної безпеки – стратегічний рівень. Стандарти – нормативно-методичний рівень. Протоколи – технічний рівень. КСЗІ – інтеграційний рівень. За відсутності методики, що забезпечує взаємодію цих рівнів, організація отримує фрагментарну систему, яка формально відповідає окремим вимогам, але не функціонує як цілісний механізм протидії сучасним загрозам.

У таких умовах актуальним постає завдання розроблення методу, який би дозволив комплексно інтегрувати політики, стандарти та протоколи в логічну структуру КСЗІ

відповідно до вимог НД ТЗІ України, а також забезпечив узгодженість між організаційними заходами і реальними технічними механізмами захисту.

Метою дослідження є розроблення методу інтеграції політик інформаційної безпеки, стандартів та мережевих протоколів у процес побудови і модернізації комплексної системи захисту інформації відповідно до вимог НД ТЗІ України та міжнародних стандартів безпеки.

Постановка проблеми.

На сьогоднішній день організації функціонують у складному та динамічному цифровому середовищі, у якому кількість кіберзагроз постійно зростає, а вимоги до захисту інформації стають жорсткішими. В умовах активної цифровізації державних сервісів, впровадження електронного документообігу, використання хмарних рішень та віддаленого доступу виникає необхідність забезпечити цілісність, конфіденційність і доступність інформаційних ресурсів. У цьому контексті комплексна система захисту інформації (КСЗІ) відіграє ключову роль, оскільки визначає організаційні, технічні та криптографічні механізми для побудови захищеного інформаційного середовища.

Однак реальна практика впровадження КСЗІ в Україні демонструє наявність суттєвого розриву між різними рівнями системи безпеки. Зокрема, політики інформаційної безпеки часто формуються на стратегічному рівні, але не мають прямого зв’язку з технічними конфігураціями інфраструктури. Водночас стандарти інформаційної безпеки – ISO/IEC 27001, NIST SP 800-53, НД ТЗІ України – встановлюють конкретні вимоги, проте в багатьох випадках вони впроваджуються частково або формально [3]. Найбільш проблемною ланкою залишається протокольний рівень, де фактичні протоколи та сервіси (FTP, Telnet, SMBv1, незахищений HTTP) не відповідають задекларованим у політиках і стандартах вимогам (TLS 1.3, SSHv2, DNSSEC, IPSec). Це створює конфігураційні вразливості, які часто залишаються непоміченими.

Існуючі методи побудови та атестації КСЗІ описують окремі аспекти – формування політик, аудит інфраструктури, оцінювання відповідності, – але не забезпечують їх інтеграції в єдину логічну модель. Внаслідок цього організації отримують фрагментарну та неузгоджену систему, де політики не узгоджені зі стандартами, стандарти – з технічними засобами, а технічні засоби – з реальними потребами процесів.

Таким чином, ненаявність єдиного методу, що забезпечує комплексну інтеграцію політик, стандартів і протоколів у структурі КСЗІ, становить ключову науково-практичну проблему, яка потребує вирішення для забезпечення цілісності, узгодженості та ефективності системи захисту інформації.

Аналіз останніх досліджень і публікацій.

Проблематика побудови комплексних систем захисту інформації та забезпечення їх відповідності вимогам нормативних документів тривалий час перебуває в центрі уваги як вітчизняних, так і зарубіжних дослідників. У працях, присвячених розробленню та впровадженню КСЗІ в органах державної влади та на об’єктах інформаційної діяльності, основна увага зосереджується на формуванні переліку загроз, виборі організаційних і технічних заходів, побудові моделей порушника, а також на процедурах атестації та оцінювання відповідності вимогам НД ТЗІ. Водночас більшість таких робіт орієнтована на опис загальної методології побудови КСЗІ й містить переважно нормативно-процедурні рекомендації без детальної формалізації процесів інтеграції політик, стандартів і протоколів.

Окремий напрямок становлять дослідження у сфері управління інформаційною безпекою на основі міжнародних стандартів, насамперед ISO/IEC 27001 та споріднених

документів сімейства ISO/IEC 27000. У цих роботах розглядаються питання впровадження систем менеджменту інформаційної безпеки, ризик-орієнтованого підходу до вибору засобів захисту [4], побудови політик і процедур, а також інтеграції вимог стандартів у організаційну структуру підприємства. Проте такі підходи переважно мають універсальний характер і не враховують специфіки побудови КСЗІ відповідно до національних нормативних документів НД ТЗІ [5], а також не деталізують зв'язок між політиками та конкретними мережевими протоколами і конфігураціями.

Значна кількість публікацій присвячена окремим аспектам захисту мережевої інфраструктури та протокольного рівня. Зокрема, досліджуються питання безпечної конфігурації протоколів TLS, SSH, IPSec, механізмів DNSSEC, побудови захищених віртуальних приватних мереж, виявлення та усунення вразливостей у реалізації мережевих сервісів. У таких роботах розробляються рекомендації щодо посилення конфігурацій, застосування криптографічних алгоритмів, впровадження систем виявлення та запобігання вторгненням [6]. Водночас ці дослідження, як правило, не розглядають протокольний рівень як складову інтегрованої КСЗІ і не описують механізми його прив'язки до організаційних політик і вимог стандартів.

