

ЯРИМОВИЧ ЮРІЙ

Національний університет «Львівська політехніка»

<https://orcid.org/0009-0006-1391-3214>email: yuyarym@gmail.com**КУНАНЕЦЬ НАТАЛІЯ**

Національний університет «Львівська політехніка»

<https://orcid.org/0000-0003-3007-2462>e-mail: nek.lviv@gmail.com

МЕТОДИ ТА ЗАСОБИ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОГО СУПРОВОДУ ПРОЦЕСІВ ОБЛІКУ ТОРГІВЛІ ВОГНЕПАЛЬНОЮ ЗБРОЄЮ

У статті проаналізовано сучасні методи та засоби інформаційно-технологічного супроводу процесів обліку торгівлі вогнепальною зброєю, що є важливою складовою державного контролю та безпеки. Особливу увагу приділено питанням автоматизації обліку, цифрової ідентифікації, відстеження руху зброї та забезпечення прозорості операцій між державними структурами й приватними учасниками ринку. Проаналізовано можливості впровадження блокчейн-технологій (зокрема Hyperledger Fabric) для забезпечення надійності та незмінності транзакцій. Розглянуто застосування графових баз даних (Neo4j, GraphDB) для моделювання складних взаємозв'язків між об'єктами обліку. Окреслено перспективи використання IoT-пристроїв, біометричних систем, методів машинного навчання для виявлення аномалій і прогнозування ризиків, а також застосування методу аналізу ієрархій (MAI) для формалізованої підтримки прийняття рішень щодо вибору технічних рішень, оцінки ризиків та визначення пріоритетів розвитку інформаційної інфраструктури в умовах обмежених ресурсів.

Ключові слова: інформаційні технології, облік зброї, RFID, блокчейн, аномалії, інтелектуальний аналіз, інформаційна безпека

YARIMOVYCH YURIY, KUNANETS NATALIYA

Lviv Polytechnic National University

METHODS AND TOOLS OF INFORMATION AND TECHNOLOGICAL SUPPORT FOR THE PROCESSES OF FIREARMS TRADE ACCOUNTING

Biometric scanners are an important element of modern security systems that provide personalized identification of persons who have access to weapons, including sellers, buyers and inspectors. Their use prevents unauthorized access, ensures that the actions of each user are recorded, and increases the level of responsibility for operations with weapons. The most common are fingerprint scanners, which provide quick and accurate identification. Face scanners are also used, which allow contactless recognition of the user, and iris scanners, which are used in conditions of increased security requirements. The article examines modern methods and tools for information and technological support of firearm trade accounting processes, which are a critical component of state control and security. Particular attention is paid to the issues of automation, digital identification, tracking of weapon movement, and ensuring transparency of operations between governmental bodies and private market participants. The potential of implementing blockchain technologies (in particular, Hyperledger Fabric) is analyzed to ensure the reliability and immutability of transactions. The use of graph databases (Neo4j, GraphDB) is considered for modeling complex relationships between accounting entities. Prospects for applying IoT devices, biometric systems, and machine learning methods are outlined to detect anomalies and predict risks. Additionally, the article highlights the use of the Analytic Hierarchy Process (AHP) for formalized decision-making support in selecting technical solutions, assessing risks, and setting development priorities for the information infrastructure under conditions of limited resources.

Keywords: information technologies, weapons accounting, RFID, blockchain, anomalies, intelligent analysis, information security.

Стаття надійшла до редакції / Received 26.05.2025

Прийнята до друку / Accepted 26.06.2025

Постановка проблеми

Проблематика обліку торгівлі вогнепальною зброєю набуває особливої ваги в умовах загроз безпеці, зростання нелегального обігу та транснаціональної злочинності. Ефективний контроль за обігом зброї є необхідною складовою національної та міжнародної безпеки, що вимагає надійних інформаційно-технологічних засобів для забезпечення прозорості, достовірності та оперативності облікових процесів.

Застарілі моделі ведення обліку, що базуються на паперових документах або фрагментарних цифрових системах, не забезпечують належного рівня верифікації, захисту та аналітики. У цьому контексті використання RFID-ідентифікації, розподілених реєстрів (блокчейн), систем виявлення аномалій на базі машинного навчання, а також захищених баз даних створює передумови для якісно нового рівня моніторингу та управління процесами торгівлі зброєю.

Актуальність теми посилюється також глобальними ініціативами, такими як Протокол ООН щодо стримування незаконної торгівлі стрілецькою зброєю, а також національними реформами у сфері цифровізації безпекових структур. Упровадження сучасних ІТ-рішень дає змогу не лише підвищити ефективність державного контролю, а й забезпечити прозору взаємодію між виробниками, дилерами, державними органами та споживачами на основі єдиних стандартів і відкритих протоколів.

Аналіз досліджень та публікацій

Супровід торгівлі вогнепальною зброєю традиційно базувався на централізованих системах обліку, де обмін інформацією між суб'єктами здійснювався через офіційні державні бази даних, з використанням документованих дозволів, ліцензій і сертифікатів. Однак такі системи часто страждають від низької прозорості, вразливості до маніпуляцій, затримок у передачі даних і труднощів в аудиторській перевірці.

У зв'язку з цим дедалі більше уваги привертають децентралізовані технології, зокрема блокчейн, які забезпечують незмінність, верифікацію та доступність транзакцій для авторизованих учасників. Блокчейн дає змогу створити надійний реєстр переміщення зброї – від виробника до кінцевого користувача – із фіксацією кожної транзакції, що дозволяє забезпечити відстеження та спростити контроль за дотриманням ліцензійних умов. У багатьох роботах аналізуються переваги використання блокчейну у сфері торгівлі зброєю. Відзначається, що транзакції не можуть бути змінені або видалені, що створює умови для довіри [1]. Дослідники визначили, що якщо пріоритетами системи є побудова довіри, надійності та збереження даних, то блокчейн є кращим рішенням щодо конфіденційності. За допомогою permissioned blockchain (доступного лише певним учасникам) можна забезпечити повну видимість ланцюга постачання без розкриття конфіденційної інформації [2]. Smart-контракти дозволяють реалізовувати автоматизовану перевірку дотримання умов угоди, наприклад, наявності ліцензії на конкретний тип зброї [3].

Розподілена архітектура на думку дослідників [4] зменшує ризики саботажу, збоїв або фальсифікацій даних [5], кібератак [6,7], що характерні для централізованих систем.

