УДК 004.056:355

В. С. Наконечний

В. В. Луценко

А. А. Побережний

ГІБРИДНІ АРХІТЕКТУРИ БЛОКЧЕЙНУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В СИСТЕМАХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У статті розглянуто моделі та методи захисту інформації у відомчих системах сектору безпеки і оборони України на основі технології блокчейн. Запропоновано концепцію гібридної архітектури блокчейну, що поєднує переваги публічних і приватних реєстрів для забезпечення балансу між відкритістю, конфіденційністю та продуктивністю системи. На основі математичного моделювання визначено залежності між кількістю вузлів, рівнем довіри, ймовірністю компрометації мережі та індексом стабільності системи. Розроблено математичну модель захисту даних, проведено порівняльний аналіз ефективності запропонованої моделі. Отримані результати доводять, що технологія блокчейн може використовуватися як комплексний механізм кіберзахисту інформаційних систем сектору безпеки і оборони України.

К л ю ч о в і с л о в а: гібридний блокчейн, захист інформації, контроль доступу, криптографічні механізми, консенсус RAFT, сектор безпеки і оборони України.

Постановка проблеми. Розвиток інформаційних технологій у секторі безпеки і оборони України, зокрема в Національній гвардії України, супроводжується різким зростанням обсягів службових, оперативних та аналітичних даних. Відомчі інформаційні системи забезпечують управління підрозділами, зв’язок, обмін розвідувальною інформацією та координацію дій у режимі реального часу [1].

Традиційні централізовані моделі зберігання даних створюють значні ризики: компрометація одного сервера може призвести до втрати цілісності або блокування великої кількості інформації. У контексті гібридних воєн та постійних кібератак проти України такі системи стають вразливими до несанкціонованого доступу та деструктивного впливу [2].

Сучасні підходи кіберзахисту – протоколи SSL/TLS, багаторівнева авторизація чи класичні корпоративні СУБД – залишаються недостатніми, оскільки покладаються на єдині точки контролю і не забезпечують гарантованої незмінності даних [3]. Це унеможливлює повноцінний прозорий аудит та швидке виявлення втручань в умовах динамічних і децентралізованих оперативних середовищ.

За таких умов одним із перспективних рішень є використання технології блокчейн, яка, завдяки децентралізованій природі, криптографічним механізмам і алгоритмам консенсусу, може забезпечити стійкість інформаційних систем до атак, прозорий аудит та захист даних без єдиного центру довіри [4].

Отже, дослідження, спрямовані на розроблення математичних моделей захисту інформації із застосуванням технології блокчейн для потреб сектору безпеки і оборони України, є вкрай актуальними.

Аналіз останніх досліджень і публікацій. Питання забезпечення кіберзахисту інформаційних систем сектору безпеки й оборони із застосуванням сучасних технологій, зокрема блокчейну, розглядаються у працях як вітчизняних, так і зарубіжних дослідників [4–8].

У цих працях висвітлюються аспекти стійкості кібероборони, проєктування захищених мереж, можливості використання блокчейну у військовій сфері та типові загрози для розподілених реєстрів.

У статті [4] основну увагу приділено забезпеченню стійкості кібероборони держави в умовах збройного конфлікту, зокрема організаційним та технічним заходам протидії кібератакам. Однак автор зосереджується переважно на загальному рівні кібероборони і не розглядає детально застосування гібридних блокчейн-архітектур у відомчих інформаційних системах, а також не пропонує формалізованих моделей довіри.

У статті [5] проаналізовано особливості проєктування захищених інформаційних систем, зокрема питання сегментації, побудови захищених каналів і організації доступу до ресурсів. Водночас

дослідження орієнтоване на класичні мережеві підходи і не враховує можливостей використання блокчейн-платформ як базового елемента інформаційної системи. Крім того, у праці не розглядаються питання інтеграції криптографічних механізмів, смарт-контрактів та моделей довіри в умовах міжвідомчих взаємодій сектору безпеки і оборони.

Автори публікації [6] розглядають застосування блокчейну у військовій сфері, зокрема для управління ресурсами, логістикою та підвищення прозорості процесів. Проте запропоновані підходи мають здебільшого оглядовий характер і не містять детального математичного моделювання стійкості мережі, оцінювання ймовірності компрометації вузлів або аналізу впливу вибору консенсусного алгоритму (наприклад, RAFT) на показники безпеки й продуктивності в умовах відомчих систем.

