Regulatory and Legal Aspects of Electronic Document Management in the State Defense Sector Governance System

UDC: 351.9:355.4+347.7+004.9 DOI: https://doi.org/10.15421/152512

Orlov Oleksandr[1]
Dr.Sc., Full Prof., https://orcid.org/0000-0001-8995-7383, avorlovav@gmail.com
Zhyvylo Yevhen[2]
Ph.D., Senior Lecturer, https://orcid.org/0000-0003-4077-7853, zhivilka@i.ua
Nesterenko Victor[1]
Ph.D. Student, https://orcid.org/0000-0002-4237-3433, svictors_1975@ukr.net
[1]V. N. Karazin Kharkiv National University, (Kharkiv, Ukraine)
[2]National University «Yuri Kondratyuk Poltava Polytechnic» (Poltava, Ukraine)

Abstract
The article examines the regulatory and legal aspects of electronic document management in the system of public administration within the national defense sector. The current state of legal regulation in this field is analyzed, and key gaps that hinder the effective implementation of artificial intelligence and blockchain technologies in the document management systems of defense institutions are identified.

Relevant legal challenges associated with the integration of AI and blockchain technologies into the electronic document management of the defense sector are identified, including: the lack of a regulatory definition of the legal status of documents created using AI algorithms; uncertainty regarding mechanisms for assigning responsibility when using automated decision-making systems; the absence of specific requirements for data protection when using distributed ledgers and AI systems; and the unresolved issues of interoperability between electronic document management systems across various defense structures.

It is substantiated that the implementation of the proposed measures will create the legal prerequisites for the effective and secure integration of AI and blockchain technologies into the electronic document management of the national defense sector, improve the efficiency of administrative processes, and ensure an adequate level of information security. Prospective directions for further research are outlined, including the development of methodological approaches for assessing legal risks associated with the introduction of emerging technologies into electronic document management systems of the defense sector, and the exploration of legal regulation aspects related to the use of quantum computing technologies to ensure the future security of electronic document management.

Keywords: electronic document management, defense sector, legal regulation, artificial intelligence, blockchain, information security, public administration, interoperability, cybersecurity, digital transformation

Нормативно-правові аспекти електронного документообігу в системі державного управління сектору оборони держави

Орлов Олександр[1], **Живило Євген**[2], **Нестеренко Віктор**[1]
[1]Харківський національний університет імені В.Н. Каразіна. (Харків, Україна)
[2]Національний університет «Полтавська політехніка імені Юрія Кондратюка», (Полтава, Україна)

Анотація
У статті досліджено нормативно-правові аспекти електронного документообігу в системі державного управління сектору оборони держави. Проаналізовано сучасний стан правового регулювання в цій сфері та виявлено ключові прогалини, що перешкоджають ефективному впровадженню технологій штучного інтелекту та блокчейну в систему документообігу оборонного відомства.

Визначено актуальні правові виклики, що пов'язані з впровадженням технологій ШІ та блокчейну в електронний документообіг оборонного сектору, зокрема: відсутність нормативного визначення правового статусу документів, створених із застосуванням алгоритмів штучного інтелекту; невизначеність механізмів розподілу відповідальності при використанні автоматизованих систем прийняття рішень; відсутність спеціальних вимог до захисту даних при використанні розподілених реєстрів та систем штучного інтелекту; неврегульованість питань інтероперабельності систем електронного документообігу в різних структурах сектору оборони.

Обґрунтовано, що реалізація запропонованих заходів дозволить створити правові передумови для ефективного та безпечного впровадження технологій ШІ та блокчейну в електронний документообіг сектору оборони держави, підвищити оперативність управлінських процесів та забезпечити належний рівень захисту інформації. Визначено перспективні напрями подальших досліджень, пов'язані з розробкою методичних підходів до оцінки правових ризиків впровадження новітніх технологій у системи електронного документообігу сектору оборони та дослідженням особливостей правового регулювання застосування технологій квантових обчислень для забезпечення безпеки електронного документообігу в майбутньому.

Ключові слова: електронний документообіг, сектор оборони, нормативно-правове регулювання, штучний інтелект, блокчейн, інформаційна безпека, державне управління, інтероперабельність, кібербезпека, цифрова трансформація

Стаття надійшла / Article arrived: 09.02.2025 Схвалено до друку / Accepted: 26.03.2025

Вступ.

