КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.975
УДК 004.056.5:004.738.5:351.862

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

Ткачук Ростислав Львович
доктор технічних наук, професор,
професор кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0001-9137-1891
lvtk@ukr.net

Маслова Наталія Олександрівна
кандидат технічних наук, доцент
доцент кафедри управління інформаційною безпекою,
Львівський державний університет безпеки життєдіяльності, Львів, Україна
ORCID: 0000-0002-9078-0973
n.maslova@ldubgd.edu.ua

ЕВОЛЮЦІЯ КСЗІ ТА ІНТЕГРАЦІЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ У КІБЕРЗАХИСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ УКРАЇНИ

Анотація. У статті досліджено еволюцію концепції комплексних систем захисту інформації (КСЗІ) в умовах цифрової трансформації державного сектору, модернізації національної системи кіберзахисту та гармонізації законодавства України з міжнародними стандартами у сфері інформаційної безпеки. Розкрито взаємозв'язок між класичними підходами до побудови КСЗІ, які базувалися на обов'язковій атестації комплексів технічного захисту, та сучасною парадигмою ризик-орієнтованого управління безпекою, що передбачена новим Законом України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». У роботі акцентовано увагу на переході від формальної атестаційної моделі до процесного підходу, який базується на профілях захисту, управлінні ризиками, постійному моніторингу та аудиті безпеки. Окремо проаналізовано потенціал блокчейн-технологій у контексті підвищення рівня стійкості державних інформаційних систем до кібератак, внутрішніх загроз і несанкціонованих змін даних. Обґрунтовано доцільність використання розподілених реєстрів для забезпечення незмінності, достовірності, прозорості та підзвітності інформаційних процесів. Визначено, що блокчейн може виступати інноваційним елементом у сучасній архітектурі КСЗІ, доповнюючи криптографічні механізми захисту, контроль доступу, аудит дій користувачів та моніторинг подій. Запропоновано концептуальну модель інтеграції блокчейн-механізмів у традиційну структуру КСЗІ, що сприяє формуванню нової екосистеми довіри в державних інформаційних ресурсах. Показано, що поєднання технологічних інновацій із вимогами Закону № 4336-IX створює основу для підвищення ефективності національної системи кіберзахисту. Метою дослідження є обґрунтування науково-методичних і технологічних напрямів модернізації КСЗІ України шляхом інтеграції блокчейн-технологій у процес забезпечення захисту державних інформаційних ресурсів відповідно до вимог чинного законодавства, міжнародних стандартів ISO/IEC 27001, 27701 та GDPR.

Ключові слова: комплексна система захисту інформації; КСЗІ; блокчейн; кіберзахист; державні інформаційні ресурси; критична інформаційна інфраструктура; управління ризиками; профіль безпеки; Закон України № 4336-IX; розподілені реєстри; цілісність даних; криптографічний захист; аудит; ISO/IEC 27001; ISO/IEC 27701; GDPR.

ВСТУП

У сучасних умовах цифрової трансформації державного управління інформація стала одним із найцінніших стратегічних ресурсів. Відповідно, питання її захисту, цілісності, автентичності та доступності набули особливого значення як на рівні держави, так і в межах критичної інформаційної інфраструктури. Зростання обсягів оброблюваних даних, активне впровадження електронного врядування, а також поширення штучного інтелекту та хмарних технологій формують нові виклики для систем захисту інформації [1]. Однією з ключових складових національної системи технічного захисту інформації України залишається комплексна система захисту інформації (КСЗІ), яка забезпечує реалізацію організаційних, технічних і криптографічних заходів для запобігання несанкціонованому доступу до інформаційних ресурсів. Модель КСЗІ, сформована у 1990-х роках, тривалий час базувалася на принципі обов'язкової атестації інформаційно-комунікаційних систем та наявності сертифікованих засобів технічного захисту інформації. Проте стрімка цифровізація та динаміка кіберзагроз зумовили необхідність переходу до нових, гнучкіших і адаптивних підходів.

У 2025 році було ухвалено Закон України № 4336-IX «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», який став логічним продовженням реалізації Національної стратегії у сфері кібербезпеки. Цей закон запровадив низку принципових новацій: перехід від жорстко регламентованої моделі КСЗІ до ризик-орієнтованого підходу, впровадження профілів безпеки, створення національної системи обміну інформацією про кіберінциденти та посилення відповідальності суб'єктів кіберзахисту. Також документ гармонізує українське законодавство з європейськими практиками управління інформаційною безпекою відповідно до стандартів ISO/IEC 27001 та ISO/IEC 27701.

У межах нової нормативної парадигми актуальним стає питання інтеграції інноваційних технологій, здатних підвищити довіру, прозорість і відмовостійкість державних інформаційних систем. Однією з таких технологій є блокчейн – розподілена система зберігання даних, що забезпечує незмінність записів і децентралізований контроль над доступом. Використання блокчейн у сфері державного управління дає можливість створювати захищені журнали подій, системи електронної ідентифікації та аудиту, а також формувати довірені середовища між різними органами влади.

Інтеграція блокчейн-рішень у структуру КСЗІ відкриває перспективи для побудови нової екосистеми довіри у державних реєстрах, фінансових, медичних та адміністративних сервісах. Зокрема, застосування технологій розподіленого реєстру може забезпечити верифікацію цілісності даних, контроль автентичності електронних транзакцій і захист від внутрішніх загроз, які традиційно складно виявити засобами класичних систем моніторингу. Разом із тим впровадження блокчейн-підходів у державні інформаційні системи має відбуватися в межах діючої нормативної бази та принципів державної політики у сфері технічного захисту інформації. Тому постає завдання дослідити, яким чином блокчейн може бути інтегрований у оновлену модель

КСЗІ, що формується відповідно до Закону № 4336-IX, і які науково-методичні засади повинні регламентувати цей процес.

Метою дослідження є обґрунтування напрямів модернізації комплексних систем захисту інформації в Україні шляхом інтеграції блокчейн-технологій у процес забезпечення кіберзахисту державних інформаційних ресурсів відповідно до вимог чинного законодавства та міжнародних стандартів інформаційної безпеки.

Постановка проблеми.

Система технічного та організаційного захисту інформації в Україні тривалий час ґрунтувалася на положеннях Закону України «Про захист інформації в інформаційно-комунікаційних системах» [1] та нормативних документах Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ). Основним інструментом реалізації вимог безпеки виступала комплексна система захисту інформації (КСЗІ), що забезпечувала регламентований набір технічних, програмних і криптографічних засобів для захисту даних в інформаційних системах.