Окрему групу становлять роботи, спрямовані на оцінювання відповідності (compliance) інформаційних систем вимогам регуляторів, стандартів і галузевих норм. У них пропонуються різні моделі аудиту, матричні методи зіставлення контролів стандартів з наявними засобами захисту, підходи до побудови показників відповідності. Однак більшість таких моделей є орієнтованими на документальний та чеклістовий контроль і не враховують динамічний характер мережевих конфігурацій та протокольних налаштувань. Крім того, вони рідко інтегруються безпосередньо в процес проєктування або модернізації КСЗІ.

Аналіз останніх досліджень і публікацій свідчить про наявність розвинутої теоретичної та методичної бази щодо окремих складових системи захисту інформації: побудови КСЗІ, впровадження систем менеджменту інформаційної безпеки за стандартами, захисту мережевих протоколів, а також оцінювання відповідності. Водночас недостатньо опрацьованою залишається проблема створення єдиного інтегрованого методу, який би поєднував політики інформаційної безпеки, вимоги міжнародних і національних стандартів та конкретні параметри протокольного рівня у структурі КСЗІ, що й зумовлює актуальність даного дослідження.

Мета статті. Метою статті є наукове обґрунтування підходу до модернізації комплексної системи захисту інформації (КСЗІ) шляхом інтеграції політик інформаційної безпеки, вимог національних та міжнародних стандартів, а також параметрів безпечних мережевих протоколів у єдину узгоджену архітектуру. Такий підхід спрямований на підвищення цілісності, керованості, прозорості та ефективності КСЗІ, забезпечення відповідності вимогам НД ТЗІ України, стандартів ISO/IEC 27001 і NIST SP 800-53, а також посилення узгодженості між організаційними політиками та реальним технічним функціонуванням інформаційної інфраструктури.

Основними завданнями статті виступають:

1. Проаналізувати існуючі підходи до побудови комплексних систем захисту інформації (КСЗІ) та визначити їх сильні й слабкі сторони у контексті сучасних вимог інформаційної безпеки.

2. Вивчити структуру та зміст політик інформаційної безпеки, їх роль у формуванні організаційної моделі захисту інформації та їх взаємодію з технічними компонентами КСЗІ.

3. Дослідити нормативно-правову базу у сфері захисту інформації, зокрема НД ТЗІ України, стандарти ISO/IEC 27001 та NIST SP 800-53, і визначити вимоги, які необхідно інтегрувати у структуру КСЗІ.

4. Охарактеризувати вимоги до безпечних мережевих протоколів (TLS 1.3, SSHv2, DNSSEC, IPSec) та визначити їх значення для забезпечення технічного рівня захисту інформаційних систем.

5. Систематизувати взаємозв'язки між політиками інформаційної безпеки, вимогами стандартів та параметрами мережевих протоколів, що впливають на формування цілісної архітектури КСЗІ.

6. Розробити метод інтеграції політик, стандартів та протоколів як цілісний підхід до побудови та модернізації КСЗІ в організації.

7. Сформувати концептуальну архітектурну модель інтегрованої КСЗІ, яка відображає узгодження організаційного, нормативного та технічного рівнів системи.

8. Обґрунтувати практичні рекомендації щодо впровадження розробленого методу в організаціях різного типу з урахуванням їхніх специфічних вимог та обмежень.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Теоретичні засади формування комплексної системи захисту інформації

Комплексна система захисту інформації (КСЗІ) є базовим інструментом забезпечення інформаційної безпеки в українських організаціях відповідно до вимог НД ТЗІ. Вона містить узгоджену сукупність організаційних, технічних, програмно-апаратних та криптографічних заходів, спрямованих на гарантування конфіденційності, цілісності та доступності інформаційних ресурсів. Ефективність КСЗІ визначається не лише наявністю окремих механізмів захисту, а й їх системною взаємодією, відповідністю нормативним вимогам і реальним загрозам.

Одним із ключових елементів побудови КСЗІ є політики інформаційної безпеки, що визначають загальні правила, принципи та вимоги до управління захистом інформації в організації. Вони охоплюють питання управління доступом, контролю привілеїв, реагування на інциденти, журналювання, криптографічного захисту, резервування, класифікації активів тощо. Політики забезпечують стратегічний рівень управління безпекою, але самі по собі не гарантують достатнього рівня захисту, якщо їх не інтегрувати з технічними параметрами інформаційної інфраструктури.

Другим важливим компонентом є стандарти інформаційної безпеки. Міжнародні стандарти, зокрема ISO/IEC 27001:2022 та NIST SP 800-53, визначають вимоги до систем менеджменту інформаційної безпеки, процедур контролю, ризик-орієнтованих підходів та методів управління життєвим циклом інформаційних ресурсів. Вони встановлюють універсальні механізми, які повинні бути враховані під час формування політик і технічного рівня КСЗІ. Національні нормативні документи, зокрема НД ТЗІ, регламентують порядок створення КСЗІ, вимоги до побудови моделі загроз, організаційних та технічних заходів, а також процедури підтвердження відповідності. Таким чином, стандарти й НД ТЗІ формують нормативно-методичний рівень системи захисту.

Третім базовим елементом є мережеві протоколи, оскільки саме вони забезпечують практичну реалізацію вимог політик і стандартів на технічному рівні. Протоколи TLS 1.3, SSHv2, DNSSEC, IPSec є основою захищеної комунікації, а правильність їх конфігурації напряму впливає на рівень безпеки інформаційної системи [7]. Водночас невідповідність між задекларованими протоколами та фактичними конфігураціями

(використання FTP, Telnet, SMBv1 або застарілих криптографічних алгоритмів) створює критичні вразливості, які не завжди враховуються під час проєктування КСЗІ.