Постановка проблеми у загальному вигляді та її зв'язок з важливими науковими чи практичними завданнями. В умовах цифрової трансформації державного управління та загострення кібербезпекових викликів особливої актуальності набуває питання ефективної та захищеної організації електронного документообігу в секторі оборони держави. Підрозділи оборонного відомства щоденно генерують та опрацьовують значний масив документів, частина яких містить інформацію з обмеженим доступом та потребує підвищених заходів захисту. Водночас оперативність прийняття управлінських рішень у секторі оборони часто має критичне значення для національної безпеки.

Впровадження новітніх технологій, зокрема штучного інтелекту (ШІ) та блокчейну, відкриває нові можливості для оптимізації процесів документообігу та забезпечення їх безпеки. Однак застосування цих інноваційних технологій у такій специфічній сфері, як оборонний сектор, потребує належного правового регулювання, яке наразі характеризується фрагментарністю та недостатньою адаптованістю до сучасних викликів.

Проблема полягає у суперечності між потребою у впровадженні передових технологічних рішень для забезпечення ефективності та захищеності електронного документообігу в секторі оборони та недосконалістю нормативно-правової бази, що регулює ці процеси в Україні. Вирішення цієї проблеми має безпосередній зв'язок із завданнями забезпечення національної безпеки, підвищення ефективності державного управління та реалізації стратегії цифрової трансформації держави.

Аналіз останніх досліджень і публікацій. Проблеми нормативно-правового забезпечення електронного документообігу в системі державного управління досліджували такі вчені, як О. Баранов, М. Швець, В. Брижко, які заклали фундаментальні підходи до розуміння правових засад інформатизації державного управління (Баранов та ін., 2019). Н. Грицяк та Л. Литвинова проаналізували особливості впровадження електронного урядування в Україні та його правові аспекти (Грицяк, & Литвинова, 2020). І. Клименко та К. Линьов розглядали технології електронного урядування з точки зору їх нормативного забезпечення (Клименко, & Линьов, 2018).

Питання безпеки електронного документообігу в державних структурах висвітлено у працях В. Бурячка, В. Толубка, С. Толюпи (Бурячок та ін., 2015). Ці дослідники зосередили увагу на технічних та організаційних аспектах захисту інформації в інформаційно-телекомунікаційних системах державних органів. Л. Чистоклетов та С. Обрембальський досліджували специфіку інформаційної безпеки в умовах інформаційних протистоянь (Чистоклетов, & Обрембальський, 2024).

Останніми роками з'явилися дослідження, присвячені застосуванню новітніх технологій у державному управлінні. Зокрема, О. Кравченко та О. Шаповал аналізували перспективи використання технології блокчейн у публічному управлінні (Кравченко та Шаповал, 2021). А. Ільєнко, С. Ільєнко, О. Яковенко, Є. Галич та В. Павленко розглядали можливості імплементації технологій штучного інтелекту в системи кібербезпеки (Ільєнко та ін., 2024).

Специфіку функціонування інформаційних систем у військовій сфері та оборонному секторі, положення, пов'язані із забезпеченням інформаційної безпеки та системами захисту інформації, яка циркулює в об'єктах інформатизації військового управління, досліджено у колективній монографії (Величко та ін., 2021), де приділено велику увагу особливим вимогам до захисту інформації військового характеру в електронних системах.

Аналіз наукових публікацій вказує на те, що дослідники здебільшого розглядали загальні питання електронного документообігу в державному управлінні або окремі аспекти застосування ШІ та блокчейну в державних інформаційних системах. Водночас недостатньо дослідженими залишаються питання комплексного нормативно-правового регулювання впровадження цих технологій саме в системі документообігу сектору оборони держави з урахуванням його специфіки, що зумовлює актуальність даного дослідження.

Метою статті є дослідження сучасного стану нормативно-правового забезпечення електронного документообігу в системі державного управління сектору оборони держави та розробка пропозицій щодо його вдосконалення з урахуванням можливостей імплементації технологій штучного інтелекту та блокчейну.

Для досягнення поставленої мети визначено такі завдання:

1. Проаналізувати чинну нормативно-правову базу, що регулює електронний документообіг у системі державного управління сектору оборони.

2. Визначити правові проблеми та колізії, що виникають при впровадженні технологій ШІ та блокчейну в електронний документообіг оборонного сектору.

3. Дослідити міжнародний досвід правового регулювання застосування інноваційних технологій у документообігу військових відомств країн-членів НАТО.