У статтях аналізуються особливості застосування RFID-міток та зчитувачів, що дозволяють контролювати переміщення, інвентаризацію та відповідність ліцензії у режимі реального часу [8,9]. Серед практичних прикладів реалізації таких рішень можна виділити пілотні проекти зі створення блокчейн-реєстрів зброї в межах міжнародного співробітництва (наприклад, проекти на базі Hyperledger Fabric для обміну інформацією між митними службами) [10]. Такі рішення дозволяють об'єднати державні, приватні та міжнародні бази даних в уніфіковану екосистему для контролю обігу зброї.

Також блокчейн може ефективно взаємодіяти з іншими технологіями супроводу фізичного відстеження переміщення одиниць зброї, або біометричними засобами ідентифікації при продажу/використанні зброї. Таким чином, блокчейн не лише вирішує технічні проблеми надійного обліку, але й створює нові парадигми довіри у відносинах між усіма учасниками процесу торгівлі зброєю – від виробника до наглядових органів.

Формулювання цілей статті

Мета статті дослідити, обґрунтувати та систематизувати сучасні методи й засоби інформаційно-технологічного супроводу процесів обліку торгівлі вогнепальною зброєю, зокрема з урахуванням використання технологій блокчейн, RFID, IoT, а також методів підтримки прийняття рішень, зокрема методу аналізу ієрархій, з метою підвищення прозорості, безпеки та ефективності інформаційних систем у цій сфері.

Виклад основного матеріалу

Інформаційно-технологічний супровід обліку торгівлі вогнепальною зброєю вимагає використання надійних технічних засобів і платформ, які забезпечують автоматизований збір, зберігання, опрацювання та контроль даних у реальному часі. З огляду на особливу чутливість об'єкта контролю, такі системи повинні відповідати високим вимогам до безпеки, масштабованості, прозорості та відповідності міжнародним нормативам.

Апаратні засоби

При побудові системи обліку продажу зброєю інтегруємо різні апаратні компоненти. Використання RFID-міток та зчитувачів у поєднанні з блокчейн-технологією забезпечує ефективний, безпечний та прозорий облік продажу вогнепальної зброї. RFID-мітки, закріплені на кожній одиниці зброї, містять унікальні ідентифікатори, що дозволяють здійснювати точну ідентифікацію, відстеження та облік зброї на всіх етапах її життєвого циклу – від виробництва до кінцевого користувача. Зчитувачі RFID встановлюються у виробничих цехах, на складах, у торгових точках, а також у митних і правоохоронних органах, що забезпечує можливість оперативного зчитування інформації без фізичного контакту. Дані, отримані через RFID-зчитувачі, автоматично фіксуються в блокчейн-мережі, де кожна транзакція набуває незмінного характеру, гарантується її достовірність та захищеність від фальсифікації. Блокчейн дозволяє прозоро відображати історію володіння кожною одиницею зброї, а смарт-контракти можуть автоматично перевіряти відповідність ліцензій та дозвільних документів під час здійснення транзакцій. Така інтегрована система значно підвищує рівень контролю над легальним обігом зброї, мінімізує ризики її нелегального використання та забезпечує державні структури необхідними інструментами для ефективного нагляду. Поєднання RFID та блокчейну сприяє автоматизації облікових процесів, зменшенню людського фактора і дозволяє оперативно здійснювати аудит дій усіх учасників системи.

У випадках, коли використання RFID-інфраструктури є технічно або економічно недоцільним, альтернативним засобом маркування зброї можуть виступати двовимірні штрихкоди, зокрема QR-коди та Datamatrix-коди. Ці технології забезпечують базову функціональність для ідентифікації та обліку об'єктів, зокрема у сфері контролю за обігом вогнепальної зброї.

QR-коди та Datamatrix-коди — це двовимірні графічні коди, здатні вміщувати значний обсяг даних порівняно зі звичайними лінійними штрихкодами. Вони наносяться на поверхню зброї або на прикріплені бирки і можуть містити інформацію про ідентифікаційний номер зброї, дату виробництва, серійний номер, дані про виробника та інші метадані. Основною перевагою цих кодів є їхня доступність і простота впровадження, оскільки для їх створення не потрібна складна апаратура, а зчитування можливе за допомогою звичайних оптичних сканерів або камер мобільних пристроїв.

QR-коди мають кращу зчитуваність на відстані, особливо при використанні візуальних пристроїв загального призначення, таких як смартфони, однак є більшими за розміром, ніж Datamatrix, що обмежує їх застосування на дрібних або вигнутих поверхнях. Datamatrix-коди, у свою чергу, компактніші, дозволяють нанесення навіть на дуже обмежені площі, наприклад, на металеві частини зброї, і часто використовуються в промисловості, де потрібне лазерне або ударне маркування.

Обидва типи кодів мають вбудовані механізми корекції помилок, що дозволяє частково зчитувати інформацію навіть у разі пошкодження коду. Водночас, на відміну від RFID, ці технології є лінійними. Зчитування можливе лише при прямій видимості та з достатньою якістю поверхні, що обмежує їхню ефективність в умовах високої швидкості обліку або великого потоку об'єктів.

Також варто відзначити, що ці коди не мають функціональності бездротового зчитування і не здатні працювати в режимі реального часу без участі оператора або відповідного технічного обладнання. Проте при інтеграції з блокчейн-системою вони можуть забезпечувати незмінність записів про транзакції, якщо після кожного сканування дані фіксуються в реєстрі за допомогою смарт-контрактів.

Узагальнюючи, QR/Datamatrix-коди є ефективною, економічно доцільною альтернативою RFID при відсутності відповідної інфраструктури, забезпечують базову ідентифікацію та простежуваність, але поступаються RFID за швидкістю, автоматизованістю та функціональністю безконтактного обліку.

Біометричні сканери є важливим елементом сучасних систем безпеки, що забезпечують персоналізовану ідентифікацію осіб, які мають доступ до зброї, зокрема продавців, покупців та інспекторів. Їх застосування дозволяє запобігти несанкціонованому доступу, забезпечити фіксацію дій кожного користувача та підвищити рівень відповідальності за операції із зброєю. Найпоширенішими є сканери відбитків пальців, які забезпечують швидку і точну ідентифікацію. Також використовуються сканери обличчя, що дозволяють безконтактно розпізнавати користувача, та сканери райдужної оболонки ока, які застосовуються в умовах підвищених вимог до безпеки. У деяких випадках впроваджуються гібридні системи, що поєднують кілька біометричних ознак для підвищення точності автентифікації. Завдяки унікальності біометричних характеристик ідентифікація є надійною і стійкою до підробки або несанкціонованої передачі прав доступу. Біометричні сканери інтегруються з інформаційними системами, зокрема з блокчейн-реєстрами, де всі дії фіксуються у незмінному цифровому журналі, що забезпечує прозорість і контрольованість процесів. Їх використання підвищує довіру до системи обігу зброї, сприяє дотриманню нормативних вимог та допомагає у розслідуванні інцидентів, пов'язаних з використанням вогнепальної зброї. Таким чином, біометричні сканери забезпечують високий рівень персоналізованого контролю, сприяючи безпеці та ефективному управлінню обігом зброї.