Як видно з таблиці 1, ефективна КСЗІ функціонує як поєднання трьох рівнів: організаційного, нормативного та технічного, кожен з яких відіграє специфічну роль, але лише їх узгоджена взаємодія забезпечує цілісність та стійкість системи.

Таблиця 1.

Взаємозв'язок рівнів КСЗІ

Рівень	Елементи	Приклади	Суть взаємодії
Організаційний	Політики ІБ	доступ, криптографія, резервування	Формують правила
Нормативний	ISO/IEC 27001, NIST, НД ТЗІ	контролі, процедури	Перетворюють правила на вимоги
Технічний	TLS 1.3, SSHv2, DNSSEC, IPSec	протоколи, конфігурації	Реалізація на практиці

Відсутність єдиної методології, яка забезпечує їх узгодженість, призводить до фрагментарності системи захисту та зниження її ефективності. Саме тому актуальним є розроблення методу, що дозволяє об'єднати ці рівні в єдину інтегровану модель КСЗІ, орієнтовану на сучасні стандарти безпеки, практики управління ризиками та вимоги нормативних документів у сфері інформаційної безпеки [8].

Політики інформаційної безпеки є фундаментом КСЗІ, оскільки задають стратегічні принципи, правила та вимоги до захисту даних в організації. Вони формують нормативно-організаційну основу, на якій вибудовується структура КСЗІ, визначають поведінку персоналу, порядок доступу до ресурсів, управління ризиками та взаємодію між підрозділами.

Сучасні підходи до формування політик ІБ спираються на міжнародні стандарти, насамперед ISO/IEC 27001:2022, що встановлює вимоги до Системи менеджменту інформаційної безпеки (СМІБ). У цьому контексті політика ІБ виступає найвищим рівнем регламентації, визначаючи цілі, принципи управління та загальні підходи до забезпечення безпеки. В КСЗІ вона одночасно задає стратегічний напрямок розвитку системи захисту та забезпечує узгодженість організаційних і технічних заходів.

Політики охоплюють ключові аспекти: управління доступом і автентифікацією, класифікацію інформаційних активів, криптографічний захист, ведення журналів і моніторинг подій, реагування на інциденти, резервування та відновлення, використання мережевих сервісів і протоколів, управління вразливостями та оновленнями. Важливо, щоб ці політики були безпосередньо пов'язані з технічними параметрами інфраструктури та вимогами міжнародних і національних стандартів. Саме така узгодженість забезпечує цілісність КСЗІ та її відповідність нормативній базі.

На практиці одним із найтиповіших недоліків є формальне затвердження політик без їх реального втілення на рівні налаштувань протоколів та технічних засобів. Наприклад, політика може забороняти використання незашифрованих протоколів, проте в інфраструктурі продовжують працювати FTP, SMBv1 чи HTTP; або декларується вимога двофакторної автентифікації, але відсутні технічні можливості для її реалізації. Така розбіжність між декларативним і операційним рівнями знижує ефективність КСЗІ та створює передумови для інцидентів [9].

Отже, політики ІБ мають розглядатися не як формальний документ, а як реальний інструмент управління конфігураціями протоколів, систем і мережевих засобів. Розроблення методу інтеграції політичних, нормативних і технічних вимог є важливою

науково-прикладною задачею, оскільки дозволяє перетворити політику ІБ на основу керованої, перевірної та вимірюваної системи, у якій кожне положення знаходить відображення в конкретних технічних механізмах захисту.

Нормативні стандарти як основа регламентації вимог до КСЗІ

Нормативно-правова база та міжнародні стандарти інформаційної безпеки визначають рамки для проєктування, впровадження та оцінювання КСЗІ. Вони створюють єдину методологічну основу, що забезпечує узгодженість між політиками, процедурами та технічними механізмами захисту. У цьому контексті ключову роль відіграють ISO/IEC 27001, NIST SP 800-53 та НД ТЗІ України.

ISO/IEC 27001:2022 встановлює вимоги до СМІБ і визначає комплекс контролів, які охоплюють управління доступом, криптографічний захист, журналювання, реагування на інциденти, управління ризиками, безпеку мереж і обробку інформації. Він є універсальним стандартом, придатним для організацій різних типів і розмірів, і забезпечує системність та відтворюваність процесів інформаційної безпеки.

NIST SP 800-53 містить деталізований каталог контролів безпеки для інформаційних систем, приділяючи особливу увагу мережевим протоколам, моніторингу, операційній безпеці та захисту від вторгнень. Він задає чіткі технічні вимоги до засобів захисту, що робить його важливим орієнтиром для організацій, які прагнуть глибокої технічної інтеграції політик і протоколів.

НД ТЗІ України (зокрема НД ТЗІ 2.5-004-2008, 2.7-010-09, 3.7-003-2005) [10] регламентують порядок створення КСЗІ, класифікацію загроз, формування моделі порушника та вимог безпеки залежно від класу системи. Ці документи визначають обов’язкові організаційні й технічні заходи для обробки інформації з обмеженим доступом [11].