4. Розробити пропозиції щодо вдосконалення нормативно-правового забезпечення впровадження ШІ та блокчейну в систему електронного документообігу сектору оборони держави.

Результати дослідження.

Нормативно-правова база, що регулює електронний документообіг у системі державного управління України загалом та у секторі оборони зокрема, представлена низкою законодавчих та підзаконних актів. Основоположними документами є Закони України "Про електронні документи та електронний документообіг" (Верховна Рада України, 2003), "Про електронні довірчі послуги" (Верховна Рада України, 2017), "Про захист інформації в інформаційно-телекомунікаційних системах" (Верховна Рада України, 1994b), "Про державну таємницю" (Верховна Рада України, 1994a).

Специфіка електронного документообігу в секторі оборони додатково регулюється нормативними актами Міністерства оборони України та Генерального штабу Збройних Сил України, зокрема наказом Міністерства оборони України "Про затвердження Порядку організації електронного документообігу в системі Міністерства оборони України" (Міністерство оборони України, 2020). Окремі аспекти захисту інформації в оборонному секторі регламентуються положеннями Закону України "Про основи національної безпеки України" (Верховна Рада України, 2018) та Стратегією кібербезпеки України (Верховна Рада України, 2021).

Аналіз зазначених нормативно-правових актів показує, що хоча вони й створюють загальну основу для функціонування електронного документообігу, проте не враховують повною мірою специфіку застосування новітніх технологій, таких як ШІ та блокчейн. Зокрема, відсутні положення, які б визначали правовий статус документів, створених із застосуванням алгоритмів штучного інтелекту або таких, що зберігаються в розподілених регистрах.

Також варто зазначити, що чинні нормативно-правові акти не забезпечують належного рівня стандартів взаємодії систем електронного документообігу в різних структурах сектору оборони та їх взаємодії з цивільними органами державної влади, що суттєво знижує ефективність управлінських процесів, особливо в умовах кризових ситуацій (Болдуєв та ін., 2024).

Впровадження технологій штучного інтелекту в системи електронного документообігу сектору оборони відкриває значні можливості для автоматизації процесів класифікації, маршрутизації, обробки та аналізу документів. Однак застосування алгоритмів машинного навчання у цій сфері породжує низку правових питань, які потребують нормативного врегулювання.

По-перше, постає питання відповідальності за рішення, прийняті з використанням систем штучного інтелекту. Чинне законодавство України не містить положень, які б визначали механізми розподілу такої відповідальності між розробниками алгоритмів, адміністраторами систем та кінцевими користувачами (Радутний, 2017). Особливої гостроти це питання набуває у контексті застосування ШІ для класифікації документів за ступенем секретності або для визначення пріоритетності документів у сфері національної безпеки та оборони.

По-друге, використання алгоритмів машинного навчання передбачає обробку великих масивів даних, що може суперечити вимогам щодо захисту інформації з обмеженим доступом. Законодавство має встановлювати чіткі критерії та умови, за яких допускається використання таких даних для навчання алгоритмів ШІ, а також визначати вимоги до захисту самих моделей машинного навчання від несанкціонованого доступу (Баранов, 2018).

Щодо технології блокчейн, її впровадження в систему електронного документообігу сектору оборони може забезпечити неспростовність та цілісність даних, що є критично важливим для документів стратегічного значення. Водночас розподілений характер зберігання даних у блокчейні створює нові виклики для забезпечення конфіденційності інформації з обмеженим доступом (Спасітєлєва, & Бурячок, 2018).

Чинна нормативно-правова база України не містить спеціальних положень щодо застосування технології розподілених реєстрів у сфері державного управління та, зокрема, в секторі оборони. Відсутні нормативні визначення таких понять як "смарт-контракт", "блокчейн", "розподілений реєстр" у контексті документообігу (Кудь та ін., 2022). Це створює правову невизначеність та стримує впровадження зазначених технологій у практику державного управління.

Аналіз міжнародного досвіду свідчить про активне формування правових рамок для застосування новітніх технологій у секторі оборони. Зокрема, у США Департамент оборони у 2020 році ухвалив "Стратегію розвитку штучного

інтелекту у сфері оборони", яка визначає правові та етичні принципи застосування ШІ у військовій сфері, включаючи системи управління документами (U.S. Department of Defense, 2020). Важливим аспектом цієї стратегії є встановлення принципу "людина у контурі", який передбачає обов'язкову участь людини у прийнятті рішень на основі рекомендацій систем штучного інтелекту.