IoT-пристрої, зокрема давачі відкриття сейфів, сенсори переміщення, температурні давачі та інші типи інтелектуальних сенсорів, відіграють важливу роль у системах обліку та контролю зберігання і транспортування зброї. Вони забезпечують безперервний моніторинг фізичних умов, оперативно фіксують події та передають дані до централізованої інформаційної системи в реальному часі. Наприклад, давачі відкриття сейфів дозволяють зафіксувати факт та точний час відкриття збройового сховища, а також особу, яка ініціювала доступ, якщо система інтегрована з біометричними або RFID-ідентифікаторами. Сенсори переміщення забезпечують виявлення несанкціонованих переміщень зброї або тари зі зброєю, що критично важливо під час транспортування або охорони об'єктів. Температурні сенсори контролюють дотримання допустимих умов зберігання, що особливо важливо для запобігання псуванню боєприпасів або виникненню аварійних ситуацій. Усі IoT-пристрої можуть бути підключені до єдиної платформи моніторингу, яка не лише накопичує дані, а й здатна генерувати автоматичні сповіщення, запускати тривоги чи активувати протоколи безпеки у випадку порушень. Крім того, завдяки інтеграції з блокчейн-реєстрами, події, зафіксовані IoT-пристроями, можуть зберігатися у незмінному вигляді для подальшого аудиту або розслідування. Таким чином, застосування IoT-технологій значно підвищує рівень прозорості, оперативності та безпеки при зберіганні і транспортуванні зброї, створюючи цифровий простір, де кожна подія документується, контролюється і може бути перевірена.

Поєднання RFID-міток, QR/Datamatrix-кодів, біометричних сканерів і IoT-пристроїв у єдину інформаційну систему обліку продажу зброї можна подати у вигляді формального подання як інтегрованої кіберфізичної системи.

Програмні платформи

В основі інформаційно-технологічного супроводу лежать спеціалізовані платформи, які підтримують облік транзакцій і ліцензій (ERP/CRM-модулі), засоби аналітики та візуалізації (BI-платформи), інтеграцію з урядовими реєстрами (API до баз даних МВС, митниці тощо).

Облік транзакцій і ліцензій, що реалізується через ERP/CRM-модулі, має низку ключових особливостей. По-перше, система забезпечує централізовану реєстрацію всіх операцій, пов'язаних із продажем, передачею, поверненням та списанням одиниць зброї, з автоматичним прив'язуванням до відповідних ліцензій, дозволів і сертифікатів. По-друге, ERP-модуль відповідає за управління ланцюгами поставок, залишками на складах, строками дії документів, а також формування фінансових звітів і податкової звітності. CRM-компонент дозволяє підтримувати облік клієнтів (фізичних і юридичних осіб), історію їхніх транзакцій, ліцензійний статус, а також здійснювати нагадування про необхідність поновлення дозволів. Система також інтегрується з реєстрами державних органів для перевірки актуальності документів у

реальному часі. Уся інформація зберігається з використанням засобів криптографічного захисту та фіксується у незмінному вигляді в журналах аудиту, що дозволяє забезпечити прозорість, відповідність законодавству та уникнення несанкціонованих дій з боку користувачів.

Засоби аналітики та візуалізації, реалізовані на основі BI-платформ, забезпечують глибоке опрацювання даних, що накопичуються в інформаційній системі обліку зброї. Вони дозволяють в режимі реального часу формувати динамічні звіти, графіки, теплові карти та інші візуальні уявлення про обіг, зберігання, використання та перевірки зброї. Особливістю є можливість аналізу ключових показників (KPI) — таких як кількість реалізованих одиниць, кількість виявлених порушень, географічна концентрація операцій, частота тривожних подій з IoT-сенсорів, тощо. BI-платформи забезпечують гнучку побудову аналітичних панелей (дашбордів) для різних категорій користувачів — від інспекторів і менеджерів складів до державних контролюючих органів. Також передбачена можливість прогностичного аналізу та виявлення аномалій, які можуть свідчити про порушення або зловживання. Інтерфейси BI-інструментів адаптовані для інтеграції з блокчейн-записами, ERP/CRM-модулями та IoT-сенсорами, що дозволяє отримати повну, зведену й достовірну картину функціонування системи в будь-який момент часу.

Інтеграція з урядовими реєстрами (через API до баз даних МВС, митниці, дозвільних органів тощо) є критично важливою особливістю інформаційної системи обліку зброї, що забезпечує легітимність і актуальність усіх транзакцій. Завдяки відкритим або захищеним програмним інтерфейсам, система автоматично звіряє дані про покупця чи продавця зі статусом їхніх дозволів, перевіряє інформацію про зброю в державних реєстрах, підтверджує її походження, серійний номер і відсутність перебування в розшуку. Також під час імпорту або експорту одиниць зброї система отримує від митних органів підтвердження проходження оформлення та дотримання відповідних нормативів. Інтеграція дозволяє виключити ручне введення даних, знижує ймовірність помилок або шахрайства, а також забезпечує автоматичне оновлення статусів ліцензій, сертифікатів, дозволів і документів. Уся взаємодія з урядовими реєстрами протоколюється, а отримані відповіді фіксуються у захищеному вигляді для подальшого аудиту та контролю.

Серед найбільш поширених рішень для побудови інформаційної системи можна назвати Microsoft Dynamics 365 + Power BI — для ведення журналів транзакцій, візуалізації та генерації звітності; Oracle Blockchain Platform — для створення захищеного реєстру постачань; Hyperledger Fabric — модульна блокчейн-архітектура, яка дозволяє створювати permissioned-мережі між державними структурами та приватними постачальниками; Neo4j / GraphDB — графові бази даних, які зручно використовувати для відстеження зв'язків між об'єктами торгівлі, суб'єктами та подіями.