Однак, модель КСЗІ, яка формувалася у 1990-2000-х роках, виявилася надто статичною та нормативно орієнтованою. Її впровадження вимагало проведення тривалих процедур проєктування, сертифікації та атестації, що часто не відповідало темпам розвитку цифрових сервісів, електронного врядування й динамічним загрозам сучасного кіберпростору [2; 3]. Підхід «жорсткої атестації» обмежував можливість оперативного реагування на нові ризики, а також ускладнював застосування інноваційних технологій, які не входили до чинних державних реєстрів засобів технічного захисту інформації.

Розвиток державних електронних сервісів (зокрема систем типу «Дія», Єдиних державних реєстрів, галузевих баз даних) та зростання кількості кіберінцидентів продемонстрували необхідність оновлення нормативної бази у сфері інформаційної безпеки. Прийняття у 2025 році Закону України № 4336-IX [4] започаткувало реформування системи кіберзахисту та поступовий перехід від моделі КСЗІ до ризик-орієнтованої архітектури безпеки. Цей підхід передбачає не стільки формальне виконання вимог, скільки постійне управління ризиками, профілями безпеки та аудитом стану захищеності [5; 6].

Разом з тим залишається відкритим питання інтеграції інноваційних технологій, таких як блокчейн, у структуру національної системи технічного захисту інформації. Попри наявність наукових досліджень щодо використання розподілених реєстрів для забезпечення цілісності даних, у вітчизняній нормативній базі відсутні механізми, які б визнавали такі рішення складовою частиною сертифікованих КСЗІ. Це створює певний розрив між потенціалом сучасних технологій і формальними вимогами державних стандартів.

Таким чином, проблема дослідження полягає у визначенні шляхів модернізації КСЗІ України через адаптацію її архітектури до ризик-орієнтованого підходу, визначеного Законом № 4336-IX, та інтеграцію блокчейн-технологій як механізму підвищення довіри, прозорості та цілісності інформаційних процесів у державних інформаційних системах.

Аналіз останніх досліджень і публікацій.

Наукові праці останнього десятиліття засвідчили зсув від суто нормативно-процедурних моделей побудови КСЗІ до ризик-орієнтованих підходів управління безпекою, що інтегрують цикли постійного моніторингу, аудит та вдосконалення (Plan-Do-Check-Act). Стандарти ISO/IEC 27001 та розширення для приватності ISO/IEC 27701 формують каркас вимог до політик, процесів і доказової бази контролів, що дедалі частіше розглядається як основа для модернізації національних режимів технічного

захисту інформації. У суміжних дослідженнях відзначено, що класичні КСЗІ ефективні для стабільних контурів, проте демонструють обмежену чутливість до швидкоплинних загроз, властивих хмарним та розподіленим середовищам [7].

Окремий пласт публікацій присвячено застосуванню блокчейн-технологій у державному секторі. Роботи з електронного урядування підкреслюють потенціал розподілених реєстрів для забезпечення цілісності журналів подій, незмінності критичних записів та підзвітності операцій доступу до даних [8]. Дослідження permissioned-архітектур (зокрема, Hyperledger Fabric) показують можливість тонкого керування правами учасників, продуктивності рівня державних реєстрів і сумісності з існуючими криптографічними засобами. Паралельно триває активна дискусія щодо поєднання блокчейн з інфраструктурою відкритих ключів (PKI) – пропонуються моделі реєстру сертифікатів та протоколювання OCSP-подій у ланцюгах блоків для підвищення довіри та відстежуваності.

Водночас наукова спільнота фіксує низку бар'єрів: колізії між immutability та вимогами права на видалення/виправлення персональних даних, зокрема у межах GDPR; питання визначення ролей controller/processor у децентралізованих екосистемах; масштабованість і затримки консенсусу; а також інтеграція з державними реєстрами, що вже використовують сертифіковані засоби технічного захисту [9]. Європейські підходи пропонують техніки «selective disclosure», off-chain зберігання чутливих атрибутів та використання нульових доказів (ZKP) для зниження ризиків розкриття .

В українському контексті в останні роки з'явилися праці, що моделюють застосування блокчейну для забезпечення цілісності та достовірності записів у міжвідомчих обмінах, а також прототипи аудиторських реєстрів подій для державних IT-систем. Паралельно напрацьовано аналітику щодо обмежень традиційної моделі атестації КСЗІ у швидкозмінних цифрових сервісах та необхідності переходу до профілів безпеки, керованих ризиками. Прийняття у 2025 році Закону України № 4336-IX зафіксувало цей поворот, формалізувавши ризик-орієнтоване управління, профілі безпеки та системну взаємодію з кіберінцидентами на національному рівні [10].

Підсумовуючи, сучасний стан досліджень демонструє: (1) зрілість процесних і ризик-орієнтованих рамок (ISO/IEC 27001/27701) для модернізації КСЗІ; (2) доказову базу користі permissioned-блокчейн-рішень для цілісності та підзвітності; (3) наявність правових і технологічних розривів (GDPR-сумісність, ролі, масштабованість) у державних застосуваннях. Невирішеною залишається задача методологічно вивіреної інтеграції блокчейн-механізмів у оновлену архітектуру КСЗІ України відповідно до Закону № 4336-IX – із чіткими профілями безпеки, критеріями оцінювання ефективності та вимогами сумісності з сертифікованими засобами ТЗІ. Саме цю лакуну адресує подальше дослідження.

Мета статті. Метою статті є наукове обґрунтування напрямів модернізації національної системи технічного захисту інформації України шляхом інтеграції інноваційних технологій, зокрема блокчейн-підходів, у структуру комплексних систем захисту інформації (КСЗІ). Такий підхід спрямований на підвищення рівня довіри, прозорості, цілісності та підзвітності державних інформаційних ресурсів у контексті реалізації положень Закону України № 4336-IX та міжнародних стандартів ISO/IEC 27001 і 27701.

Основними завданнями статті виступають:

1. Проаналізувати еволюцію розвитку КСЗІ в Україні від моменту формування базових принципів технічного захисту інформації до впровадження сучасних ризик-орієнтованих моделей управління кібербезпекою.

2. Дослідити нормативно-правові передумови реформування національної системи технічного захисту інформації у зв'язку з прийняттям Закону України № 4336-IX та гармонізацією законодавства із європейськими стандартами.

3. Розкрити сутність ризик-орієнтованого підходу до управління інформаційною безпекою та визначити його переваги порівняно з традиційною моделлю атестації КСЗІ.

4. Оцінити потенціал блокчейн-технологій у підвищенні стійкості державних інформаційних систем до кіберзагроз, забезпеченні незмінності, автентичності й достовірності даних.