Європейський Союз розробив "Етичні настанови щодо надійного ШІ", які хоч і мають рекомендаційний характер, але закладають основи для гармонізації правового регулювання застосування ШІ в державному управлінні країн-членів ЄС (High-Level Expert Group on Artificial Intelligence, 2019). Ці настанови пропонують підхід до регулювання ШІ, заснований на оцінці ризиків, що є особливо актуальним для сектору оборони.

Щодо технології блокчейн, показовим є досвід Естонії, яка імплементувала KSI Blockchain у державні реєстри для забезпечення цілісності даних. Особливістю естонського підходу є розмежування відкритих даних, які зберігаються у традиційних базах даних, та криптографічних доказів цілісності цих даних, які фіксуються у блокчейні (Ковач та Ковач, 2023). Такий підхід дозволяє забезпечити баланс між прозорістю та захистом конфіденційної інформації.

НАТО в рамках ініціативи "NATO 2030" визначило розвиток технологій ШІ та блокчейну як один із пріоритетних напрямів технологічної трансформації Альянсу. У 2021 році було ухвалено "Стратегію НАТО з штучного інтелекту", яка серед іншого регламентує питання застосування ШІ в системах обміну інформацією між країнами-членами (NATO, 2021). Особливу увагу приділено питанням сумісності національних систем та стандартизації підходів до забезпечення безпеки даних.

На основі проведеного аналізу пропонуються такі напрями вдосконалення нормативно-правового забезпечення електронного документообігу в системі державного управління сектору оборони держави з урахуванням впровадження технологій ШІ та блокчейну:

1. Розробка та ухвалення спеціального закону "Про застосування технологій штучного інтелекту та розподілених реєстрів у державному управлінні", який би визначав основні поняття, принципи та механізми використання цих технологій в державних інформаційних системах, включаючи системи сектору оборони. Закон має встановлювати:

– правовий статус документів, створених із застосуванням технологій ШІ;

– механізми розподілу відповідальності при використанні автоматизованих систем прийняття рішень;

– вимоги до прозорості алгоритмів та їх аудиту;

– порядок застосування смарт-контрактів у державному управлінні.

2. Внесення змін до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" у частині регламентації процедур захисту даних при використанні розподілених реєстрів та систем штучного інтелекту. Зокрема, необхідно встановити додаткові вимоги до захисту моделей машинного навчання, які використовуються для обробки інформації з обмеженим доступом, та визначити особливості застосування криптографічних методів захисту інформації в блокчейн-системах (Верховна Рада України, 1994b).

3. Розробка галузевого стандарту для сектору оборони щодо застосування технологій ШІ та блокчейну в системах електронного документообігу, який би враховував специфіку інформації, що циркулює в цих системах, та особливі вимоги до її захисту. Стандарт має визначати:

– критерії допустимості автоматизованої обробки документів різних категорій;

– вимоги до наборів даних, що використовуються для навчання алгоритмів ШІ;

– протоколи верифікації результатів роботи систем ШІ;

– архітектурні рішення для побудови блокчейн-систем з урахуванням вимог конфіденційності.

4. Ухвалення нормативного акту Кабінету Міністрів України "Про порядок забезпечення інтероперабельності систем електронного документообігу в секторі безпеки і оборони", який би регламентував стандарти обміну даними між різними відомствами сектору оборони та їх взаємодію з цивільними органами державної влади в умовах використання технологій ШІ та блокчейну.

5. Внесення змін до наказу Міністерства оборони України "Про затвердження Порядку організації електронного документообігу в системі Міністерства оборони України" з метою врегулювання процедур використання алгоритмів машинного навчання для класифікації, маршрутизації та аналізу документів, а також застосування технології блокчейн для забезпечення цілісності та неспростовності критично важливих документів (Міністерство оборони України, 2020).

Соціальні мережі стали невід'ємною частиною нашого спілкування, але в умовах

війни вони можуть становити серйозну загрозу для безпеки як окремих військовослужбовців, так і підрозділів в цілому. Необхідно на законодавчому рівні затвердити рекомендації щодо безпечного користування соціальними мережами, захисту особистої інформації та уникнення публікації контенту, який може бути використаний ворогом (Міністерство оборони України, б.д.).