Рішення Microsoft Dynamics 365 у поєднанні з Power BI є потужним комплексом для ведення журналів транзакцій, візуалізації даних та автоматизованої звітності, що добре підходить для реалізації інформаційної системи обліку продажу зброї. Dynamics 365 забезпечує облік транзакцій і ліцензій, дозволяючи створювати гнучку модель зберігання даних про операції з продажу, переміщення та зберігання зброї, при цьому журнали транзакцій інтегруються з модулями CRM для керування взаємодією з клієнтами та ERP для керування логістикою, фінансами, ліцензіями й запасами. Система підтримує автоматизацію перевірок чинності дозвільних документів, таких як ліцензії й сертифікати, а також обмежень на купівлю чи продаж, при цьому бізнес-процеси налаштовуються відповідно до національного законодавства та процедур контролю, включаючи можливість інтеграції з зовнішніми API, наприклад державними реєстрами. Power BI, у свою чергу, дозволяє створювати динамічні звіти та дашборди, такі як карти розподілу операцій зі зброєю, графіки продажів, історія змін статусу одиниць зброї, структура дозволів, а також підтримує аналітику ризиків із виявленням аномалій у поведінці користувачів або в ланцюгах постачання, зокрема частих тривожних подій з IoT-сенсорів чи незвичних обсягів продажу. Завдяки прямій інтеграції з Dynamics 365, Power BI забезпечує доступ до даних ERP/CRM без дублювання чи експорту, що дозволяє ефективно управляти інформацією в єдиному середовищі. Комбінація цих двох платформ гарантує повну відслідковуваність транзакцій і дій користувачів, надає можливість створення персоналізованої аналітики для різних ролей, включаючи інспекторів, продавців та представників державних органів, забезпечує інтеграцію з блокчейн-модулями, IoT-сенсорами та API-інтерфейсами, високий рівень безпеки, контроль доступу та аудит дій. Крім того, рішення готове до масштабування як під більші обсяги операцій, так і під інші регіони. Водночас, серед можливих обмежень варто врахувати необхідність закупівлі ліцензій та витрат на впровадження, потребу в адаптації системи до специфіки обліку зброї, а також залежність від IT-підтримки для забезпечення сумісності з державними сервісами та IoT-пристроями. Загалом Microsoft Dynamics 365 разом із Power BI формують сучасну, масштабовану та безпечну інформаційну платформу, що ефективно підтримує цифровий облік продажу зброї, контроль за ліцензіями та аналітичне супроводження діяльності відповідальних органів.

Oracle Blockchain Platform є високонадійним корпоративним рішенням для створення захищеного, децентралізованого реєстру, що ідеально підходить для відстеження постачань у критично важливих сферах, зокрема в обліку й контролі обігу вогнепальної зброї. Платформа забезпечує незмінність записів. Усі події, пов'язані з виробництвом, імпортом, зберіганням, передачею та продажем зброї, фіксуються у блокчейні як транзакції, які неможливо змінити чи видалити, що забезпечує юридичну цінність таких даних. Децентралізована довіра між учасниками ланцюга постачання, такими як виробники, постачальники, продавці, державні інспектори, реалізується без потреби у єдиному адміністраторі — кожен має можливість перевіряти записи самостійно. Розмежування доступу реалізується через смарт-контракти, які дозволяють

визначити, хто і яку інформацію може бачити, наприклад, інспектори мають доступ лише до перевірок, але не до персональних даних покупців. Oracle Blockchain також підтримує смарт-контракти для автоматизованої перевірки умов — наприклад, якщо ліцензія чинна, транзакцію буде дозволено і запис потрапляє в блокчейн, що підвищує відповідність нормативним вимогам. Платформа інтегрується з IoT-пристроями (сенсори відкриття сейфів, температури тощо) і ERP-системами, зокрема Oracle ERP Cloud або сторонніми системами, як-от SAP, створюючи єдине цифрове середовище. В результаті можливе формування повної прозорості ланцюга постачання, а історія руху товару від виробника до кінцевого користувача зберігається у незмінному реєстрі. Це забезпечує високий рівень довіри та відповідність стандартам безпеки, включаючи ISO/IEC, GDPR, а також дозволяє виконувати вимоги законодавства у сфері обігу зброї. Платформа також гарантує захист від шахрайства через криптографічні механізми й неможливість редагування історії постачань, а її хмарна інфраструктура на базі Oracle Cloud дозволяє масштабувати систему для роботи з великими обсягами транзакцій. Водночас впровадження цієї технології може бути пов'язане з викликами — високі витрати на налаштування й обслуговування, потреба у фахівцях зі смарт-контрактів, а також необхідність нормативної узгодженості з державними структурами для API-інтеграції. Oracle Blockchain Platform — це технологічно зріле, безпечне і масштабоване рішення, яке забезпечує прозорість, контроль і незмінність у сфері обліку постачань зброї, створюючи надійну основу для цифрової трансформації галузі у поєднанні з ERP, IoT та BI-інструментами.