5. Запропонувати концептуальну модель інтеграції блокчейн-механізмів у структуру сучасної КСЗІ з урахуванням вимог чинного законодавства та міжнародних стандартів безпеки.

6. Сформулювати рекомендації щодо подальшого розвитку нормативної та методологічної бази побудови КСЗІ на принципах управління ризиками, прозорості й інноваційності.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Аналіз еволюції архітектури КСЗІ

Формування системи технічного захисту інформації в Україні розпочалося ще у 1990-х роках, коли державні органи вперше зіткнулися з потребою створення єдиних підходів до захисту електронних даних у державних інформаційно-комунікаційних системах. В основі цієї моделі лежав нормативно-регламентований підхід, який передбачав чітке визначення засобів, процедур і етапів побудови комплексних систем захисту інформації (КСЗІ) [1; 2].

Перші КСЗІ проектувалися відповідно до вимог Закону України «Про захист інформації в інформаційно-комунікаційних системах» (1994 р.) та стандарту ДСТУ 3396.2-96, який визначав базові принципи технічного захисту інформації. Відповідно до цих документів, побудова КСЗІ включала послідовність етапів: обстеження інформаційної системи, розроблення моделі загроз, проектування комплексу захисту, впровадження технічних засобів, випробування, сертифікацію та атестацію [11].

Такий підхід забезпечував високу формалізацію процесів, проте мав обмежену гнучкість. У період активного розвитку ІКТ (2000-2015 рр.) виникла проблема технологічного відставання КСЗІ від реальних потреб державних і комерційних структур. Модель «жорсткої атестації» не враховувала швидкоплинність кіберзагроз і появу нових типів сервісів (хмарні платформи, електронні сервіси, віддалений доступ), що не підпадали під класичні схеми сертифікації.

Крім того, централізований характер управління КСЗІ призводив до фрагментації систем захисту – кожна установа проектувала власну систему без уніфікованих профілів безпеки чи механізмів взаємодії. Це обмежувало міжвідомчий обмін інформацією, ускладнювало аудит і підвищувало ризики людського фактора.

Починаючи з 2020-х років, під впливом міжнародних тенденцій (зокрема стандартів ISO/IEC 27001, ISO/IEC 27701, NIST SP 800-53) почала формуватися нова парадигма ризик-орієнтованого управління безпекою. Вона передбачає відхід від суто атестаційної логіки до постійного циклу оцінки ризиків, моніторингу загроз та вдосконалення контрзаходів (Plan-Do-Check-Act). У 2021 р. прийняття Національної стратегії кібербезпеки [12] закріпило цей підхід на рівні державної політики.

Ключовим етапом еволюції стало ухвалення у 2025 р. Закону України № 4336-IX, який фактично перезапускає нормативну архітектуру КСЗІ. Закон вводить:

- ризик-орієнтовану модель безпеки, де головним об’єктом управління стають ризики, а не формальні атестаційні показники;
- профілі безпеки – типові конфігурації заходів для систем різного рівня критичності;
- національну систему обміну інформацією про кіберінциденти;
- посилення ролі аудиту та внутрішнього контролю у системах кіберзахисту.

Така еволюція означає перехід від закритої моделі «КСЗІ як продукту» до моделі «КСЗІ як процесу», що постійно вдосконалюється та реагує на нові загрози. Основними ознаками сучасної архітектури є:

- адаптивність (оновлення заходів захисту відповідно до динаміки ризиків);
- сумісність (інтеграція з міжвідомчими системами через захищені шлюзи й профілі безпеки);
- транспарентність (журналювання та контроль дій у реальному часі);
- довіра (використання інноваційних технологій, таких як блокчейн, для верифікації подій).

Інтеграція блокчейн-рішень у нову архітектуру КСЗІ логічно продовжує цю еволюцію. Технологія розподілених реєстрів може стати «четвертим рівнем довіри» після організаційного, технічного та криптографічного – забезпечуючи незмінність аудиту, доказовість дій користувачів і незалежну перевірюваність даних у масштабах міжорганізаційної взаємодії [13].

Таким чином, еволюція КСЗІ – це шлях від нормативно закритої, централізованої системи до гнучкої, інтегрованої, ризик-орієнтованої моделі кіберзахисту, яка здатна функціонувати у середовищі цифрової держави.

Інтеграція блокчейн-технологій у структуру КСЗІ

Подальший розвиток архітектури комплексних систем захисту інформації в Україні вимагає впровадження інноваційних технологій, здатних підвищити рівень цілісності, довіри та прозорості інформаційних процесів у державних системах. Однією з найперспективніших у цьому контексті є блокчейн-технологія, що забезпечує зберігання даних у вигляді послідовних, криптографічно зв’язаних блоків, які неможливо змінити без згоди учасників мережі [14].

У класичній архітектурі КСЗІ основна увага зосереджується на превентивних заходах: криптографічному захисті, ідентифікації користувачів, розмежуванні доступу та аудиті дій. Проте у середовищах з підвищеною міжвідомчою взаємодією цього недостатньо – адже класичні системи журналювання та моніторингу зберігають записи централізовано, що залишає ризик їх модифікації або видалення адміністраторами.

Блокчейн дозволяє реалізувати незмінний журнал подій (immutable audit trail), у якому кожна транзакція (доступ до даних, зміна запису, видача дозволу) фіксується у вигляді блоку, підписаного цифровими ключами відповідальних суб’єктів. Такий підхід забезпечує криптографічну достовірність, повну простежуваність і незалежну перевірюваність історії подій.

Можливі напрями інтеграції блокчейн у КСЗІ:

1. Журналювання транзакцій доступу (Audit blockchain) – фіксація фактів звернень до конфіденційної інформації, дій адміністраторів і змін у системі у вигляді блоків, що підписуються криптографічно та зберігаються у permissioned-мережі.

2. Верифікація цілісності даних (Data integrity control) – збереження контрольних гешів об’єктів даних у блокчейні для виявлення несанкціонованих змін у базах даних або державних реєстрах.

3. Управління цифровими сертифікатами (Blockchain PKI) – реєстрація, перевірка та відкликання сертифікатів електронних підписів у децентралізованому реєстрі, що зменшує залежність від єдиного центру сертифікації [15].

4. Децентралізоване управління доступом (Smart-contract access control) – використання смарт-контрактів для автоматизованого підтвердження прав користувачів на доступ до інформаційних об'єктів залежно від контексту, часу або ролі.

5. Верифікація подій кіберзахисту (Incident validation) – обмін повідомленнями між державними CSIRT/SOC через блокчейн-реєстр інцидентів, що унеможливлює фальсифікацію результатів розслідувань.