У дослідженні [7] блокчейн розглядається як засіб вирішення проблем інформаційної безпеки та конфіденційності даних. Автор систематизує основні переваги технології для захисту інформації в різних галузях. Однак дослідження не орієнтоване на специфіку сектору безпеки і оборони, не пропонує математичну модель системи захисту даних, адаптовану до багаторівневих структур військових та правоохоронних органів.

У статті [8] подано огляд ключових проблем безпеки блокчейн-систем, зокрема атак на консенсус, вразливостей смарт-контрактів та загроз цілісності розподілених реєстрів. Хоча автори формують цінну класифікацію загроз, запропоновані підходи залишаються загальними й не враховують особливостей гібридних (публічно-приватних) архітектур, а також не описують механізмів побудови моделі довіри й оцінювання поведінкових характеристик вузлів у відомчих інформаційних системах.

У праці [9] здійснено ґрунтовний огляд архітектури блокчейну, консенсусних механізмів та базових підходів до забезпечення безпеки. Разом із тим автори зосереджуються на класифікації рішень і не пропонують інтегральних показників стійкості системи, які б одночасно враховували кількість вузлів, ризик їх компрометації, затримки транзакцій та енергоспоживання. Також не розглянуто питання відповідності блокчейн-рішень вимогам міжнародних стандартів кібербезпеки у контексті оборонних інформаційних систем.

У статті [10] проаналізовано перспективи використання технології блокчейн у сфері захисту інформації для потреб сектору безпеки і оборони України. Автори окреслюють можливі сценарії впровадження та переваги децентралізованих реєстрів для відомчих систем. Водночас робота має переважно концептуальний характер: не подано формалізованих математичних моделей оцінювання стійкості, не розглянуто механізми побудови гібридних архітектур (із поєднанням публічних і приватних реєстрів), а також відсутній кількісний аналіз впливу параметрів консенсусу і рівня довіри між вузлами на загальний рівень захищеності.

Незважаючи на наявність публікацій за даним напрямом, у жодній з відомих праць не розглядається постановка та виконання завдання щодо створення гібридних архітектур блокчейну для забезпечення захисту інформації в системах сектору безпеки і оборони України

Метою статті є розроблення гібридного блокчейн-рішення для забезпечення захисту службових і оперативних даних у відомчих інформаційних системах сектору безпеки і оборони України, зокрема у Національній гвардії України.

Відповідно до поставленої мети сформульовано такі завдання дослідження.

1. Розробити математичну модель системи захисту даних у децентралізованій інформаційній системі, що враховує рівень довіри між вузлами, ризики їх компрометації та параметри криптографічного захисту.
2. Сформувати модель довіри та консенсусу користувачів, орієнтовану на забезпечення цілісності та незмінності даних у розподілених інформаційних системах.
3. Провести імітаційне та експериментальне моделювання середовища гібридної блокчейн-архітектури, а також провести його з різною кількістю вузлів для оцінювання продуктивності, затримки транзакцій, енергоспоживання й стійкості до атак.

Виклад основного матеріалу

Математична модель системи захисту даних. На відміну від підходів, описаних у працях [5, 6], які зосереджуються переважно на загальних принципах застосування блокчейну у відомчих інформаційних системах і не враховують специфіки довірчих взаємодій, оцінки ризику компрометації вузлів та адаптивного контролю доступу, запропонована у статті математична модель спрямована на забезпечення незмінності записів, децентралізованої автентифікації та динамічної політики доступу у міжвідомчих інформаційних системах сектору безпеки і оборони.

Для опису процесів захисту службових та операційних даних у відомчих інформаційних системах використаємо множину $D = \{d_1, d_2, \dots, d_n\}$, що представляє об'єкти даних, які потребують шифрування та контролю доступу. Нехай $U = \{u_1, u_2, \dots, u_n\}$ – множина користувачів або вузлів системи, кожен з яких має власний набір прав $A(ui) \subseteq \{r, w, x\}$, де r – право читання даних, w – право на запис або модифікація, x – право на виконання або ініціація операцій у системі.

Для опису процесів шифрування, хешування та фіксації транзакцій у блокчейні введемо функцію, яка визначає результат перетворення даних перед їх включенням до блокчейну. Функцію формалізуємо таким чином:

$$F(D, K, T) = H(E(D, K), T), \tag{1}$$

де $E(D, K)$ – функція симетричного шифрування даних з набором ключів
$K = \{k_1, k_2, \dots, k_n\}$;
$H(T)$ – хеш-функція, що враховує часову позначку транзакції T.