Hyperledger Fabric — це модульна блокчейн-архітектура з відкритим кодом, розроблена Linux Foundation, яка надає гнучку платформу для побудови дозволених мереж і особливо добре підходить для створення захищених міжорганізаційних систем, наприклад, у сфері контролю обігу вогнепальної зброї між державними структурами — МВС, митницею, інспекціями — та приватними учасниками ринку — виробниками, дистриб'юторами, продавцями. На відміну від публічних блокчейнів, таких як Ethereum або Bitcoin, архітектура Fabric передбачає участь у мережі виключно перевірених суб'єктів із використанням сертифікатів, виданих авторизованими центрами, що дозволяє точно регламентувати доступ до створення й перегляду транзакцій. Високий рівень модульності системи дозволяє конфігурувати алгоритми консенсусу, політики доступу, формати транзакцій і правила зберігання даних відповідно до правових, технічних і організаційних вимог галузі. Fabric підтримує мультиканальність — функціонал створення приватних каналів, у межах яких певні групи учасників можуть обмінюватися конфіденційними даними, не доступними для інших — наприклад, окремий канал для взаємодії МВС та митниці або окремий для продавців та контролюючих органів. Завдяки підтримці смарт-контрактів (chaincode), можна автоматизувати перевірку транзакцій — наприклад, транзакція передавання зброї дозволяється лише за наявності чинної ліцензії та проходження митного оформлення. Ці смарт-контракти виконуються ізольовано та підлягають аудиту, що підвищує прозорість і надійність системи. Fabric також підтримує приватність завдяки можливості зберігати конфіденційні дані поза блокчейном у спеціальних колекціях, доступ до яких мають лише уповноважені сторони. Усе це сприяє високому рівню міжвідомчої взаємодії з можливістю юридично значущого аудиту дій усіх учасників, забезпеченню незмінності даних, побудові доказової бази для перевірок, судових справ і розслідувань. Платформа також легко інтегрується з IoT-пристроями й ERP-системами завдяки SDK для Go, Java, Node.js, що дозволяє реалізовувати глибоку бізнес-логіку, взаємодіяти із сенсорами, журналами подій тощо. Fabric підтримує масштабування за рахунок попереднього виконання транзакцій (execute-order-validate), що забезпечує високу продуктивність. Попри всі переваги, система має низку обмежень: складність налаштування дозволених мереж із мультиканальним доступом вимагає глибокої технічної експертизи, високі вимоги до IT-інфраструктури для гарантування надійності та безперебійної роботи, а також потребу в організаційній узгодженості між усіма учасниками щодо правил, політик і сертифікаційної моделі. Загалом, Hyperledger Fabric є зручною платформою для побудови блокчейн-рішень у чутливих сферах, де важливі конфіденційність, контроль транзакцій і керованість доступом. У контексті обігу зброї ця платформа дозволяє реалізувати безпечну, регламентовану та прозору взаємодію між державними і приватними структурами, підтримує гнучке керування політиками та легко інтегрується з іншими модулями — ERP, CRM, IoT, аналітикою.

У свою чергу, Neo4j та GraphDB — це графові бази даних, які спеціалізуються на моделюванні та аналізі взаємозв'язків між об'єктами, що робить їх надзвичайно придатними для інформаційних систем, пов'язаних із торгівлею зброєю. У таких системах важливо ефективно відображати й аналізувати складні зв'язки між постачальниками, покупцями, одиницями зброї, подіями, інспекціями та географічними локаціями. Дані в графових БД можна представити у вигляді вершин (наприклад, “Зброя”, “Інспектор”, “Покупець”, “Подія”) і зв'язків між ними (наприклад, “продав”, “перевірив”, “використовував”), що дозволяє прямо моделювати реальні сценарії обігу зброї. Така структура дає змогу виконувати глибинний аналіз — наприклад, виявляти повторювані або підозрілі патерни поведінки (одна й та ж особа, пов'язана з кількома інцидентами, тривожними подіями тощо). Графові СУБД оптимізовані для складних запитів типу “знайди всі одиниці зброї, які проходили через інспектора X і були пов'язані з покупцями, афілійованими з Y”, що важко реалізується в реляційних базах. Крім того, ці системи мають гнучку схему даних, що дозволяє легко адаптувати модель до змін у законодавстві чи процедурі. Neo4j, як вузькоспеціалізована графова БД, має власну мову запитів Cypher, що дозволяє формулювати складну логіку у зрозумілому форматі, а також підтримує візуалізацію графів, що зручно для інспекторів і слідчих при аналізі схем поставок. Neo4j

інтегрується з мовами програмування (Python, Java) та аналітичними інструментами (Power BI, Tableau) і вже використовується у сферах безпеки, розслідувань, соціальних мереж. GraphDB, натомість, базується на семантичних технологіях RDF і SPARQL, що дозволяє формувати запити на основі онтологій, а також інтегруватися з урядовими класифікаторами, стандартами й довідниками. Це робить її придатною для сценаріїв, де важлива контекстна відповідність — наприклад, визначення дозволених типу зброї в конкретному регіоні відповідно до сертифікації. Графові бази забезпечують наочну візуалізацію взаємозв'язків, допомагають миттєво виявляти підозрілі чи нелегальні зв'язки, інтегруються з блокчейн і аналітичними модулями, проте мають і певні обмеження. Вони потребують спеціалізованої експертизи, не підходять для класичного транзакційного обліку фінансів, тому мають використовуватися спільно з ERP чи блокчейн-компонентами, а також можуть потребувати налаштування на масштабованість у багатокористувацьких сценаріях. Neo4j та GraphDB є ефективними інструментами для побудови глибоких зв'язкових моделей у сфері обліку зброї. Вони забезпечують видимість усіх учасників, подій і маршрутів у єдиному графі, полегшують розслідування, контроль і попередження ризиків, а також забезпечують гнучке масштабування системи у відповідь на зміни в правовому полі або в структурі даних. Ідеальні як аналітичний модуль у складі більшої системи з ERP, блокчейн та IoT-компонентами.

Щоб обрати найбільш доцільне рішення для розроблення інформаційної системи обліку продажу зброї із запропонованих альтернатив за допомогою методу аналізу ієрархій (AHP – Analytic Hierarchy Process), потрібно покроково виконати алгоритм.

Крок 1. Визначити критерії оцінювання.

Для системи обліку продажу зброї логічними критеріями будуть:

1. Безпека – наскільки рішення забезпечує захищеність транзакцій, даних, доступу.
2. Масштабованість – здатність рішення розширюватися з ростом системи.
3. Інтеграційна сумісність – можливість з'єднання з державними реєстрами, ERP, IoT, BI тощо.
4. Придатність для контролю та аналітики – наскільки добре рішення підтримує аналіз зв'язків, перевірку подій, пошук аномалій.

перевірку подій, пошук аномалій.

Крок 2. Побудувати ієрархію за критеріями безпека, масштабованість, інтеграційна сумісність, придатність для контролю та аналітики.