Використання месенджерів для оперативного обміну службовою інформацією стає невід'ємною частиною сучасних комунікаційних процесів у державному управлінні. В умовах динамічного інформаційного середовища месенджери стають ефективним інструментом оперативної комунікації, проте потребують особливих підходів до забезпечення безпеки інформації.

Сучасне розуміння електронного документообігу, як правило, не включає безпосереднє спілкування через месенджери як основний компонент, але може використовувати їх для певних супутніх цілей. Інтеграція захищених месенджерів у систему електронного документообігу є перспективним напрямком розвитку, який потребує належного правового регулювання. Сьогодні необхідно констатувати, що використання месенджерів у службовій комунікації створює новий вид документів, правовий статус яких залишається невизначеним. Ця проблема особливо актуальна для оборонного сектору, де комунікація може містити інформацію з обмеженим доступом. Відсутність чітких правових механізмів використання месенджерів у службовій комунікації створює ризики для інформаційної безпеки та ускладнює документування управлінських рішень.

Висновки.

У результаті проведеного дослідження встановлено, що чинна нормативно-правова база, яка регулює електронний документообіг у системі державного управління сектору оборони України, характеризується фрагментарністю та недостатньою адаптованістю до викликів, пов'язаних із впровадженням новітніх технологій, зокрема штучного інтелекту та блокчейну. Відсутність спеціального правового регулювання цих технологій створює ризики як для ефективності їх застосування, так і для інформаційної безпеки держави.

Аналіз міжнародного досвіду свідчить про активне формування правових рамок для застосування ШІ та блокчейну в секторі оборони, зокрема в системах електронного документообігу. При цьому особлива увага приділяється питанням сумісності систем, забезпечення балансу між ефективністю та безпекою, а також дотримання етичних принципів при використанні автоматизованих систем.

Для вдосконалення нормативно-правового забезпечення електронного документообігу в системі державного управління сектору оборони України запропоновано комплекс заходів, які включають розробку спеціального закону, внесення змін до чинних нормативно-правових актів, розробку галузевих стандартів та відомчих нормативних документів. Реалізація цих пропозицій дозволить створити правові передумови для ефективного та безпечного впровадження технологій ШІ та блокчейну в електронний документообіг сектору оборони держави.

Ключовими викликами у створенні ефективної нормативно-правової бази для інноваційних напрямків розвитку ЕДО сектору оборони залишаються:

– необхідність балансування між інноваційністю та безпекою;

– забезпечення гнучкості правового регулювання з урахуванням швидкого розвитку технологій;

– гармонізація національного законодавства зі стандартами НАТО та ЄС;

– розробка специфічних технічних стандартів та протоколів;

– підготовка фахівців з відповідними компетенціями.

Для ефективного впровадження ШІ в систему ЕДО сектору оборони необхідно розробити та прийняти нормативно-правові акти, які регулюватимуть:

– критерії та процедури валідації алгоритмів ШІ, які застосовуються в оборонному документообігу;

– межі автономності систем ШІ у прийнятті рішень різного рівня;

– питання відповідальності за рішення, прийняті з використанням ШІ;

– механізми контролю та аудиту систем ШІ;

– специфічні вимоги до безпеки та захисту даних при використанні ШІ в документообігу, що містить інформацію з обмеженим доступом.

Нормативно-правове забезпечення використання блокчейну в системі ЕДО сектору оборони повинно охоплювати:

– визначення юридичного статусу документів, що зберігаються у блокчейн-системах;

– регламентацію процедур верифікації та валідації транзакцій у блокчейні;

– стандарти для використання різних типів блокчейн-мереж (публічних, приватних,

гібридних) залежно від рівня секретності інформації;

– правила розподілу відповідальності між учасниками блокчейн-мережі;

– механізми інтеграції блокчейн-систем з існуючими системами ЕДО та іншими інформаційними системами.

Перспективними напрямками вдосконалення нормативно-правової бази є:

– розробка концепції правового забезпечення цифрової трансформації документообігу в секторі оборони;

– створення спеціалізованих нормативних актів щодо використання ШІ, блокчейну та месенджерів;

– впровадження регуляторних "пісочниць" для тестування інноваційних рішень;

– розробка галузевих стандартів та протоколів безпеки;

– внесення змін до існуючого законодавства для усунення правових колізій та прогалин.