Основна проблема полягає в тому, що міжнародні стандарти та НД ТЗІ часто впроваджуються розрізнено: ISO/IEC 27001 – переважно в частині документації, НД ТЗІ – у технічній площині. Внаслідок цього виникає розрив між організаційним, нормативним і технічним рівнями, що ускладнює побудову єдиної інтегрованої КСЗІ, яка одночасно відповідала б міжнародним практикам і національному законодавству. Правильна інтеграція стандартів і НД ТЗІ стає критичною умовою ефективності системи та її відповідності вимогам безпеки.

Мережеві протоколи як технічна основа формування КСЗІ

Мережеві протоколи становлять технічне ядро КСЗІ, оскільки забезпечують передачу, обробку та доступ до інформації. Реальний рівень захищеності інформаційної системи визначається тим, наскільки коректно налаштовані протоколи, які криптографічні механізми застосовано та чи відповідають вони вимогам політик і стандартів.

Використання застарілих або небезпечних протоколів, таких як FTP, Telnet, HTTP без TLS [12], SMBv1 чи старі реалізації SSL, створює значні ризики: дані передаються у відкритому вигляді, зростає вразливість до перехоплення, атак «людина посередині» та компрометації облікових даних. При цьому у формальних політиках такі протоколи часто вже заборонені, але фактично продовжують використовуватися через історичні обмеження, відсутність централізованого контролю або слабкі аудиторські процедури [13].

Сучасні стандарти орієнтують на використання TLS 1.3 для захисту веб-трафіку, SSHv2 – для безпечного адміністрування, DNSSEC – для забезпечення достовірності DNS-відповідей, IPSec – для шифрування трафіку та побудови VPN. Однак навіть впровадження цих протоколів не гарантує безпеки без коректної конфігурації:

застосування слабких шифрів, помилки в управлінні сертифікатами або ключами можуть нівелювати переваги сучасних протоколів.

Таким чином, протокольний рівень потребує не лише впровадження рекомендованих технологій, а й постійного моніторингу й перевірки відповідності вимогам політик і стандартів. Відсутність системного механізму, який би пов'язував політики та налаштування протоколів, призводить до конфігураційних вразливостей, що не завжди виявляються під час атестації КСЗІ.

Інтеграція політик, стандартів і протоколів у межах КСЗІ

Інтеграція політик інформаційної безпеки, нормативних стандартів та мережевих протоколів є ключовою умовою побудови цілісної та ефективної КСЗІ. Лише синхронізація організаційного, нормативного та технічного рівнів дозволяє забезпечити узгоджене функціонування механізмів захисту та відповідність вимогам НД ТЗІ, ISO/IEC 27001 і NIST SP 800-53 [14].

У інтегрованому підході політики формуються з урахуванням вимог стандартів, а не ізольовано; ці вимоги далі трансформуються в технічні параметри конфігурацій протоколів, а їх відповідність регулярно перевіряється. Встановлення зворотного зв'язку між змінами в інфраструктурі, оновленням нормативної бази й корекцією політик дає змогу підтримувати КСЗІ в актуальному стані. У результаті система набуває властивостей «живої» – такої, що адаптується до змін технологій, загроз і регуляторних вимог, не перетворюючись на формальний набір документів і застарілих технічних засобів.

Отже, інтеграція політик, стандартів і протоколів забезпечує узгодженість усіх компонентів КСЗІ, підвищує її керованість, зменшує конфігураційні ризики та дозволяє формувати сучасну, нормативно вивірену інфраструктуру інформаційної безпеки.

Розроблення методу інтеграції політик, стандартів і протоколів у КСЗІ

Ефективне функціонування комплексної системи захисту інформації неможливе без цілісного підходу, який поєднує організаційні, нормативні та технічні складові в єдину логічну структуру [15]. Для усунення розривів між політиками ІБ, вимогами стандартів та фактичними параметрами мережевих протоколів запропоновано метод інтеграції, який базується на поетапному узгодженні контрольних вимог, технічних конфігурацій та регламентів безпеки.

Метод складається з трьох основних структурних блоків:

1. Нормативно-аналітичний блок – визначення вимог політик ІБ, контролів стандартів ISO/IEC 27001 та NIST SP 800-53, а також положень НД ТЗІ.

2. Техніко-протокольний блок – аналіз фактичних конфігурацій протоколів, визначення їх відповідності криптографічним і конфігураційним вимогам [16].

3. Інтеграційно-оцінювальний блок – формування узгодженої моделі КСЗІ та оцінювання рівня відповідності через інтегральний показник.

Центральним елементом методу є індикатор відповідності (Compliance Score), який дозволяє кількісно оцінити ступінь узгодженості між політиками, стандартами та протоколами. На відміну від традиційних підходів, що фокусуються лише на документальному аналізі або технічних аудитах, даний показник забезпечує комплексний вимір, інтегруючи три ключові компоненти КСЗІ.

Згідно з формулою (1), загальний рівень відповідності визначається як зважена сума трьох часткових показників: відповідність політик (P), відповідність стандартів (S) та відповідність протоколів (T).

Формула (1) – інтегральний показник відповідності КСЗІ (CS):

$$CS = \frac{W_p \cdot P + W_s \cdot S + W_t \cdot T}{W_p + W_s + W_t}$$

де:

P – рівень відповідності політик (0-1),

S – відповідність стандартам (0-1),

T – відповідність протокольним конфігураціям (0-1),

W_p, W_s, W_t – вагові коефіцієнти важливості.