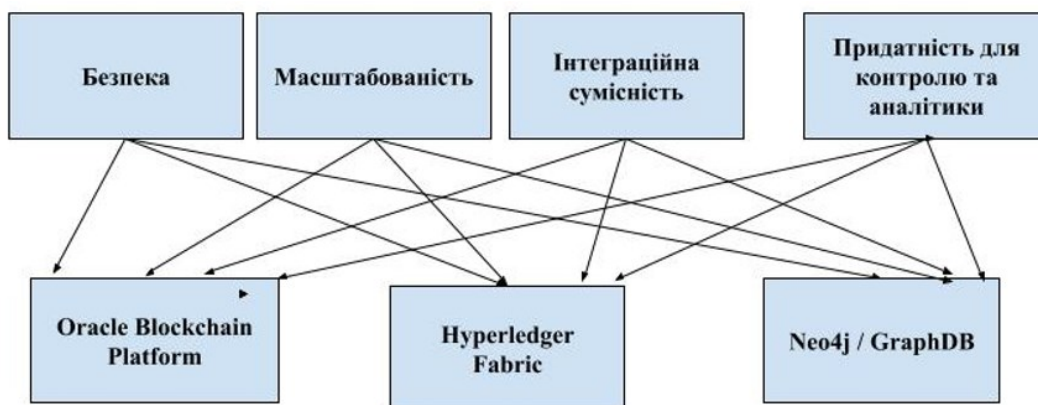


Рис.1. Ієрархію альтернатив за критеріями

Крок 3. Створення матриці парних порівнянь критеріїв

Таблиця 1

Попарне порівняння ваг критеріїв				
Критерії	Безпека	Масштабованість	Інтеграційна сумісність	Контроль/Аналітика
Безпека	1	2	2	3
Масштабованість	0.5	1	2	2
Інтеграційна сумісність	0.5	0.5	1	2
Контроль/Аналітика	0.33	0.5	0.5	1

Після нормалізації та обчислення ваг (можна деталізувати за потреби), наприклад:

- Безпека — 0.38
- Масштабованість — 0.27
- Інтеграційна сумісність — 0.20
- Контроль/Аналітика — 0.15

Крок 4. Оцінювання альтернатив за кожним критерієм (0–1 або за шкалою Сааті)

Таблиця 2

Оцінки альтернатив за критеріями

Критерій/альтернатива	Oracle Blockchain Platform	Hyperledger Fabric	Neo4j / GraphDB — 0.6
Безпека	0.9	1.0	0.6
Масштабованість	0.8	0.9	0.7
Інтеграційна сумісність	0.7	0.9	0.8
Контроль / Аналітика	0.6	0.7	1.0

Крок 5. Обчислення зважених балів

Таблиця 3

Зважені бали

Альтернатива	Безпека	Масштабованість	Інтеграція	Аналітика	Сума
Oracle Blockchain	0.342	0.216	0.14	0.09	0.788
Hyperledger Fabric	0.38	0.243	0.18	0.105	0.908
Neo4j / GraphDB	0.228	0.189	0.16	0.15	0.727

Найбільш збалансованим рішенням згідно з методом аналізу ієрархій є Hyperledger Fabric, оскільки воно має найвищу сумарну зважену оцінку (0.908). Його модульність, підтримка permissioned-мереж та гнучка інтеграція роблять його оптимальним для побудови державної системи з високими вимогами до безпеки та масштабованості.

Розроблення сучасної інформаційної системи обліку продажу зброї — це технологічно та організаційно складне завдання, що передбачає поєднання високого рівня безпеки, точності, аналітики та міжвідомчої кооперації. Проте завдяки інтеграції блокчейну, IoT, графових БД, біометрії та сучасних BI-платформ, така система може суттєво підвищити прозорість обігу зброї, зменшити зловживання, пришвидшити контрольні процеси та створити надійний інструмент для аудиту й кримінального розслідування.

Структура системи

Нехай інформаційна система обліку продажу зброї описується як п'ятірка:

$$S = \langle Z, U, B, I, L \rangle,$$

де Z — множина одиниць зброї, U — множина користувачів системи (продавці, покупці, інспектори), B — множина біометричних ідентифікаторів користувачів, I — множина IoT-подій (відкриття сейфу, переміщення, температурні відхилення тощо), L — розподілений журнал (ledger), який базується на блокчейн-технології.

Інформаційна система містить важливі компоненти маркування RFID / QR / Datamatrix.

Кожна одиниця зброї має унікальний маркер:

$$\forall z \in Z, \exists! m_z \in M: m_z \in RFID \cup QR \cup DM,$$

де M — множина маркерів, RFID, QR, DM — відповідно множини RFID-міток, QR- та Datamatrix-кодів.

У спеціалізованому магазині покупець звертається з метою придбання вогнепальної зброї. Кожна одиниця зброї у магазині перед продажем проходить процедуру маркування. Залежно від доступної інфраструктури, до зброї прикріплено одну з форм ідентифікаторів RFID-мітку, QR-код або Datamatrix-код, які містять унікальний ідентифікаційний номер, серію, модель, дату виробництва та дані про виробника.

Продавець за допомогою RFID-зчитувача або оптичного сканера (у випадку QR/Datamatrix) зчитує код маркування, після чого система автоматично витягує всю пов'язану з цим кодом інформацію з бази даних. Водночас, покупець проходить біометричну автентифікацію для підтвердження особи та наявності дозволу на придбання зброї. Дані про ідентифікатор зброї, особу покупця, час продажу, місце і відповідального продавця автоматично формують транзакцію, яка фіксується у розподіленому блокчейн-реєстрі.

Таким чином, компоненти маркування (RFID / QR / Datamatrix) відіграють ключову роль у забезпеченні точного, однозначного та автоматизованого зв'язку між фізичним об'єктом (зброєю) та цифровими записами в інформаційній системі, що унеможливорює підміну, втрату чи дублювання об'єктів під час продажу або перевірки. Інформаційна система використовує технології маркування для забезпечення ідентифікації, відстежуваності та безпеки у процесі обліку і продажу зброї.

Ідентифікація користувачів проводиться декількома способами. Біометрична функція виконується $\beta: U \rightarrow B$, і ставить у відповідність кожному користувачеві його біометричний шаблон (відбиток пальця, зображення обличчя тощо). Функція автентифікації відбувається таким чином

$$\alpha: B \times B \rightarrow \{0,1\}, \alpha(b_1, b_2) = \begin{cases} 1, & \text{якщо } b_1 \approx b_2 \\ 0, & \text{інакше} \end{cases}$$

Ідентифікація користувачів проводиться декількома способами — поєднанням паролів, RFID-ідентифікаторів і біометричних даних — для підвищення рівня безпеки та запобігання несанкціонованому доступу до критично важливих об'єктів.

Розглянемо використання автентифікації при доступ інспектора до сховища зі зброєю на складі. Інспектор внутрішньої служби прибуває на склад для перевірки обліку та умов зберігання вогнепальної зброї. Щоб отримати доступ до електронної системи обліку та фізичного сейфу, інспектор проходить багаторівневу ідентифікацію. Спочатку система запитує введення персонального ідентифікатора (логіну) та пароля, що є базовим способом автентифікації. Після цього інспектор прикладає палець до біометричного сканера, який звіряє відбиток із збереженим шаблоном у системі. Третій етап включає зчитування персоналізованої RFID-картки, яку інспектор носить як службове посвідчення.