Такі механізми забезпечують не лише підзвітність і прозорість, а й підтримують реалізацію принципів Zero Trust Architecture, передбачених сучасними концепціями кіберзахисту [6].

Переваги та обмеження інтеграції:

Переваги: підвищення довіри між суб'єктами міжвідомчої взаємодії; створення незалежного джерела доказів дій у системі; мінімізація ризику внутрішніх загроз; забезпечення незмінності журналів аудиту; узгодженість з ризик-орієнтованою моделлю управління безпекою.

Обмеження: відсутність у національних стандартах формальних вимог до сертифікації блокчейн-компонентів у складі КСЗІ; потреба у створенні законодавчих підстав для визнання блокчейн-записів юридично значущими; необхідність розробки методик оцінки продуктивності та надійності блокчейн-рішень [16]. Таким чином, інтеграція блокчейн-технологій у структуру КСЗІ дозволяє реалізувати принцип «довіра через технологію» – забезпечуючи перевірюваність, цілісність і доказовість усіх транзакцій у державних інформаційних системах. Вона є ключовим кроком у переході від традиційних централізованих механізмів до розподіленої архітектури кіберзахисту, що відповідає цілям цифрової трансформації держави та вимогам Закону № 4336-IX.

Ризик-орієнтований підхід до управління інформаційною безпекою та його переваги над традиційною моделлю атестації КСЗІ

Сучасна парадигма управління інформаційною безпекою у державних і корпоративних системах ґрунтується на ризик-орієнтованому підході, який поступово замінює традиційну модель атестації КСЗІ.

На відміну від регламентованої системи, де головним критерієм ефективності була відповідність технічним вимогам і наявність атестата, нова модель орієнтована на безперервне виявлення, оцінювання й мінімізацію ризиків, що загрожують активам інформаційної системи [17].

Ризик-орієнтований підхід базується на системному циклі «Plan-Do-Check-Act» (PDCA), передбаченому стандартом ISO/IEC 27001:2022, і розглядає інформаційну безпеку як динамічний процес управління ризиками, а не як статичний стан відповідності.

У центрі цієї моделі – оцінювання ризиків (risk assessment), яке охоплює:

- Ідентифікацію активів і загроз (hardware, software, data, персонал, бізнес-процеси);
- Оцінку вразливостей та ймовірності реалізації загроз;
- Квантифікацію ризику (за формулою Risk = Threat × Vulnerability × Impact);
- Вибір оптимальних контрзаходів із урахуванням витрат, ефективності й критичності об'єкта;
- Моніторинг і постійне вдосконалення засобів безпеки.

Такий підхід забезпечує гнучкість системи, оскільки дозволяє змінювати набір захисних механізмів залежно від актуальної ситуації, рівня загроз і пріоритетів організації.

Ключовою особливістю ризик-орієнтованої моделі є орієнтація на наслідки (impact-oriented thinking): головне завдання – не запобігти кожній атаці, а мінімізувати її потенційний вплив на критичні бізнес-процеси. Це відповідає концепції "cyber resilience", яка передбачає здатність системи продовжувати функціонування навіть після успішного інциденту безпеки [18].

У традиційній моделі КСЗІ, яка домінувала в Україні до 2020-х років, головним завданням було створити та атестувати систему відповідно до нормативних вимог.

Фактично, процес безпеки завершувався на етапі отримання "атестата відповідності", після чого система могла тривалий час функціонувати без переоцінки ризиків.

Таке управління мало формальний характер і не враховувало еволюцію загроз, що призводило до технологічного відставання і низької оперативності реагування на інциденти [5].

На противагу цьому, ризик-орієнтований підхід передбачає безперервність управління безпекою.

Він вимагає періодичного перегляду оцінок ризику, оновлення профілів захисту та документування всіх змін.

Рішення щодо впровадження контрзаходів приймаються не "згори", а на основі аналізу фактичних загроз, статистики атак, аудиту SOC/CSIRT і результатів внутрішнього моніторингу. Порівняльні характеристики моделей подано в таблиці 1.

Таблиця 1.

Порівняння традиційної та ризик-орієнтованої моделей управління безпекою КСЗІ

Критерій	Традиційна модель атестації КСЗІ	Ризик-орієнтована модель управління безпекою
Основна мета	Відповідність нормативним вимогам	Безперервне управління ризиками
Оцінка безпеки	Проводиться одноразово (перед атестацією)	Проводиться регулярно, за зміною середовища
Підхід до контролю	Формальний, документальний	Аналітичний, базований на фактичних даних
Критерій ефективності	Наявність сертифіката/атестата	Зниження рівня залишкового ризику
Реакція на загрози	Реактивна (після інцидентів)	Проактивна (на основі прогнозів і моніторингу)
Управління змінами	Рідко або відсутнє	Постійне, із зворотним зв'язком
Роль людини	Централізоване прийняття рішень	Розподілена відповідальність, автоматизація
Міжвідомча взаємодія	Відсутня або обмежена	Кооперативна через спільні профілі ризиків
Технологічна адаптивність	Обмежена сертифікованими засобами	Відкрита до інновацій (блокчейн, AI, ML)

Порівняльний аналіз (табл. 1) показав, що ризик-орієнтований підхід забезпечує вищу гнучкість і адаптивність систем захисту, дозволяючи своєчасно реагувати на нові кіберзагрози. На відміну від традиційної моделі атестації КСЗІ, яка має статичний і формальний характер, ризик-орієнтована модель передбачає постійний моніторинг,

оновлення контрзаходів та зниження залишкового ризику. Такий підхід узгоджується з міжнародними стандартами ISO/IEC 27001, 27005 і Законом України № 4336-IX, формуючи основу для побудови сучасної системи управління кібербезпекою державних інформаційних ресурсів. Використання ризик-орієнтованої моделі забезпечує низку стратегічних переваг:

- Гнучкість – можливість адаптації системи безпеки до змін зовнішнього середовища та нових типів загроз;
- Оптимальність витрат – пріоритезація контрзаходів за критичністю активів;
- Прозорість – документування процесів оцінки ризиків і прийняття рішень;
- Безперервність захисту – впровадження моніторингу, аналітики SOC та динамічних політик доступу;
- Інтеграція з міжнародними стандартами – відповідність вимогам ISO/IEC 27001, ISO/IEC 27005, GDPR, NIST CSF;
- Підґрунтя для інновацій – створення умов для застосування блокчейн, машинного навчання, поведінкової аналітики.

Таким чином, ризик-орієнтований підхід трансформує КСЗІ з пасивної, сертифікаційної системи у активну, самонавчальну екосистему кіберзахисту, що забезпечує адаптивність, стійкість і доказовість безпеки у державних інформаційних системах.