Для ефективної та безпечної інтеграції месенджерів у систему ЕДО сектору оборони необхідно розробити нормативно-правову базу, яка визначатиме:

– типи інформації, що може передаватися через месенджери;

– вимоги до захисту інформації при використанні месенджерів (шифрування, автентифікація);

– порядок документування та архівування комунікацій через месенджери, що мають юридичне значення;

– процедури верифікації ідентичності користувачів месенджерів;

– регламентацію використання державних та комерційних месенджерів в оборонному секторі;

– порядок інтеграції месенджерів з офіційними системами ЕДО.

Перспективними напрямами подальших досліджень є розробка методичних підходів до оцінки правових ризиків впровадження новітніх технологій у системи електронного документообігу сектору оборони, а також дослідження особливостей правового регулювання застосування технологій квантових обчислень для забезпечення безпеки електронного документообігу в майбутньому.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Баранов, О. (2018). Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом. *Інформація і право,* 4, 46–70. Відновлено з http://nbuv.gov.ua/UJRN/Infpr_2018_4_7

Баранов, О., Швець, М., & Брижко, В. (2019). Електронне урядування в Україні: правові аспекти. *Інформація і право*, 2, 39–51.

Болдуєв, М. В., Болдуєва, О. В., & Лищенко, О. Г. (2024). Потенціал і проблеми запровадження електронного документообігу в Україні. *Ефективна економіка*, 4. https://doi.org/10.32702/2307-2105.2024.4.9

Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., & Толюпа, С. В. (2015). *Інформаційна та кібербезпека: соціотехнічний аспект* (В. Б. Толубко, ред.). Київ: ДУТ.

Величко, О. Ф., Гриб, Д. А., Демідов, Б. О., Коростельов, О. П., Кучеренко, Ю. Ф., Луханін, М. І., Чепков, І. Б., & Хмелевська, О. О. (2021). *Методологічні й системотехнічні аспекти інформаційного забезпечення управління системами військового призначення та діяльністю в оборонній сфері* (Б. О. Демідов & О. П. Коростельов, ред.). Київ: Видавничий дім "Стилос".

Верховна Рада України. (1994a). *Про державну таємницю* (Закон № 3855-XII). Відновлено з https://zakon.rada.gov.ua/laws/show/3855-12

Верховна Рада України. (1994b). *Про захист інформації в інформаційно-телекомунікаційних системах* (Закон № 80/94-ВР). Відновлено з https://zakon.rada.gov.ua/laws/show/80/94-вр

Верховна Рада України. (2003). *Про електронні документи та електронний документообіг* (Закон № 851-IV). Відновлено з https://zakon.rada.gov.ua/laws/show/851-15

Верховна Рада України. (2017). *Про електронні довірчі послуги* (Закон № 2155-VIII). Відновлено з https://zakon.rada.gov.ua/laws/show/2155-19

Верховна Рада України. (2018). *Про основи національної безпеки України* (Закон № 2469-VIII). Відновлено з https://zakon.rada.gov.ua/laws/show/2469-19

Верховна Рада України. (2021). *Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"* (Указ Президента № 447/2021). Відновлено з https://zakon.rada.gov.ua/laws/show/447/2021

Грицяк, Н., & Литвинова, Л. (2020). Електронне урядування: нормативно-правове забезпечення та особливості впровадження в Україні. *Публічне врядування в Україні: стан, виклики та перспективи розвитку*, 3, 121-134.

Ільєнко, А., Ільєнко, С., Яковенко, О., Галич, Є., & Павленко, В. (2024). Перспективи інтеграції штучного інтелекту в системи кібербезпеки. *Кібербезпека: освіта, наука, техніка*, 1(25), 318–329. https://doi.org/10.28925/2663-4023.2024.25.318329

Клименко, І., & Линьов, К. (2018). *Технології електронного урядування*. Київ: Центр навчальної літератури.

Ковач, О. В., & Ковач, Д. Л. (2023). Досвід країн ЄС щодо використання технології блокчейн (технології розподіленого реєстру) у публічному управлінні: порівняльно-правовий аналіз. *У Фінансова архітектоніка та сценарії конкурентних моделей розвитку: тези доповідей Міжнародної науково-практичної конференції* (с. 135–136). Харків: Державний біотехнологічний університет.

Кравченко, О. В., & Шаповал, О. Б. (2021). Блокчейн технології: стан та перспективи розвитку в Україні. *Вісник Хмельницького національного університету. Серія "Економічні науки",* 6(2), 267–272.

Кудь, А., Кучерявенко, М., & Смичок, Є. (2022). Ц*ифрові активи та їх правове регулювання у світі розвитку технології блокчейн*. Харків: Право.