Лише у випадку успішного проходження всіх етапів ідентифікації, система надає дозвіл на відкриття сейфу, а також дозволяє перегляд і редагування записів у базі даних про збережену зброю. Кожен етап входу та використання фіксується в системному журналі, який пізніше може бути перевірений керівництвом або аудитором.

Використання IoT-сенсорів дозволяє генерувати події $i: T \rightarrow I, i(t) =$ подія, зафіксована у момент t . Події можуть бути представлені як кортежі $i = \langle z, u, t, \delta \rangle$, де $z \in Z$ — одиниця зброї, $u \in U$ — користувач, що спричинив подію, $t \in T$ — час події, δ — тип події (наприклад, відкриття сейфу, переміщення, перевищення температури).

Розглянемо використання IoT-сенсорів для виявлення несанкціонованого відкриття сейфу зі зброєю. У нічний час на складі, де зберігається службова вогнепальна зброя, спрацьовує давач відкриття сейфу, підключений до інформаційної системи через IoT-інфраструктуру. Давач фіксує, що дверця сейфу було відкрито о 02:43 без попереднього зареєстрованого доступу з боку авторизованого персоналу.

У цей момент IoT-сенсор генерує подію, яка автоматично передається до централізованого сервера системи контролю доступу. Подія містить такі параметри як час спрацювання, геолокація сейфу, серійний номер зброї, що зберігається, а також інформацію про відсутність успішної ідентифікації користувача через RFID або біометричний сканер.

У відповідь система запускає ланцюг безпекових дій. Активується сигналізація, на пульт охорони надходить сповіщення, одночасно надсилається SMS-повідомлення черговому інспектору. Подія також автоматично записується у блокчейн-реєстр, де її неможливо змінити або видалити.



Рис.2. Ланцюжок подій, зафіксовані IoT-пристроями

Далі відбувається реєстрація транзакцій у блокчейні. Кожна транзакція записується у блокчейн як:

$$\tau = \langle z, u_s, u_r, t, m_z, i, \sigma \rangle,$$

де $u_s, u_r \in U$ — відправник і отримувач (продавець та покупець), m_z — маркер зброї, i — подія з IoT, σ — цифровий підпис транзакції (гарантія достовірності).

Всі транзакції формують розподілений реєстр $L = \{\tau_1, \tau_2, \dots, \tau_n\}$.

Розглянемо як відбувається продаж одиниці зброї через авторизовану торгову точку. Покупець звертається до ліцензованого магазину для придбання мисливської рушниці. Після перевірки дозволів та проходження біометричної ідентифікації, продавець сканує Datamatrix-код на зброї, який містить унікальний ідентифікаційний номер виробу. Система підтверджує відповідність зброї обліковим даним у базі та генерує транзакцію продажу. Ця транзакція містить ID зброї; ID продавця та покупця (зі зв'язком до їхніх біометричних ідентифікаторів); час і місце операції; цифровий підпис обох сторін; технічні дані з IoT-сенсорів, які підтверджують факт відкриття сейфу та переміщення зброї.

Далі відбувається реєстрація транзакції у блокчейні. Система формує блок із відповідними криптографічними хешами, підписує його цифровими ключами продавця і покупця, і додає його до розподіленого журналу. Всі наступні транзакції з цією одиницею зброї будуть ланцюгово пов'язані з цією початковою операцією продажу. Після цього покупець отримує підтвердження покупки у вигляді захищеного цифрового сертифіката, а уповноважені державні органи — миттєвий доступ до запису про операцію через вузли блокчейн-системи. Реєстрація транзакцій у блокчейні забезпечує прозорість, незмінність та довіру до процесу обліку продажу зброї, фіксуючи кожну дію як юридично значущу подію в захищеному цифровому реєстрі.

Цільова функція системи

Метою системи є гарантування відстежуваності, персоніфікації та безпеки:

$$\Phi: S \rightarrow \{\text{Безпечна, Прозора, Перевірювана}\}$$

Таким чином, система S поєднує фізичні об'єкти (зброю, маркування, сенсори), користувачів з біометричним контролем доступу та інформаційно-обчислювальну інфраструктуру (IoT і блокчейн), що забезпечує цілісність, безпеку та відстежуваність усіх операцій у режимі реального часу.

Реалізацію цільової функції системи передбачає досягнення таких ключових властивостей, як безпека, відстежуваність і можливість перевірки усіх операцій із вогнепальною зброєю. Проводиться аудит постачання та продажу партії зброї. У рамках планової перевірки Державна служба контролю обігу зброї ініціює аудит постачання і реалізації партії мисливських карабінів, що надійшли на склад великого дистриб'ютора три місяці тому. Завдяки інтегрованій інформаційній системі, інспектор швидко отримує доступ до повного цифрового ланцюга подій, пов'язаних з кожною одиницею зброї в партії. Система забезпечує безпеку, оскільки доступ до даних можливий лише після автентифікації через біометричний сканер та службове посвідчення з RFID-модулем. Усі дії інспектора фіксуються в системі, а перегляд даних дозволено лише в межах його повноважень. Відстежуваність реалізується тим, що для кожної одиниці зброї інспектор бачить повний маршрут - від маркування (RFID / QR / Datamatrix) і дати надходження на склад до подій, зафіксованих IoT-сенсорами (відкриття сейфу, транспортування, температурні режими), моменту продажу з біометрично підтвердженими даними покупця та геолокаційних міток кожної події. Можливість перевірки досягається завдяки збереженню всіх операцій у блокчейн-реєстрі, де інспектор перевіряє хеш-транзакцій для підтвердження автентичності записів. У процесі перевірки виявляється, що одна одиниця зброї не пройшла через процедуру продажу, але була фізично переміщена — ця подія також була зафіксована IoT-сенсором і відображена як тривожна у системі. На підставі цієї інформації формується звіт про потенційне порушення, і керівництво ініціює службове розслідування. Реалізація цільової функції системи полягає у забезпеченні повного контролю та цифрової прозорості на кожному етапі життєвого циклу зброї, включно з її постачанням, зберіганням, реалізацією та аудитом, що є критично важливим для державного і правового регулювання.