Кожен новий блок формується як

$$Bj = \langle H_{j-1}, F(D_j, K_j, T_j), S_{igj}, PK_j \rangle, \tag{2}$$

де H_{j-1} – хеш попереднього блоку;
S_{igj} – цифровий підпис учасника транзакції (вузла, користувача або сервісу);
PK_j – його відкритий ключ.

Така структура блоку унеможливлює фальсифікацію або непомітну модифікацію службових записів, що особливо важливо у розподілених інформаційних системах командного управління та зв'язку, де достовірність даних є критичною для прийняття рішень.

Для формального оцінювання захисту пропонується ввести інтегральний показник рівня безпеки S_{sec}, який враховує ризики компрометації вузла, криптографічну складність та якість механізму консенсусу.

Загальна формула має такий вигляд:

$$S_{sec} = \alpha \left(1 - \prod_{i=1}^{N} (1 - p_i)\right) + \beta \frac{\log_2(C_{hash})}{E_{comp}} + \gamma \frac{R_{cons}}{T_{lat}}, \tag{3}$$

де p_i – ймовірність зламу вузла i;
C_{hash} – криптографічна складність обчислення колізії хеша (наприклад, 2 128 для SHA-256);
E_{comp} – середні витрати енергії на операцію перевірки;
R_{cons} – коефіцієнт надійності консенсусного алгоритму;
T_{lat} – середня затримка транзакції;
α, β, γ – вагові коефіцієнти, що відображають пріоритет параметрів безпеки;
N – загальна кількість вузлів, що враховуються у оцінюванні стійкості системи.

Вагові коефіцієнти α, β, γ визначаються залежно від пріоритетності окремих аспектів безпеки для конкретної інформаційної системи. Їх значення встановлюються шляхом нормування експертних оцінок або параметричної оптимізації, що враховує вимоги до рівня стійкості системи, допустимі затримки транзакцій та обмеження на енергоспоживання. Зазвичай значення коефіцієнтів вибирають так, щоб кожен з параметрів відображав критичність відповідного компонента для цільового застосування, наприклад, для військових систем пріоритет зміщується у бік мінімізації ризику компрометації вузлів.

Коефіцієнт надійності консенсусного алгоритму R_{cons} визначається через імовірність успішного підтвердження транзакції за умови наявності недобросовісних або скомпрометованих вузлів. Для цього враховуються параметри алгоритму консенсусу, як-от: допуск до кількості відмов, модель довіри та ймовірність того, що мережа зберігає працездатність за наявності атак.

Цей показник дозволяє порівнювати різні реалізації блокчейн-систем за рівнем їхньої стійкості до атак та оптимізувати архітектуру з погляду на співвідношення безпеки та продуктивності.

Модель довіри та консенсусу користувачів. У відомчих інформаційних системах сектору безпеки і оборони, де відсутній єдиний центр контролю, надзвичайно важливим є механізм взаємної перевірки достовірності дій вузлів.

Для формалізації цього процесу застосовано модель довіри, яка базується на оцінюванні історії взаємодій, цифрових підписів і поведінкових показників вузлів. Рівень довіри для кожного вузла визначається за такою формулою:

$$Trust(u_i) = \frac{\delta_1 C_i + \delta_2 V_i + \delta_3 U_i}{\delta_1 + \delta_2 + \delta_3}, \quad (4)$$

де C_i – кількість підтверджених операцій без порушень політик безпеки;

V_i – успішність перевірок з боку інших вузлів;

U_i – показник активності у мережі;

$\delta_1, \delta_2, \delta_3$ – вагові коефіцієнти, що визначають важливість відповідних параметрів під час оцінювання довіри.

Значення вагових коефіцієнтів задаються шляхом експертного оцінювання або калібрування моделі довіри на основі експериментальних даних. Зазвичай їх нормують таким чином, щоб вони відображали відносну важливість кожного чинника для конкретного середовища.

На основі рівня довіри до вузлів (4) визначається загальний рівень довіри до системи:

$$T_{avg} = \frac{1}{N} \sum_{i=1}^{N} Trust(u_i), \quad (5)$$

а консенсус вважається досягнутим, якщо

$$T_{avg} \geq T_{crit}, \quad (6)$$

де T_{crit} – порогове значення (зазвичай 0,7–0,8).