Міністерство оборони України. (2020). *Про затвердження Порядку організації електронного документообігу в системі Міністерства оборони України* (Наказ № 256). Відновлено з https://www.mil.gov.ua/content/mou_orders/mou_2020/nm_256.pdf

Міністерство оборони України. (б.д.). *Особиста кібербезпека: паролі та месенджери*. https://mod.gov.ua/osobista-kiberbezpeka-paroli-ta-mesendzheri

Радутний, О. Є. (2017). *Criminal liability of the artificial intelligence. Problems of Legality*, 138, 132–141. https://doi.org/10.21564/2414-990x.138.105661

Спасітєлєва, С. О., & Бурячок, В. Л. (2018). Перспективи розвитку додатків блокчейн в Україні. *Кібербезпека: освіта, наука, техніка*, 1(1), 35–48. https://doi.org/10.28925/2663-4023.2018.1.3548

Чистоклетов, Л., & Обрембальський, С. (2024). Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. *Академічні візії,* 29. Відновлено з https://www.academy-vision.org/index.php/av/article/view/1141

High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. European Commission. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

NATO. (2021). *Summary of the NATO Artificial Intelligence Strategy*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_187617.htm

U.S. Department of Defense. (2020). *DoD adopts ethical principles for artificial intelligence.* Retrieved from https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

REFERENCES

Baranov, O. (2018). Internet rechey (IoT): Rehulyuvannya nadannya posluh robotamy zi shtuchnym intelektom [Internet of Things (IoT): Regulation of services provided by robots with artificial intelligence]. *Informatsiya i Pravo,* 4, 46–70. http://nbuv.gov.ua/UJRN/Infpr_2018_4_7

Baranov, O., Shvets, M., & Bryzhko, V. (2019). Elektronne uryaduvannya v Ukrayini: Pravovi aspekty [Electronic governance in Ukraine: Legal aspects]. *Informatsiya i Pravo*, 2, 39–51.

Bolduev, M. V., Boldueva, O. V., & Lyshchenko, O. H. (2024). Potentsial i problemy zaprovadzhennya elektronnogo dokumentoobigu v Ukrayini [Potential and problems of implementing electronic document management in Ukraine]. *Efektyvna Ekonomika*, 4. https://doi.org/10.32702/2307-2105.2024.4.9

Buryachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Tolyupa, S. V. (2015). *Informatsiyna ta kiberbezpeka: Sotsiotekhnichnyy aspekt [Information and cybersecurity: Sociotechnical aspect]* (V. B. Tolubko, Ed.). Kyiv: DUT.

Chystokletov, L., & Obrembalskyy, S. (2024). Osoblyvosti zabezpechennya informatsiynoyi bezpeky v umovakh rosiysko-ukrayinskoyi viyny [Features of ensuring information security during the Russian-Ukrainian war]. *Akademichni Viziyi*, 29. Retrieved from https://www.academy-vision.org/index.php/av/article/view/1141

Grytsyak, N., & Lytvynova, L. (2020). Elektronne uryaduvannya: Normatyvno-pravove zabezpechennya ta osoblyvosti vprovadzhennya v Ukrayini [Electronic governance: Legal framework and features of implementation in Ukraine]. *Publichne Vryaduvannya v Ukrayini: Stan, Vyklyky ta Perspektyvy Rozvytku,* 3, 121–134.

High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI.* European Commission. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Ilienko, A., Ilienko, S., Yakovenko, O., Halych, Ye., & Pavlenko, V. (2024). Perspektyvy intehratsiyi shtuchnoho intelektu v systemy kiberbezpeky [Prospects for integrating artificial intelligence into cybersecurity systems]. *explode: Osvita, Nauka, Tekhnika*, 1(25), 318–329. Retrieved from https://doi.org/10.28925/2663-4023.2024.25.318329

Klymenko, I., & Lynyov, K. (2018). *Tekhnolohiyi elektronnogo uryaduvannya [Electronic governance technologies].* Kyiv: Tsentr Navchalnoyi Literatury.

Kovach, O. V., & Kovach, D. L. (2023). Dosvid krayin YES shchodo vykorystannya tekhnolohiyi blokcheyn (tekhnolohiyi rozpodilenoho reyestru) u publichnomu upravlinni: Porivnyalno-pravovyy analiz [Experience of EU countries in using blockchain technology (distributed ledger technology) in public administration: Comparative legal analysis]. In *Finansova Arkhitektonika ta Stsenariyi Konkurentnykh Modeley Rozvytku: Tezy Dopovidey Mizhnarodnoyi Naukovo-Praktychnoyi Konferentsiyi* (pp. 135–136). Kharkiv: Derzhavnyy Biotekhnolohichnyy Universytet.