Потенціал блокчейн-технологій у підвищенні стійкості державних інформаційних систем

Сучасні державні інформаційні системи України переживають трансформацію, спричинену одночасно процесами цифровізації публічного сектору та зростанням складності кіберзагроз [19]. Перехід від розрізнених баз даних і сервісів до взаємопов’язаної інфраструктури електронного урядування висуває нові вимоги до надійності, довіри й прозорості обробки інформації. У цих умовах традиційні моделі захисту, засновані на централізованих засобах контролю та атестації, дедалі частіше демонструють обмеження: вони не забезпечують перевірюваність подій у режимі реального часу, залежать від людського фактору й не дають гарантії незмінності даних у міжвідомчому середовищі.

Одним із напрямів технологічної модернізації, який здатен усунути ці недоліки, є застосування блокчейн-технологій – розподілених реєстрів, що поєднують принципи криптографічного підтвердження, консенсусу та незалежної верифікації транзакцій. У контексті кібербезпеки державних систем блокчейн розглядається не як заміна традиційних засобів захисту, а як додатковий рівень довіри, що підсилює цілісність і достовірність інформаційних процесів.

Блокчейн забезпечує створення єдиного простору довіри між різними суб’єктами – державними органами, муніципалітетами, підрядниками, банками та громадянами. Його принципова відмінність полягає у відсутності центрального контролера: кожен учасник системи має копію ланцюга транзакцій і може перевірити правильність будь-якої операції. Це усуває можливість прихованих змін у даних, фальсифікації записів або маніпуляцій з боку адміністраторів системи.

Впровадження блокчейн-підходу особливо актуальне для тих сфер, де відсутність довіри між учасниками є критичною проблемою: ведення державних реєстрів, розподіл фінансових ресурсів, управління виборчими процесами, ідентифікація громадян. Усі ці напрями об’єднує потреба у гарантованій незмінності та доказовості дій, які здійснюються в електронному вигляді.

У державних інформаційних системах традиційно контроль за подіями здійснюється через журнали аудиту, які зберігаються централізовано. Проте така модель має очевидні ризики: адміністратор може змінити або видалити записи; неможливо довести, що певна операція справді відбулася чи, навпаки, не виконувалася. Блокчейн вирішує цю проблему, адже кожна подія записується у вигляді транзакції з унікальним криптографічним підписом, а її підтвердження потребує узгодження більшості вузлів мережі. Будь-яка спроба підробки призведе до розходження у хеш-ланцюгу, що буде миттєво виявлено. Таким чином, система отримує властивість криптографічної незмінності (immutability) – фундаментальний критерій кіберстійкості [20].

Ще однією перевагою є автоматизація процесів управління доступом. Використання смарт-контрактів дає змогу задати правила, за якими система самостійно перевіряє повноваження користувача перед виконанням операції. Наприклад, при запиті до державного реєстру блокчейн може автоматично перевірити цифровий сертифікат, підтвердити автентичність запиту й зафіксувати результат перевірки у спільному реєстрі. У такий спосіб знижується ризик людської помилки або навмисного порушення процедур доступу.

Крім підвищення цілісності даних, блокчейн сприяє формуванню нового рівня підзвітності. Усі дії користувачів, адміністраторів і сервісів залишають незмінний цифровий слід. Це суттєво полегшує розслідування інцидентів, дає змогу проводити незалежні аудити та формує доказову базу у випадку порушення безпеки.

Такі властивості надзвичайно важливі в умовах реформування системи технічного захисту інформації відповідно до Закону України № 4336-IX, який вимагає прозорості, відстежуваності та доказовості дій у кіберпросторі.

З точки зору архітектури КСЗІ, блокчейн можна розглядати як надбудову над традиційними засобами контролю, що додає четвертий – верифікаційний рівень. Якщо раніше систему будували на основі трьох компонентів – організаційного, технічного та криптографічного – то блокчейн створює додатковий шар підтвердження, який унеможливлює порушення узгодженості між ними. Таким чином, з’являється концепція “trust through technology” – довіра забезпечується не організаційними наказами, а математичними доказами.

Варто наголосити, що ефективність блокчейн-підходу безпосередньо залежить від типу мережі. Для державних систем прийнятними є permissioned-мережі (з обмеженим колом учасників), такі як Hyperledger Fabric або Quorum. Вони дозволяють поєднати переваги розподіленої структури з вимогами нормативного контролю: зберігати анонімність публічних вузлів, керувати доступом і сертифікатами через довірені центри, дотримуючись вимог законодавства про захист персональних даних.

У практичному сенсі інтеграція блокчейну може бути реалізована у вигляді “реєстру контрольних відбитків” (hash ledger). Це означає, що самі дані залишаються у внутрішніх базах державних установ, а до блокчейну записуються лише контрольні хеші – криптографічні відбитки, які дають змогу підтвердити цілісність без розкриття змісту. Такий підхід відповідає принципам off-chain storage, рекомендованим GDPR, і не суперечить політикам конфіденційності.

У стратегічній перспективі впровадження блокчейн-технологій створює передумови для переходу державних систем до моделі розподіленого управління ризиками. Дані про інциденти безпеки, аномальні події чи зміни конфігурацій можуть фіксуватися в єдиному блокчейн-реєстрі, доступному для CSIRT-центрів різних органів влади. Це спрощує обмін достовірною інформацією, скорочує час реакції на атаки та дозволяє виявляти міжвідомчі залежності у ланцюгах кіберінцидентів.

Попри очевидні переваги, блокчейн не є “чарівною таблеткою”. Його ефективність обмежується потужністю мережі, рівнем синхронізації вузлів і необхідністю гармонізації з чинними процедурами КСЗІ. Технологія не замінює криптографічного захисту чи політик доступу, але істотно підсилює їхню доказовість. Найбільший ефект досягається тоді, коли блокчейн впроваджується не як окремий компонент, а як інтегрована частина ризик-орієнтованої архітектури, де кожна транзакція оцінюється через призму потенційного впливу на безпеку.

Потенціал блокчейн-технологій полягає у створенні нової моделі довіри для державних інформаційних систем. Вона базується на прозорості процесів, взаємному контролі учасників і технічній неможливості приховати чи спотворити дані. Це не лише підвищує кіберстійкість, а й формує основу для сучасного цифрового урядування, у якому довіра громадян і органів влади підтримується математично, а не адміністративно.