Для ілюстрації практичного використання формули застосовано умовні значення часткових показників, результати яких наведено у табл. 2. Як видно з таблиці, за умови наявності високого рівня відповідності протоколів та помірного рівня відповідності стандартам загальний CS може бути достатньо високим, навіть за незначних відхилень у політиках ІБ.

Таблиця 2.

Приклад розрахунку показника CS

Компонент	Значення	Вага	Внесок
Політики (P)	0.85	0.4	0.34
Стандарти (S)	0.72	0.35	0.252
Протоколи (T)	0.95	0.25	0.2375
Сумарний CS	–	–	0.8295

Отримане значення CS=0.8295 свідчить про достатньо високу інтегровану відповідність, що вказує на узгодженість ключових компонентів КСЗІ. Разом з тим, модель дозволяє швидко визначити, які саме елементи системи потребують корекції чи підсилення.

Описаний метод може бути використаний як основа для модернізації існуючих КСЗІ, планування заходів із підвищення відповідності вимогам стандартів, а також для періодичного контролю стану інформаційної безпеки в організації [17].

Запропонований метод інтеграції політик, стандартів і протоколів забезпечує кількісну та якісну оцінку узгодженості компонентів КСЗІ. Використання інтегрального показника CS дозволяє визначати пріоритетні напрями удосконалення системи, зменшувати конфігураційні ризики та забезпечувати відповідність сучасним вимогам інформаційної безпеки.

Архітектурна модель інтегрованої КСЗІ

Архітектурна модель інтегрованої комплексної системи захисту інформації (КСЗІ) має забезпечувати узгодження організаційних, нормативних та технічних компонентів у єдину структуру, яка гарантує керованість, цілісність і відповідність вимогам сучасної інформаційної безпеки [18]. На відміну від традиційного підходу, який передбачає роздільний розгляд політик, стандартів і технічних параметрів, інтегрована архітектура орієнтується на формування взаємопов'язаних рівнів, кожен з яких впливає на інші та забезпечує повний життєвий цикл захисту інформації.

Узагальнена структурна модель побудована на трьох ключових шарах:

1. Організаційний рівень (рівень політик ІБ) – регламентує вимоги, правила, заборони, процедури доступу, порядок обробки інформації, поведінку персоналу та ролі

відповідальних осіб. Цей рівень визначає, які протоколи можна застосовувати, які ключові контролі необхідні, які криптографічні механізми мають бути впроваджені та які процеси повинні бути стандартизовані.

2. Нормативний рівень (стандарти та НД ТЗІ) – переводить загальні вимоги політик у чіткі контрольні заходи, критерії, регуляторні вимоги та параметри, яких необхідно дотримуватися [19]. Саме на цьому рівні формується нормативна "матриця відповідності", що задає єдині правила оцінювання процесів, конфігурацій та технічних параметрів.

3. Технічний рівень (мережеві протоколи та конфігурації) – виконує реалізацію вимог двох попередніх рівнів через конкретні конфігурації систем, криптографічні алгоритми, налаштування протоколів, обмеження доступу, аудит та моніторинг.

Логіка взаємодії цих рівнів відображена у рис. 1, де представлене ієрархічне поєднання політик, стандартів і протоколів, яке забезпечує перехід від декларативних вимог до фактичних механізмів технічного захисту.

Запропонована архітектура передбачає такі ключові механізми взаємодії:

– паралельне формування політик і нормативної матриці, що дозволяє одразу забезпечити відповідність вимогам ISO/IEC 27001, NIST та НД ТЗІ;

– автоматизоване зіставлення вимог політик із параметрами протоколів з використанням контрольних списків і конфігураційних профілів;

– агреговане оцінювання відповідності, де отриманий індикатор CS застосовується як зворотний зв'язок для корекції політик і налаштувань;

– циклічне оновлення архітектури, яке відбувається у разі змін у нормативній базі, протоколах чи інфраструктурі.

Практична цінність архітектурної моделі полягає в тому, що вона дозволяє:

– забезпечувати безперервний моніторинг відповідності політик і протоколів нормативним вимогам;

– швидко виявляти конфігураційні розриви, коли політика декларує одне, а протокол функціонує інакше;

– формувати технічно обґрунтовані політики ІБ, що базуються не лише на регламентах, а й на реальному стані інфраструктури;

– гарантувати гнучку модернізацію КСЗІ відповідно до змін стандартів та появи нових протоколів;

– забезпечувати інтеграцію з процесами управління ризиками та інцидентами інформаційної безпеки.

Отже, архітектурна модель інтегрованої КСЗІ забезпечує цілісний механізм побудови системи захисту, орієнтований на узгодження всіх рівнів інформаційної безпеки, усунення конфігураційних вразливостей і підтримання нормативної відповідності в умовах динамічного технічного середовища.