Імітаційне та експериментальне моделювання. Для оцінювання ефективності запропонованої математичної моделі системи захисту даних було проведене імітаційне моделювання у середовищі Python із використанням Hyperledger Fabric SDK. У експериментах змодельовано обмін даними між різними відомчими вузлами, які представляли окремі елементи інформаційних систем сектору безпеки і оборони України.

Тестування проводилося для 10, 20, 50 та 100 вузлів. Результати показали підвищення рівня безпеки на 22 % зі зростанням кількості вузлів до 100, при цьому середня затримка транзакції становила близько 410 мс (рис. 1).

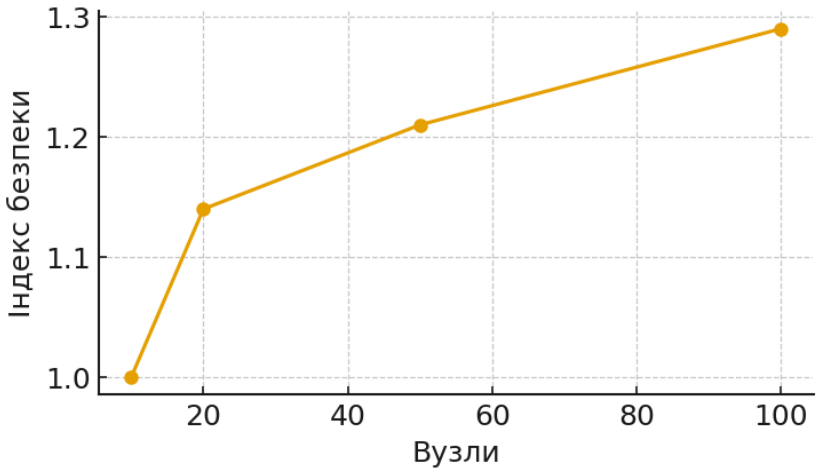

Рисунок 1 – Покращення безпеки залежно від кількості вузлів (базовий рівень: 10 вузлів=1,00)

Моделювання показало, що запропонована математична модель на основі консенсусу RAFT забезпечує значно нижчі обчислювальні витрати, порівнюючи з енергозатратними механізмами типу Proof-of-Work, та демонструє зменшення енергоспоживання на 37 %.

Хоча сучасні алгоритми DPoS та BFT характеризуються ще нижчим енергоспоживанням, їх використання у відомчих системах є обмеженим через залежність від делегованих валідаторів DPoS, низьку масштабованість та високі комунікаційні накладні витрати при збільшенні числа вузлів BFT.

Розроблена математична модель узгоджується з міжнародними та національними вимогами до захисту інформації у секторі безпеки і оборони. Вона відповідає принципам стандартів ISO/IEC 27001:2022 (управління інформаційною безпекою), NIST SP 800-207 (Zero Trust Architecture) та положенням Закону України «Про національну безпеку України» щодо розвитку спроможностей у сфері кібероборони.

Система реалізує контроль доступу на основі ролей (RBAC) і контекстних політик безпеки, а також забезпечує незмінність та аудит усіх транзакцій у розподіленому реєстрі, що робить її сумісною з концепціями «Zero Trust» та «Secure by Design».

Для практичного підтвердження працездатності запропонованої математичної моделі було створене експериментальне середовище на базі приватної блокчейн-мережі Hyperledger Fabric 2.5, розгорнутої у віртуалізованій інфраструктурі Docker. Система включала три вузли організації, які виконували роль валідаторів транзакцій, та один вузол клієнта, який ініціював операції доступу до даних.

Для шифрування даних використовувався алгоритм AES-256 у режимі GCM, що забезпечує автентифікацію повідомлень.

Архітектура математичної моделі передбачає, що перед завантаженням файлу користувач здійснює цифровий підпис даних і виконує локальне шифрування. До блокчейну передаються лише хеш файлу та супровідні метадані: ідентифікатор власника, позначка часу та посилання на політику доступу. Самі правила доступу визначаються у смарт-контракті, який не зберігає дані, а відстежує виконання встановлених умов та автоматично перевіряє, чи має користувач достатні права для обробки запиту. Під час кожної операції система звіряє цифровий підпис та рівень доступу користувача з політиками, визначеними у смарт-контракті.

Взаємодія між користувачем та блокчейном здійснюється через REST API, що забезпечує сумісність із зовнішніми додатками.