Концептуальна модель інтеграції блокчейн-механізмів у структуру сучасної КСЗІ

Перехід України до цифрового врядування, що охоплює електронні послуги, міжвідомчий обмін та автоматизоване прийняття рішень, потребує якісно нового рівня довіри у взаємодії між державними установами [21]. Традиційна архітектура КСЗІ, заснована на централізованому управлінні й статичних засобах контролю, не забезпечує належного рівня прозорості та доказовості процесів, особливо в умовах зростання міжорганізаційних транзакцій.

Блокчейн-технології дозволяють розширити межі класичних систем захисту, додавши до них механізми розподіленої верифікації, незмінності та доказовості даних [22]. У поєднанні з ризик-орієнтованою моделлю, визначеною Законом України № 4336-IX, це створює основу для формування нового типу КСЗІ – гнучкої, самоверифікованої та прозорої системи кіберзахисту.

У межах проведеного дослідження запропоновано узагальнену концептуальну модель інтеграції блокчейн-механізмів у структуру сучасної КСЗІ, яка враховує принципи безперервного управління ризиками, багаторівневий моніторинг безпеки та необхідність доказовості усіх дій користувачів (рис. 1). Модель узгоджена з положеннями Закону України № 4336-IX, ISO/IEC 27001:2022 та ISO/IEC 27701.

Рис. 1. Модель інтеграції блокчейн-технологій у структуру КСЗІ

Модель відображає поетапну взаємодію трьох рівнів захисту – організаційного, технічного та верифікаційного, що функціонують у єдиному замкненому циклі інформаційної безпеки.

На організаційному рівні формується нормативно-управлінське середовище: визначаються політики захисту, правила доступу, механізми управління ризиками, а також відповідальність суб'єктів за дії в системі. Тут закладається логіка ризик-орієнтованого управління, коли всі процеси безпеки оцінюються через призму потенційного впливу на активи та загальну стійкість системи. Цей рівень задає рамкові параметри взаємодії між учасниками – хто може реєструвати події, підтверджувати транзакції, здійснювати моніторинг або аудит.

На технічному рівні реалізуються класичні засоби захисту інформації: криптографічні алгоритми, автентифікація користувачів, контроль доступу, антивірусний і мережевий моніторинг. Саме тут відбувається інтеграція блокчейн-технологій: кожна критична транзакція або подія в системі автоматично фіксується у вигляді хешу у розподіленому реєстрі. Такий підхід забезпечує незмінність аудиту та повну простежуваність дій, незалежно від системного адміністратора.

Важливо, що дані користувачів не зберігаються у блокчейні напряму – у ланцюгу реєструються лише контрольні відбитки, що виключає ризики порушення вимог GDPR і Закону України «Про захист персональних даних».

Верифікаційний рівень виступає технологічною надбудовою, яка забезпечує незалежне підтвердження достовірності дій та інформаційних транзакцій. Тут реалізуються смарт-контракти, які автоматизують перевірку прав доступу, верифікацію подій і контроль політик безпеки. На цьому ж рівні функціонують аудиторські вузли, які підтверджують правильність транзакцій за допомогою консенсусу. Таким чином, формується додатковий рівень довіри – коли доказовість дій забезпечується не організаційним контролем, а технологічним механізмом.

Взаємодія між рівнями є циклічною: організаційні правила формують політику дій; технічні системи реалізують ці політики; верифікаційний рівень підтверджує правильність і фіксує результат у незмінному журналі. Отже, КСЗІ перетворюється на самоперевірювану систему, де контроль і довіра є невіддільними властивостями.

Розроблена модель демонструє, що інтеграція блокчейн-механізмів у КСЗІ не лише підвищує технічну стійкість системи до несанкціонованих змін, а й створює нову парадигму кіберзахисту – від централізованого адміністрування до розподіленої відповідальності та доказовості.

Завдяки цьому забезпечується повна підзвітність усіх дій, мінімізується ризик маніпуляцій з боку адміністраторів, спрощується аудит і формуються умови для міжвідомчого обміну достовірною інформацією.

Така архітектура повністю узгоджується з положеннями Закону України № 4336-IX, який орієнтує систему технічного захисту на безперервний моніторинг, оцінку ризиків і прозорість процесів.

Блокчейн, у цьому контексті, виконує роль технологічного каталізатора: він не замінює традиційні механізми КСЗІ, але переводить їх на рівень верифікованої довіри, де кожен факт обробки даних може бути доведений, перевірений і підтверджений без зовнішнього посередника.

У підсумку, модель інтеграції блокчейн-механізмів у КСЗІ можна розглядати як етап еволюції національної системи кіберзахисту: від формальної атестації – до ризик-орієнтованого управління, від централізованого контролю – до технологічно

підтвердженої прозорості, від закритих інформаційних структур – до відкритих, але захищених екосистем цифрової довіри.

За результатами проведеного аналізу можна сформулювати низку практичних рекомендацій щодо подальшого розвитку нормативної, методологічної та технологічної бази побудови КСЗІ в Україні:

1. Перехід до ризик-орієнтованих профілів безпеки. Доцільно передбачити у підзаконних актах до Закону № 4336-IX типові профілі безпеки для державних інформаційних систем різного рівня критичності, що базуються на оцінюванні ризиків та залишкового ризику відповідно до ISO/IEC 27005.

2. Інституціоналізація блокчейн-компонентів у системі ТЗІ. Необхідно розробити методичні рекомендації ДССЗЗІ щодо використання технологій розподіленого реєстру (permissioned blockchain) як елементу КСЗІ – зокрема для забезпечення незмінності журналів подій, аудиту та контролю доступу.

3. Правове визнання блокчейн-записів. Доцільно внести зміни до нормативно-правових актів у сфері електронного документообігу та технічного захисту інформації, що гарантуватимуть юридичну силу даних, зафіксованих у блокчейн-журналах, у процесах аудиту, атестації та розслідування інцидентів.

4. Удосконалення системи сертифікації. Варто створити окрему процедуру оцінювання надійності та продуктивності блокчейн-рішень, інтегрованих у КСЗІ, із залученням механізмів лабораторної перевірки та пілотних державних проектів (наприклад, у реєстрах Мін'юсту, МОЗ, МВС).

5. Розвиток національної мережі обміну кіберінцидентами. Рекомендується інтегрувати блокчейн-реєстри подій у взаємодію між урядовими CSIRT/SOC для створення прозорої та довіреної системи фіксації інцидентів кібербезпеки з унеможливленням їх фальсифікації або втрати.

6. Підготовка кадрів та оновлення освітніх програм. Доцільно розширити навчальні плани підготовки фахівців з кібербезпеки новими модулями з ризик-менеджменту, цифрової довіри та блокчейн-технологій, формуючи компетентності для практичного застосування таких рішень у державних ІКС.