Висновки

У статті розглянуто сучасні підходи до інформаційно-технологічного супроводу процесів обліку торгівлі вогнепальною зброєю з урахуванням вимог безпеки, простежуваності, перевірюваності та міжвідомчої інтеграції. Запропоновано використання RFID-міток, QR/Datamatrix-кодів, біометричних сканерів, IoT-сенсорів і блокчейн-технологій як ключових компонентів системи. Окрема увага приділена ролі ERP/CRM-модулів, BI-платформ та графових баз даних для підтримки операційного управління, візуалізації й аналізу зв'язків між суб'єктами торгівлі та об'єктами обліку. Проаналізовано переваги використання платформ Microsoft Dynamics 365, Oracle Blockchain Platform, Hyperledger Fabric та Neo4j/GraphDB у межах архітектури цільової системи. Проаналізовано особливості проектування інформаційної системи обліку продажу зброї. Зроблено висновок, що поєднання таких засобів дозволяє створити інтегровану, надійну та адаптивну інформаційну систему, здатну ефективно супроводжувати всі етапи життєвого циклу обігу зброї — від маркування до реалізації та моніторингу після продажу.

Література

1. Chowdhury M., Colman A., Kabir A., Han J., Sarda P. Blockchain Versus Database: A Critical Analysis // Proceedings of the 2018 IEEE TrustCom/BigDataSE. — 2018. — С. 1348–1353. — DOI: 10.1109/TrustCom/BigDataSE.2018.00186.
2. Aleinikova O., Kravchenko O., Hurochkina V., Zvonar V., Brechko O. Improving Public Administration by Block Chain Technologies // International Journal of Future Generation Communication and Networking. — 2020. — Vol. 13, № 4. — P. 1824–1835.
3. Кунанець Н., Яримович Ю. Створення смарт-контрактів у інформаційній системі обліку продажу зброї // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. — 2025. — № 58. — С. 212–224. — DOI: 10.36910/6775-2524-0560-2025-58-25.
4. Луцків А.М., Гладій В.В. Особливості функціонування та класифікації розподілених систем зберігання даних // Матеріали XII міжнар. наук.-практ. конф. молодих учених та студентів «Актуальні задачі сучасних технологій» (6–7 грудня 2023 р.). — Тернопіль: ТНТУ, 2022. — С. 455.

5. Zhang C., Chen T., Wang Y., Liu Y. Anomaly detection in financial transactions using machine learning: A case study in weapon trade data // *Expert Systems with Applications*. – 2021. – Vol. 184. – Article ID: 115487. – DOI: 10.1016/j.eswa.2021.115487.
6. Павлюк А.В., Луценко М.М. Аналіз механізмів захисту технології блокчейн від кібератак // *Сучасний захист інформації*. – 2022. – № 2. – С. 59–65.
7. Williams S. 20 Real-World Uses for Blockchain Technology [Електронний ресурс] / Sean Williams // *The Motley Fool*. – 2018. – Режим доступу: <https://www.fool.com/investing/2018/04/11/20-real-world-uses-forblockchain-technology.aspx>.
8. Kamble S., Gunasekaran A., Arha H. Understanding the Blockchain technology adoption in supply chains – Indian context // *International Journal of Production Research*. – 2018. – Vol. 57. – P. 1–25. – DOI: 10.1080/00207543.2018.1518610.
9. Kumar R., Reddy P.K., Tiwari M.K. Secure RFID-based inventory and identification system for critical assets // *Journal of Network and Computer Applications*. – 2022. – Vol. 197. – Article ID: 103316. – DOI: 10.1016/j.jnca.2021.103316.
10. Soni N. Evolution of Blockchain [Електронний ресурс] / Neha Soni. – 2020. – Режим доступу: <https://medium.com/@nehasoni1812/evolution-ofblockchainf243f7509fe6#:~:text=Stefan%20Konst%20published%20his%20theory,linked%20together%20using%20cryptographic%20methods>.

References

1. Chowdhury M., Colman A., Kabir A., Han J., Sarda P. Blockchain Versus Database: A Critical Analysis // *Proceedings of the 2018 IEEE TrustCom/BigDataSE*. – 2018. – C. 1348–1353. – DOI: 10.1109/TrustCom/BigDataSE.2018.00186.
2. Aleinikova O., Kravchenko O., Hurochkina V., Zvonar V., Brechko O. Improving Public Administration by Block Chain Technologies // *International Journal of Future Generation Communication and Networking*. – 2020. – Vol. 13, № 4. – P. 1824–1835.
3. Kusanets N., Yarymovych Y. Development of Smart Contracts in the Information System for Weapons Sales Accounting // *Computer-Integrated Technologies: Education, Science, Production..* – 2025. – № 58. – C. 212–224. – DOI: 10.36910/6775-2524-0560-2025-58-25.
4. Lutsiv A.M., Hladiy V.V. Features of Functioning and Classification of Distributed Data Storage Systems // *Proceedings of the 12th International Scientific and Practical Conference of Young Scientists and Students "Current Issues of Modern Technologies" (December 6–7, 2023)*. – Ternopil: TNTU, 2022. – C. 455.
5. Zhang C., Chen T., Wang Y., Liu Y. Anomaly detection in financial transactions using machine learning: A case study in weapon trade data // *Expert Systems with Applications*. – 2021. – Vol. 184. – Article ID: 115487. – DOI: 10.1016/j.eswa.2021.115487.
6. Pavliuk A.V., Lutsenko M.M. Analysis of Blockchain Technology Protection Mechanisms Against Cyberattacks // *Modern Information Protection*. – 2022. – № 2. – С. 59–65.
7. Williams S. 20 Real-World Uses for Blockchain Technology [Електронний ресурс] / Sean Williams // *The Motley Fool*. – 2018. – Режим доступу: <https://www.fool.com/investing/2018/04/11/20-real-world-uses-forblockchain-technology.aspx>.
8. Kamble S., Gunasekaran A., Arha H. Understanding the Blockchain technology adoption in supply chains – Indian context // *International Journal of Production Research*. – 2018. – Vol. 57. – P. 1–25. – DOI: 10.1080/00207543.2018.1518610.
9. Kumar R., Reddy P.K., Tiwari M.K. Secure RFID-based inventory and identification system for critical assets // *Journal of Network and Computer Applications*. – 2022. – Vol. 197. – Article ID: 103316. – DOI: 10.1016/j.jnca.2021.103316.
10. Soni N. Evolution of Blockchain [Електронний ресурс] / Neha Soni. – 2020. – Режим доступу: <https://medium.com/@nehasoni1812/evolution-ofblockchainf243f7509fe6#:~:text=Stefan%20Konst%20published%20his%20theory,linked%20together%20using%20cryptographic%20method>s.