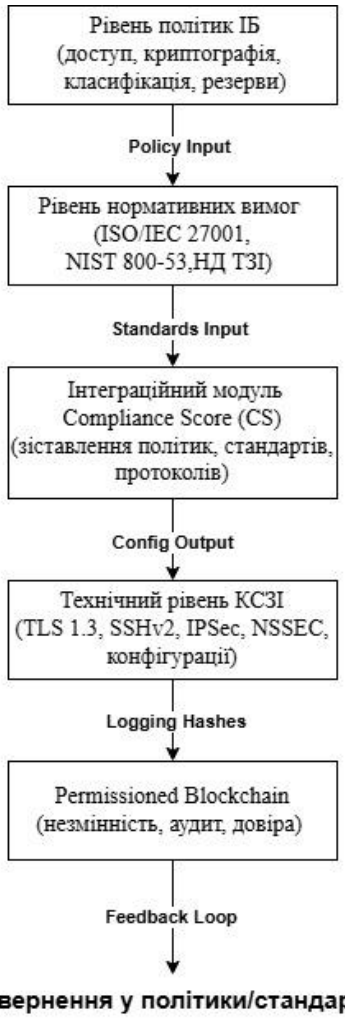

Рис. 1. Інтегрована модель узгодження політик, стандартів, протоколів та механізмів аудиту в архітектурі КСЗІ

Подана на рисунку модель деталізує послідовність інтеграції політик інформаційної безпеки, нормативних вимог, технічних конфігурацій та механізмів блокчейн-аудиту в єдину архітектуру КСЗІ. Вона демонструє, що організаційний рівень (політики ІБ) задає первинні вимоги та обмеження, які надходять на нормативний рівень для перетворення у стандартизовані контрольні заходи відповідно до ISO/IEC 27001, NIST SP 800-53 та НД ТЗІ України [20]. На наступному етапі ці вимоги порівнюються та узгоджуються в інтеграційному модулі, що формує показник відповідності (Compliance Score), який відображає ступінь кореляції між політиками, стандартами та технічними параметрами системи.

На технічному рівні здійснюється практична реалізація вимог шляхом налаштування безпечних протоколів (TLS 1.3, SSHv2, IPSec, DNSSEC) [21] та інших елементів КСЗІ. Далі всі зміни, події та конфігураційні стани фіксуються у permissioned-блокчейні, що забезпечує незмінність, аудиторську довіру та верифікованість журналів безпеки. Завдяки механізму зворотного зв'язку результати блокчейн-аудиту повертаються на рівень політик і стандартів, дозволяючи актуалізувати нормативні документи, оновлювати регламенти та адаптувати КСЗІ до нових загроз і технологій [22]. Модель реалізує циклічний процес удосконалення КСЗІ, у якому кожен рівень впливає

на інший, забезпечуючи безперервну відповідність, контрольованість та підвищення рівня інформаційної безпеки в організації.

Запропонована модель демонструє, що інтеграція блокчейн-технологій дозволяє забезпечити прозорий, незмінний та перевірний життєвий цикл КСЗІ, у якому політики, стандарти та технічні конфігурації узгоджуються між собою. Наявність зворотного зв'язку створює умови для постійної модернізації системи та підвищення її відповідності сучасним вимогам інформаційної безпеки [23].

ВИСНОВКИ

У проведеному дослідженні сформовано цілісний підхід до інтеграції політик інформаційної безпеки, нормативних стандартів та технічних механізмів захисту у структуру комплексної системи захисту інформації (КСЗІ). Показано, що фрагментарний підхід, коли політики ІБ створюються окремо від реальної конфігурації протоколів і лише частково узгоджуються зі стандартами ISO/IEC 27001, NIST SP 800-53 та НД ТЗІ України, формує стійкі розриви між організаційним та технічним рівнями. Саме ці розриви стають основним джерелом конфігураційних вразливостей, недоліків атестації, недостовірних журналів та зниження ефективності управління ризиками.

Запропонований метод інтеграції політик, стандартів і протоколів забезпечує системність побудови КСЗІ за рахунок уніфікації вимог, переведення організаційних положень у технічні параметри та використання кількісного механізму оцінювання відповідності (Compliance Score). Це дозволяє перетворити КСЗІ із сукупності розрізнених компонентів на комплексну керовану структуру, у якій кожен рівень має чітке підґрунтя та взаємозв'язки. Перевагою підходу є можливість швидко виявляти невідповідності між політиками та фактичними конфігураціями, що особливо важливо у великих або динамічних інфраструктурах.

Окрему увагу приділено використанню permissioned-blockchain як технологічної основи для забезпечення незмінності, прозорості та перевірності журналів безпеки. Інтеграція блокчейну у КСЗІ дає змогу забезпечити неможливість фальсифікації даних аудиту, відслідковувати зміни конфігурацій, забезпечувати надійний доказовий матеріал під час розслідування інцидентів та створювати захищений механізм контролю відповідності. Такий підхід підвищує рівень довіри до системи та зменшує ризики внутрішніх загроз, маніпуляцій і прихованих змін у конфігураціях.

Запропонована архітектурна модель інтегрованої КСЗІ демонструє, що ефективна система захисту повинна функціонувати не як статичний набір документів, а як динамічний механізм із постійним зворотним зв'язком. Завдяки циклічному процесу модернізації, що включає оновлення політик, стандартизацію вимог, перевірку конфігурацій та блокчейн-аудит, КСЗІ здатна адаптуватися до змін технологічного середовища, нових загроз та вимог регуляторів.