7. Створення науково-технічних центрів компетенцій. Варто підтримати створення міжвідомчих лабораторій і центрів дослідження інноваційних технологій КСЗІ (зокрема блокчейн, Zero Trust, AI-аналітика), що виконуватимуть функції експертної підтримки ДССЗЗІ та органів кіберзахисту.

Запровадження наведених рекомендацій дозволить перейти від фрагментованої системи технічного захисту інформації до цілісної екосистеми управління ризиками, що базується на принципах довіри, прозорості та технологічної верифікації.

ВИСНОВКИ

Проведене дослідження дозволило всебічно проаналізувати еволюцію підходів до побудови комплексних систем захисту інформації (КСЗІ) в Україні та визначити напрями їх модернізації в умовах цифрової трансформації державного сектору. Встановлено, що традиційна атестаційна модель, яка формувалася у 1990–2000-х роках, забезпечувала високий рівень формальної відповідності нормативним вимогам, проте не відповідала динаміці сучасних кіберзагроз і темпам розвитку інформаційно-комунікаційних технологій. Її надмірна зарегламентованість та централізований характер управління призводили до фрагментації систем безпеки, обмеженої адаптивності та низької швидкості реагування на інциденти.

Прийняття у 2025 році Закону України № 4336-IX стало ключовим етапом реформування системи технічного захисту інформації та започаткувало перехід до ризик-орієнтованого підходу, який відповідає міжнародним стандартам ISO/IEC 27001, 27005 та 27701. Така трансформація спрямована на побудову гнучких, процесно-орієнтованих КСЗІ, у яких головним об'єктом управління стає не набір технічних засобів, а ризики, що загрожують інформаційним активам. Цей підхід дозволяє забезпечити безперервний моніторинг стану безпеки, пріоритизацію контрзаходів за критичністю активів, зниження залишкового ризику та інтеграцію сучасних механізмів кіберзахисту.

У межах роботи обґрунтовано, що інтеграція блокчейн-технологій може суттєво підвищити рівень довіри, прозорості та доказовості у функціонуванні державних інформаційних систем. Блокчейн, як технологія розподіленого реєстру, здатний забезпечити незмінність записів, незалежну верифікацію транзакцій і підтвердження достовірності дій користувачів без залучення посередників. Це відкриває нові можливості для формування прозорого журналювання подій, управління цифровими сертифікатами, аудиту та контролю доступу. Таким чином, блокчейн виступає не заміною існуючих механізмів КСЗІ, а додатковим рівнем технологічної довіри, який підсилює організаційні та криптографічні компоненти системи.

Запропонована в статті концептуальна модель інтеграції блокчейн-механізмів у структуру КСЗІ демонструє можливість поєднання трьох рівнів – організаційного, технічного та верифікаційного – у єдиний замкнений цикл безпеки. Така модель дозволяє реалізувати принцип «довіри через технологію», коли контроль і аудит дій користувачів забезпечуються не адміністративним, а криптографічно підтвердженим шляхом. Вона сприяє підвищенню стійкості систем до несанкціонованих змін, зниженню ризику людського фактора та спрощує міжвідомчий обмін достовірною інформацією.

Результати дослідження свідчать, що модернізація КСЗІ на основі ризик-орієнтованого управління та впровадження блокчейн-технологій створює передумови для побудови нової екосистеми кіберзахисту державних інформаційних ресурсів. Така екосистема характеризується високою прозорістю, доказовістю, гнучкістю та здатністю до самоперевірки. У перспективі вона може стати основою для реалізації принципів цифрової довіри, посилення національної кіберстійкості та формування цілісної культури інформаційної безпеки в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Balatska, V. S., & Opirskyy, I. R. (2023). Ensuring personal data confidentiality and cybersecurity through blockchain. *Cybersecurity: Education, Science, Technology, (4)(20),* 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. № 80/94-ВР. *Відомості Верховної Ради України.*
3. Закон України № 4336-IX від 27.03.2025 р. «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури». *Відомості Верховної Ради України,* 2025.
4. ДСТУ 3396.2-96. (1996). *Захист інформації. Технічний захист інформації. Терміни та визначення.* Київ: Держстандарт України.
5. ДСТУ ISO/IEC 27005:2019. (2019). *Інформаційні технології. Методи захисту. Керування ризиками інформаційної безпеки.* Київ: ДП «УкрНДНЦ».
6. ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* Geneva: ISO.
7. ISO/IEC 27701:2019. (2019). *Security techniques – Extension to ISO/IEC 27001 and 27002 for privacy information management – Requirements and guidelines.* Geneva: ISO.

8. NIST. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Gaithersburg: National Institute of Standards and Technology.
9. ENISA. (2020). *Risk management guidelines for the EU.* Athens: ENISA.
10. Національна стратегія у сфері кібербезпеки України на 2021–2025 роки. (2021). *Указ Президента України від 26.08.2021 № 447/2021.* Офіційний вісник Президента України.
11. Розпорядження Кабінету Міністрів України № 160-р від 07.03.2023 р. *Про затвердження плану заходів із реалізації Національної стратегії у сфері кібербезпеки України на 2023–2025 роки.* Київ, 2023.
12. Міністерство цифрової трансформації України. (2021). *Цифрова стратегія України – 2030*. Київ, 48 с.
13. OECD. (2018). *Blockchains unchained: Blockchain technology and its use in the public sector.* Paris: OECD.
14. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. Sebastopol, CA: O'Reilly Media.
15. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review, 2*, 6–19.
16. Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security & Privacy Workshops*, 180–184.
17. Androulaki, E., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the EuroSys Conference 2018.*
18. Finck, M. (2019). *Blockchain and the GDPR.* Brussels: European Parliamentary Research Service (EPRS).
19. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2), 92–100.
20. Балацька, В. С., & Опірський, І. Р. (2023). Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. *Кібербезпека: освіта, наука, техніка, 4*(20), 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
21. Balatska, V., Opirskyy, I., & Slobodian, N. (2024). Blockchain for enhancing transparency and trust in government registries. In *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024)* (pp. 50–59). Kyiv, Ukraine. https://ceur-ws.org/Vol-3826/
22. Балацька, В. С., & Дмитрів, Н. М. (2025). Міжорганізаційний обмін конфіденційними персональними даними на основі дозвільного блокчейну. *Кібербезпека: освіта, наука, техніка, 2*(29), 178–193. https://doi.org/10.28925/2663-4023.2025.29.875
23. Балацька, В. С., Побережник, В. О., Стефанків, А. В., & Шевчук, Ю. А. (2025). Розробка методу забезпечення достовірності та безпеки персональних даних у блокчейн-системах державних реєстрів. *Комп'ютерні системи та мережі, 7*(1), 1–16. https://doi.org/10.23939/csn2025.01.001