У процесі тестування було перевірено стійкість математичної моделі до несанкціонованого доступу, модифікації даних та атак повторного відтворення. За результатами тестування система забезпечила 100 % виявлення спроб зміни або повторного використання токенів автентифікації.

Для об’єктивного оцінювання ефективності запропонованої математичної моделі системи захисту даних був проведений порівняльний аналіз з існуючими підходами до захисту даних, що використовують централізовану архітектуру. В аналізі враховувалися такі критерії: надійність зберігання, захист від змін даних, масштабованість, продуктивність та енергоспоживання.

Централізовані системи (класичні СУБД або корпоративні сервери) показали високу швидкість обробки транзакцій, але низьку стійкість до збоїв та кібератак. Блокчейн-рішення, навпаки, мають дещо вищу затримку, але забезпечують значно вищу цілісність даних та прозорість усіх дій користувача. Експериментальні вимірювання показали, що зі збільшенням кількості вузлів з 10 до 100 загальний рівень безпеки збільшився на 21 %, тоді як середній час транзакції збільшився лише на 0,3 с.

Це свідчить про задовільний компроміс між безпекою та продуктивністю системи. Порівняно з іншими платформами (Ethereum, Quorum, Multichain), Hyperledger Fabric продемонстрував найвищу ефективність у корпоративних сценаріях завдяки використанню консенсусного алгоритму RAFT та гнучкої системи політик доступу. Аналіз також показав, що децентралізовані системи забезпечують краще дотримання міжнародних вимог до безпеки персональних даних.

Наприклад, у контексті GDPR блокчейн гарантує відстежуваність усіх операцій та можливість проведення аудитів, а також спрощує реалізацію механізмів «права бути забутим», зберігаючи лише хеші даних, а не самі файли.

У сукупності ці результати підтверджують, що запропонована технологія блокчейн забезпечує баланс між безпекою, швидкістю та відповідністю нормативним вимогам і придатна для використання у великих організаціях, де важливо підтримувати високий рівень надійності без значних втрат продуктивності.

Висновки

1. У статті запропоновано математичну модель системи захисту даних на основі технології блокчейн, що поєднує криптографічні механізми, алгоритми консенсусу RAFT та децентралізоване управління довірою. Для конфігурацій з 0, 20, 50 та 100 вузлами обчислено інтегральний показник S_{sec} і середній рівень довіри T_{avg}, що продемонструвало зростання S_{sec} на 20–22 % порівняно з базовою конфігурацією N=10.

2. Розроблена модель довіри та консенсусу користувачів, яка кількісно описує залежність стійкості системи від кількості вузлів і рівня довіри між ними. Результати моделювання засвідчили, що при зростанні кількості вузлів з 10 до 100 та підтриманні середнього рівня довіри $T_{avg} \geq 0{,}8$ інтегральний показник стійкості мережі підвищується з 1,00 до 1,22, що вказує на зменшення впливу компрометації окремих вузлів.

3. Проведене імітаційне та експериментальне моделювання середовища гібридної блокчейн-архітектури з прототипом на базі Hyperledger Fabric 2.5 з консенсусом RAFT показало, що запропонований підхід забезпечує суттєве підвищення захищеності: середня затримка транзакції для N=100 вузлів становила близько 410 мс (зростання часу обробки лише приблизно на 0,3 с порівняно з централізованою системою), енергоспоживання зменшилося на 37 %, система забезпечила 100 % виявлення спроб модифікації даних та атак повторного відтворення токенів, перевищуючи традиційні рішення за рівнем безпеки.

Теоретичне значення праці полягає у формалізації математичних залежностей між кількістю вузлів, імовірністю їх компрометації та загальним рівнем довіри у мережі. Отримані результати можуть бути використані для подальшого розвитку методів оцінювання стійкості та надійності блокчейн-архітектур у критично важливих системах.

Практичне значення полягає у створенні функціонального прототипу гібридної блокчейн-системи, яка забезпечує прозорість дій користувачів, адаптивний контроль доступу та стійкість до кібератак. Запропонована математична модель системи захисту даних є перспективною для впровадження в інформаційних системах, що працюють з конфіденційними або критичними даними.

Напрямами подальших досліджень є розвиток інтелектуальних механізмів моніторингу й прогнозування загроз на основі машинного навчання, удосконалення енергоефективності консенсусних протоколів, а також дослідження інтеграції блокчейн-технологій із квантово-стійкими алгоритмами шифрування. У перспективі така архітектура може стати базовою для побудови єдиної довіреної інформаційної системи сектору безпеки і оборони України.