Результати дослідження є практично значущими для організацій державного та приватного сектору. Запропонований підхід може бути використаний під час створення нових КСЗІ, модернізації існуючих систем, автоматизації процесів аудиту, впровадження систем менеджменту інформаційної безпеки та підготовки до атестації згідно з НД ТЗІ. Дослідження формує методологічне підґрунтя для розвитку інтегрованих систем кіберзахисту, знижує ризики, пов'язані з людським фактором та некоректними конфігураціями, і забезпечує високу якість управління інформаційною безпекою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* Geneva: ISO.
2. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations.* Gaithersburg, MD: NIST.
3. Balatska, V. S., Tkachuk, R. L., & Maslova, N. V. (2025). Evolution of integrated information security systems and blockchain technologies in cybersecurity of state information systems of Ukraine. *Cybersecurity: Education, Science, Technique, 2*(30), 316–332. https://doi.org/10.28925/2663-4023.2025.30.975
4. Stallings, W. (2023). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
5. State Service for Special Communications and Information Protection of Ukraine. (2008). *ND TZI 2.5-004-2008. Procedure for developing a comprehensive information protection system (KSZI).* Kyiv.
6. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain application concept in SSO technology context. *CEUR Workshop Proceedings, 3654*, 38–49. https://ceur-ws.org/Vol-3654/
7. Kent, S., & Seo, K. (2005). *Security Architecture for the Internet Protocol (IPSec)* (RFC 4301). IETF. https://www.rfc-editor.org/rfc/rfc4301
8. Balatska, V. S., & Opirskyy, I. R. (2023). Ensuring personal data confidentiality and cybersecurity through blockchain. *Cybersecurity: Education, Science, Technique, 4*(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
9. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
10. State Service for Special Communications and Information Protection of Ukraine. (2009). *ND TZI 2.7-010-09. Classification of threats and model of the violator.* Kyiv.
11. Balatska, V., Slobodian, N., & Opirskyy, I. (2024). Blockchain for enhancing transparency and trust in government registries. *CEUR Workshop Proceedings, 3826*, 50–59. https://ceur-ws.org/Vol-3826/
12. Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3* (RFC 8446). IETF. https://www.rfc-editor.org/rfc/rfc8446
13. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Using Non-Fungible Tokens and blockchain for access control in state registries. *Cybersecurity: Education, Science, Technique, 4*(24), 99–114. https://doi.org/10.28925/2663-4023.2024.24.99114
14. ENISA. (2022). *Cybersecurity Policy Implementation Guide.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu
15. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the learning management system concept based on blockchain technology. *CEUR Workshop Proceedings, 3550*, 138–146.
16. Gartner Group. (2023). *Market Guide for Zero Trust Network Access.* Gartner.
17. Balatska, V., & Poberezhnyk, V. (2024). Concept of applying blockchain technologies to enhance the protection of personal data in the Diia platform: compliance with GDPR and Ukrainian legislation. *Cybersecurity: Education, Science, Technique, 2*(26), 268–290.
18. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *DNS Security Introduction and Requirements* (RFC 4033). IETF. https://www.rfc-editor.org/rfc/rfc4033
19. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. *CEUR Workshop Proceedings, 3800*, 70–80. https://ceur-ws.org/Vol-3800/
20. State Service for Special Communications and Information Protection of Ukraine. (2005). *ND TZI 3.7-003-2005. Procedure for conformity assessment of technical information protection means.* Kyiv.
21. Shirey, R. (2007). *Internet Security Glossary* (RFC 4949). IETF. https://www.rfc-editor.org/rfc/rfc4949
22. Ivanusa, A., Tkachuk, R., Brych, T., Balatska, V., & Tkachenko, A. (2024). Methods and models for designing a system for automated search of vulnerabilities in web applications. *Visnyk Lviv State University of Life Safety, 30*, 110–122. https://doi.org/10.32447/20784643.30.2024.11
23. Balatska, V., & Dmytriv, N. (2025). Inter-organizational exchange of confidential personal data based on permissioned blockchain. *Cybersecurity: Education, Science, Technique, 2*(29), 178–193. https://doi.org/10.28925/2663-4023.2025.29.875

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023

Valeriia S. Balatska
PhD, Senior Lecturer of the Department of Information Security Management,
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0002-6262-6792
v.balatska@ldubgd.edu.ua

Andriy I. Ivanusa
Candidate of Technical Sciences, Associate Professor,
Head of the Department of Information Security Management,
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0001-9141-8039
a.ivanusa@ldubgd.edu.ua

Ulyana P. Panovyk
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management,
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0002-9663-4328
u.panovyk@ldubgd.edu.ua

METHOD FOR INTEGRATING INFORMATION SECURITY POLICIES, STANDARDS AND PROTOCOLS INTO THE DEVELOPMENT OF A COMPREHENSIVE INFORMATION SECURITY SYSTEM IN AN ORGANIZATION