Kravchenko, O. V., & Shapoval, O. B. (2021). Blokcheyn tekhnolohiyi: Stan ta perspektyvy rozvytku v Ukrayini [Blockchain technologies: State and prospects of development in Ukraine]. *Visnyk Khmelnytskoho Natsionalnoho Universytetu. Seriya "Ekonomichni Nauky*", 6(2), 267–272.

Kud, A., Kucheryavenko, M., & Smychok, Ye. (2022). *Tsyfrovi aktyvy ta yikh pravove rehulyuvannya u sviti rozvytku tekhnolohiyi blokcheyn [Digital assets and their legal regulation in the context of blockchain technology development]*. Kharkiv: Pravo.

Ministry of Defense of Ukraine. (2020). *Pro zatverdzhennya Poryadku orhanizatsiyi elektronnogo dokumentoobigu v systemi Ministerstva oborony Ukrayiny [On approval of the procedure for organizing electronic document management in the system of the Ministry of Defense of Ukraine]* (Order No. 256). https://www.mil.gov.ua/content/mou_orders/mou_2020/nm_256.pdf

Ministry of Defense of Ukraine. (n.d.). *Osobysta kiberbezpeka: Paroli ta mesendzhery [Personal cybersecurity: Passwords and messengers]*. Retrieved from https://mod.gov.ua/osobista-kiberbezpeka-paroli-ta-mesendzheri

NATO. (2021). *Summary of the NATO Artificial Intelligence Strategy*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_187617.htm

Radutnyi, O. E. (2017). Criminal liability of the artificial intelligence. *Problems of Legality*, 138, 132–141. https://doi.org/10.21564/2414-990x.138.105661

Spasiteleva, S. O., & Buriachok, V. L. (2018). Perspektyvy rozvytku dodatkiv blokcheyn v Ukrayini [Prospects for the development of blockchain applications in Ukraine]. *explode: Osvita, Nauka, Tekhnika*, 1(1), 35–48. https://doi.org/10.28925/2663-4023.2018.1.3548

U.S. Department of Defense. (2020). *DoD adopts ethical principles for artificial intelligence*. Retrieved from https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

Velychko, O. F., Gryb, D. A., Demidov, B. O., Korostelov, O. P., Kucherenko, Yu. F., Lukhanin, M. I., Chepkov, I. B., & Khmelevska, O. O. (2021). *Metodolohichni y systemotekhnichni aspekty informatsiynoho zabezpechennya upravlinnya systemamy viyskovoho pryznachennya ta diyalnistyu v oboronniy sferi [Methodological and system-technical aspects of information support for the management of military systems and activities in the defense sector]* (B. O. Demidov & O. P. Korostelov, Eds.). Kyiv: Vydavnychyy Dim “Stylos”.

Verkhovna Rada of Ukraine. (1994a). *Pro derzhavnu tayemnytsyu [On state secrets]* (Law No. 3855-XII). Retrieved from https://zakon.rada.gov.ua/laws/show/3855-12

Verkhovna Rada of Ukraine. (1994b). *Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh [On protection of information in information and telecommunication systems]* (Law No. 80/94-VR). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр

Verkhovna Rada of Ukraine. (2003). *Pro elektronni dokumenty ta elektronnyy dokumentoobih [On electronic documents and electronic document management]* (Law No. 851-IV). Retrieved from https://zakon.rada.gov.ua/laws/show/851-15

Verkhovna Rada of Ukraine. (2017). *Pro elektronni dovirchi posluhy [On electronic trust services]* (Law No. 2155-VIII). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19

Verkhovna Rada of Ukraine. (2018). *Pro osnovy natsionalnoyi bezpeky Ukrayiny [On the fundamentals of national security of Ukraine]* (Law No. 2469-VIII). Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19

Verkhovna Rada of Ukraine. (2021). *Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku “Pro Stratehiyu kiberbezpeky Ukrayiny” [On the decision of the National Security and Defense Council of Ukraine of May 14, 2021 “On the Cybersecurity Strategy of Ukraine”]* (Presidential Decree No. 447/2021). Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021