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

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

Rostyslav L. Tkachuk
Doctor of Technical Sciences, Professor,
Professor of the Department of Information Security Management,
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0001-9137-1891
lvtk@ukr.net

Nataliia O. Maslova
Candidate of Technical Sciences, Associate Professor,
Associate Professor of the Department of Information Security Management,
Lviv State University of Life Safety, Lviv, Ukraine
ORCID: 0000-0002-9078-0973
n.maslova@ldubgd.edu.ua

EVOLUTION OF INTEGRATED INFORMATION SECURITY SYSTEMS AND THE INTEGRATION OF BLOCKCHAIN TECHNOLOGIES IN THE CYBER PROTECTION OF STATE INFORMATION SYSTEMS OF UKRAINE

Abstract. The article examines the evolution of the concept of Integrated Information Security Systems (IISS) in the context of the digital transformation of the public sector, modernization of the national cybersecurity framework, and harmonization of Ukrainian legislation with international information security standards. The study reveals the relationship between classical approaches to building IISS—based on mandatory certification of technical protection complexes—and the modern paradigm of risk-oriented security management introduced by the new Law of Ukraine No. 4336-IX "On Amendments to Certain Laws of Ukraine on the Protection of Information and Cybersecurity of State Information Resources and Critical Information Infrastructure Objects." The research emphasizes the shift from a formal certification model to a process-oriented approach based on security profiles, risk management, continuous monitoring, and security auditing. Special attention is devoted to analyzing the potential of blockchain technologies in enhancing the resilience of state information systems against cyberattacks, insider threats, and unauthorized data modifications. The study substantiates the feasibility of using distributed ledgers to ensure the immutability, authenticity, transparency, and accountability of information processes. It is determined that blockchain can serve as an innovative component of the modern IISS architecture, complementing cryptographic protection mechanisms, access control, user activity auditing, and event monitoring. A conceptual model of blockchain integration into the traditional structure of IISS is proposed, forming a new trust ecosystem within state information resources. The combination of technological innovation with the legal requirements of Law No. 4336-IX creates a foundation for improving the effectiveness of the national cybersecurity system. The purpose of the study is to substantiate the scientific, methodological, and technological directions for the modernization of Ukraine's Integrated Information Security Systems through the integration of blockchain technologies in protecting state information resources in accordance with current legislation and international standards ISO/IEC 27001, ISO/IEC 27701, and GDPR.

Keywords: Integrated Information Security System (IISS); blockchain; cybersecurity; state information resources; critical information infrastructure; risk management; security profile; Law of Ukraine No. 4336-IX; distributed ledgers; data integrity; cryptographic protection; auditing; ISO/IEC 27001; ISO/IEC 27701; GDPR.

REFERENCES

1. Balatska, V. S., & Opirskyy, I. R. (2023). Ensuring personal data confidentiality and cybersecurity through blockchain. *Cybersecurity: Education, Science, Technology, (4)(20),* 6–19. https://doi.org/10.28925/2663-4023.2023.20.619
2. Zakon Ukrainy "Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh" vid 05.07.1994 r. № 80/94-VR. *Vidomosti Verkhovnoi Rady Ukrainy.*
3. Zakon Ukrainy № 4336-IX vid 27.03.2025 r. "Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury". *Vidomosti Verkhovnoi Rady Ukrainy*, 2025.
4. DSTU 3396.2-96. (1996). *Zakhyst informatsii. Tekhnichnyi zakhyst informatsii. Terminy ta vyznachennia* . Kyiv: Derzhstandart Ukrainy.
5. DSTU ISO/IEC 27005:2019. (2019). *Informatsiini tekhnolohii. Metody zakhystu. Keruvannia ryzykamy informatsiinoi bezpeky*. Kyiv: DP "UkrNDNC."
6. ISO/IEC 27001:2022. (2022). *Information security, cybersecurity and privacy protection – Information security management systems – Requirements.* Geneva: ISO.
7. ISO/IEC 27701:2019. (2019). *Security techniques – Extension to ISO/IEC 27001 and 27002 for privacy information management – Requirements and guidelines.* Geneva: ISO.
8. National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Gaithersburg, MD: NIST.
9. European Union Agency for Cybersecurity (ENISA). (2020). *Risk management guidelines for the European Union.* Athens: ENISA.
10. Natsionalna stratehiia u sferi kiberbezpeky Ukrainy na 2021–2025 rr. (2021). *Ukaz Presydenta Ukrainy vid 26.08.2021 r. № 447/2021.* Ofitsiinyi visnyk Presydenta Ukrainy.
11. Rozporiadzhennia Kabinetu Ministriv Ukrainy № 160-r vid 07.03.2023 r. *Pro zatverdzhennia planu zakhodiv iz realizatsii Natsionalnoi stratehii u sferi kiberbezpeky Ukrainy na 2023–2025 roky*. Kyiv, 2023.
12. Ministerstvo tsyfrovoi transformatsii Ukrainy. (2021). *Tsyfrova stratehiia Ukrainy–2030*. Kyiv, 48 p.
13. Organisation for Economic Co-operation and Development (OECD). (2018). *Blockchains unchained: Blockchain technology and its use in the public sector.* Paris: OECD.
14. Swan, M. (2015). *Blockchain: Blueprint for a new economy.* Sebastopol, CA: O'Reilly Media.
15. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond Bitcoin. *Applied Innovation Review, 2,* 6–19.
16. Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *IEEE Security & Privacy Workshops,* 180–184.
17. Androulaki, E., et al. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. *Proceedings of the EuroSys Conference 2018.*
18. Finck, M. (2019). *Blockchain and the GDPR.* Brussels: European Parliamentary Research Service (EPRS).
19. Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92–100.
20. Balatska, V., Opirskyy, I., & Slobodian, N. (2024). Blockchain for enhancing transparency and trust in government registries. In *Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2024)* (pp. 50–59). Kyiv, Ukraine. https://ceur-ws.org/Vol-3826/
21. Balatska, V. S., & Dmytriv, N. M. (2025). Inter-organizational exchange of confidential personal data based on permissioned blockchain. *Cybersecurity: Education, Science, Technology, 2*(29), 178–193. https://doi.org/10.28925/2663-4023.2025.29.875
22. Balatska, V. S., Poberezhnyk, V. O., Stefankiv, A. V., & Shevchuk, Y. A. (2025). Development of a method for ensuring the reliability and security of personal data in blockchain systems of state registers. *Computer Systems and Networks, 7*(1), 1–16. https://doi.org/10.23939/csn2025.01.001