Перелік джерел посилання

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL:https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.11.2025).

2. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право.* Київ, 2016. № 3/4 (31/32). С. 117–124. DOI:10.20535/2308-5053.2016.3/4(31/32). URL:https://visnyk-psp.kpi.ua/article/view/140496 (дата звернення: 12.11.2025).

3. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 р. № 447/2021. URL:https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 12.11.2025).

4. Савченко В. А. Забезпечення стійкості кібероборони держави в умовах збройного конфлікту. *Сучасний захист інформації*. 2023. № 3 (55). С. 6–11. DOI: 10.31673/2409-7292.2023.030001.

5. Особливості проєктування захищених інформаційних мереж / В. Хорошко та ін. *Science-based technologies*. 2024. № 62. С. 154–163. DOI:10.18372/2310-5461.62.18709.

6. Blockchain Applications in the Military Domain: A Systematic Review / Kostopoulos N. et al. *Technologies*. 2025. Vol. 13. No. 1. Pp. 30–38. DOI:https://doi.org/10.3390/technologies13010023.

7. Ndung'u R. N. Blockchain as a Solution of Information Security and Data Privacy Issues: Review. *International Journal of Computer Applications Technology and Research.* 2022. Vol. 11. No. 8. Pp. 337–340. DOI:10.7753/IJCATR1108.1007.

8. Lin I. C., Liao T. C. A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*. 2017. Vol. 19. No. 5. Pp. 653–659. DOI:10.6633/IJNS.201709.19(5).01.

9. An Overview of Blockchain Technology: Architecture, Consensus and Security / Z. Zheng et al. *IEEE International Congress on Big Data*. 2017. Pp. 557–564. DOI:10.1109/BigDataCongress.2017.85.
10. Перспективи використання технології блокчейн у сфері захисту інформації для потреб сектора безпеки і оборони / Куцаєв П. В., Данилюк І. А., Паламарчук С. А., Чередниченко О. Ю. *Системи і технології зв'язку, інформатизації та кібербезпеки*. 2024. Вип. 6. С. 93–104. DOI:10.58254/viti.6.2024.07.93.

Стаття надійшла до редакції 16.11.2025 р.

UDC 004.056:355

V. Nakonechnyi, V. Lutsenko, A. Poberezhnyi

HYBRID BLOCKCHAIN ARCHITECTURES FOR ENSURING INFORMATION PROTECTION IN SECURITY AND DEFENSE SECTOR SYSTEMS OF UKRAINE

The article studies models and methods of information protection in departmental systems of the security and defense sector of Ukraine based on blockchain technology. The concept of a hybrid blockchain architecture is proposed, which combines the advantages of public and private registries to ensure a balance between openness, confidentiality and system performance. Based on mathematical modeling, the dependencies between the number of nodes, the level of trust, the probability of network compromise and the system stability index are determined. A mathematical model of the data protection system in a decentralized information system is developed, which takes into account the level of trust between nodes, the risks of their compromise and the parameters of cryptographic protection. A block structure is proposed that makes it impossible to falsify or imperceptibly modify service records, which is especially important in distributed command and control and communication information systems, where data reliability is critical for decision-making. A model of user trust and consensus is formed to ensure the integrity and immutability of data in distributed information systems. Simulation and experimental modeling of a hybrid blockchain architecture environment with different numbers of nodes was conducted to evaluate performance, transaction latency, power consumption, and attack resistance. Comparative analysis of the proposed model and traditional centralized protection systems showed a 20–25% improvement in data security without significant performance loss. The results demonstrate that blockchain technology can serve as a comprehensive cybersecurity mechanism for information systems in the security and defense sector of Ukraine, ensuring trust, transparency, and resilience to cyberattacks.

K e y w o r d s: hybrid blockchain, information protection, access control, cryptographic mechanisms, RAFT consensus, security and defense sector of Ukraine.

Наконечний Володимир Сергійович – доктор технічних наук, професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
https://orcid.org/0000-0002-0247-5400

Луценко Владислав Володимирович – аспірант кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка.
https://orcid.org/0000-0002-2377-1858

Побережний Андрій Анатолійович – науковий співробітник науково-дослідної лабораторії службово-бойового застосування Національної гвардії України Національної академії Національної гвардії України.
https://orcid.org/0000-0002-8984-6912