Abstract. The article addresses the problem of the discrepancy between declared information security policies, the requirements of standards and protocols, and the actual functioning of organizational information infrastructures. In practice, components of comprehensive information security systems (CISS) are often developed formally, without considering real risks, characteristics of network protocols, or compliance with international and national security standards. As a result, information security policies are not aligned with technical configuration parameters, leading to fragmentation of protection mechanisms and a decrease in overall system effectiveness. Another critical issue is the continued use of outdated or insecure protocols that remain operational due to the absence of systematic compliance control mechanisms. This study proposes a method for integrating information security policies, standard requirements (ISO/IEC 27001:2022, NIST SP 800-53, Ukrainian ND TZI), and secure network protocols (TLS 1.3, SSHv2, DNSSEC, IPSec) into the process of developing a comprehensive information security system. The method consists of four stages: asset and protocol analysis, development and formalization of security policies, compliance mapping with standards, and construction of an integrated CISS architecture based on the obtained results. To quantitatively assess the consistency of CISS components, a compliance scoring algorithm is introduced, enabling objective evaluation of the information infrastructure's conformity with regulatory requirements and internal policies. Experimental validation of the method in a test environment demonstrated an increase in compliance with standards from 52% to 92%, the elimination of outdated or insecure protocols (FTP, SMB1, HTTP), and improved accuracy of CISS parameterization due to automated mapping of policies to technical security mechanisms. The obtained results confirm the feasibility and effectiveness of the proposed method for designing and modernizing CISS in organizations of various types. The purpose of this study is to develop a method for integrating information security policies, standards, and protocols into the formation of a comprehensive information security system within an organization.

Keywords: comprehensive information security system; CISS; information security policy; information security management; CISS modelling; information security standards; ND TZI; ISO/IEC 27001; NIST SP 800-53; secure network protocols; TLS 1.3; SSHv2; DNSSEC; IPSec; compliance assessment.

REFERENCES

1. ISO. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* Geneva: ISO.
2. National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Revision 5. Security and Privacy Controls for Information Systems and Organizations.* Gaithersburg, MD: NIST.
3. Balatska, V. S., Tkachuk, R. L., & Maslova, N. V. (2025). Evolution of integrated information security systems and blockchain technologies in cybersecurity of state information systems of Ukraine. *Cybersecurity: Education, Science, Technique, 2*(30), 316–332. https://doi.org/10.28925/2663-4023.2025.30.975
4. Stallings, W. (2023). *Network Security Essentials: Applications and Standards* (7th ed.). Pearson.
5. State Service for Special Communications and Information Protection of Ukraine. (2008). *ND TZI 2.5-004-2008. Procedure for developing a comprehensive information protection system (KSZI).* Kyiv.
6. Balatska, V., Poberezhnyk, V., Petriv, P., & Opirskyy, I. (2024). Blockchain application concept in SSO technology context. *CEUR Workshop Proceedings, 3654*, 38–49. https://ceur-ws.org/Vol-3654/
7. Kent, S., & Seo, K. (2005). *Security Architecture for the Internet Protocol (IPSec)* (RFC 4301). IETF. https://www.rfc-editor.org/rfc/rfc4301
8. Balatska, V. S., & Opirskyy, I. R. (2023). Ensuring personal data confidentiality and cybersecurity through blockchain. *Cybersecurity: Education, Science, Technique, 4*(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
9. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.
10. State Service for Special Communications and Information Protection of Ukraine. (2009). *ND TZI 2.7-010-09. Classification of threats and model of the violator.* Kyiv.
11. Balatska, V., Slobodian, N., & Opirskyy, I. (2024). Blockchain for enhancing transparency and trust in government registries. *CEUR Workshop Proceedings, 3826*, 50–59. https://ceur-ws.org/Vol-3826/
12. Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3* (RFC 8446). IETF. https://www.rfc-editor.org/rfc/rfc8446
13. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Using Non-Fungible Tokens and blockchain for access control in state registries. *Cybersecurity: Education, Science, Technique, 4*(24), 99–114. https://doi.org/10.28925/2663-4023.2024.24.99114
14. ENISA. (2022). *Cybersecurity Policy Implementation Guide.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu
15. Poberezhnyk, V., Balatska, V., & Opirskyy, I. (2023). Development of the learning management system concept based on blockchain technology. *CEUR Workshop Proceedings, 3550*, 138–146. https://ceur-ws.org/Vol-3550/
16. Gartner Group. (2023). *Market Guide for Zero Trust Network Access.* Gartner.
17. Balatska, V., & Poberezhnyk, V. (2024). Concept of applying blockchain technologies to enhance the protection of personal data in the Diia platform: compliance with GDPR and Ukrainian legislation. *Cybersecurity: Education, Science, Technique, 2*(26), 268–290.
18. Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005). *DNS Security Introduction and Requirements* (RFC 4033). IETF. https://www.rfc-editor.org/rfc/rfc4033
19. Balatska, V., Poberezhnyk, V., & Opirskyy, I. (2024). Utilizing blockchain technologies for ensuring the confidentiality and security of personal data in compliance with GDPR. *CEUR Workshop Proceedings, 3800*, 70–80. https://ceur-ws.org/Vol-3800/
20. State Service for Special Communications and Information Protection of Ukraine. (2005). *ND TZI 3.7-003-2005. Procedure for conformity assessment of technical information protection means.* Kyiv.
21. Shirey, R. (2007). *Internet Security Glossary* (RFC 4949). IETF. https://www.rfc-editor.org/rfc/rfc4949
22. Ivanusa, A., Tkachuk, R., Brych, T., Balatska, V., & Tkachenko, A. (2024). Methods and models for designing a system for automated search of vulnerabilities in web applications. *Visnyk Lviv State University of Life Safety, 30*, 110–122. https://doi.org/10.32447/20784643.30.2024.11
23. Balatska, V., & Dmytriv, N. (2025). Inter-organizational exchange of confidential personal data based on permissioned blockchain. *Cybersecurity: Education, Science, Technique, 2*(29), 178–193. https://doi.org/10.28925/2663-4023.2025.29.875