Харківський національний університет імені В. Н. Каразіна
Міністерство освіти і науки України

Кваліфікаційна наукова праця
на правах рукопису

НЕСТЕРЕНКО ВІКТОР ОЛЕКСАНДРОВИЧ

УДК: 004.056.5:004.89:651.4/.9

ДИСЕРТАЦІЯ

ДЕРЖАВНІ МЕХАНІЗМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЕЛЕКТРОННОГО МІЖВІДОМЧОГО ДОКУМЕНТООБІГ У СФЕРИ ОБОРОНИ

Спеціальність 281 Публічне управління та адміністрування
(Галузь знань 28 Публічне управління та адміністрування)

Подається на здобуття наукового ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ В.О. Нестеренко

Науковий керівник:
ОРЛОВ Олександр Валентинович, доктор наук з державного управління, професор.

Харків – 2026

АНОТАЦІЯ

Нестеренко В.О. Державні механізми інформаційного забезпечення системи електронного міжвідомчого документообігу сфери оборони. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 – Публічне управління та адміністрування (галузь знань – 28 Публічне управління та адміністрування). – Харківський національний університет імені В. Н. Каразіна Міністерства освіти і науки України, Харків, 2026.

У дисертації 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 штучного інтелекту 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. Особливу увагу приділено питанням автоматизації процесів документообігу, протидії кібератакам та вдосконаленню механізмів прийняття рішень на основі штучного інтелекту, що забезпечує стійкість критичної інформаційної інфраструктури сектору оборони.

Обґрунтовано, що реалізація запропонованих заходів дозволить створити правові передумови для ефективного та безпечного впровадження технологій штучного інтелекту 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.

На виконання поставленої мети у представленій дисертації здійснено комплексну розробку теоретико-методологічних засад та сформульовано практичні рекомендації, спрямовані на створення та вдосконалення захищеної системи електронної взаємодії і міжвідомчого документообігу в органах державної влади України. Такий підхід забезпечує наукову обґрунтованість запропонованих рішень і враховує актуальні виклики цифрової трансформації державного управління.

У дисертації враховано контекст цифрової трансформації, виклики повоєнного відновлення та стратегічні орієнтири європейської інтеграції. Проведено аналіз міжнародного досвіду, охоплено нормативно-правові, організаційні й технологічні аспекти функціонування відповідних систем у провідних країнах. Обґрунтовано інтеграцію сучасних інноваційних технологій, зокрема штучного інтелекту, блокчейну, локальних великих мовних моделей та інструментів контейнеризації, як ключових чинників підвищення ефективності, автоматизації процесів, стійкості до кібератак та забезпечення інтероперабельності цифрових рішень у сфері публічного управління та електронного урядування, з акцентом на суб'єкти сектору безпеки та оборони України.

На основі проведеного дослідження, яке охоплює аналіз міжнародного досвіду, нормативно-правової бази, технологічних рішень і розробку практичних рекомендацій, сформульовано висновки, що структуровані за ключовими напрямами:

1. Порівняльний аналіз і адаптація міжнародного досвіду.

Моделі електронної взаємодії. Розроблена методологічна структура порівняльного аналізу за вісьмома критеріями (технологічна архітектура, безпека, інтероперабельність, масштабованість, правове забезпечення, організаційна координація, інноваційність, економічна ефективність) дозволила ідентифікувати резерви для вдосконалення української системи електронної взаємодії. Досвід країн ЄС (Естонія – X-Road, Нідерланди – Digikoppeling, Німеччина – IT-Grundschutz, Фінляндія – KEJO) та інших країн (Ізраїль, Данія, Австралія, Південна Корея) показує, що децентралізовані архітектури, стандартизовані API, цифрові ідентичності та багаторівневий захист є ключовими для ефективних систем електронної взаємодії.

Адаптація до українських реалій. Запропонована модель "Цифрового стрибка" інтегрує елементи естонської децентралізації, ізраїльського захисту критичної інфраструктури, данської цифрової інклюзії, австралійської міжрівневої координації та південнокорейських інновацій. Модель адаптовано до повоєнного контексту України, враховуючи обмежені ресурси, воєнні виклики та потреби європейської інтеграції.

Синергетичний ефект. Встановлено, що міжвідомча інтеграція через системи електронної взаємодії забезпечує синергетичний ефект у п'яти аспектах: підвищення ефективності управління, прозорості, зручності для громадян, стимулювання інновацій та конкурентоспроможності держави. Порівняльна таблиця ефектів демонструє нелінійні результати, що перевищують суму окремих покращень, особливо в умовах повоєнної відбудови.

2. Нормативно-правове забезпечення.

Фрагментарність законодавства. Аналіз чинної нормативно-правової бази України виявив фрагментарність, недостатню адаптацію до інноваційних технологій (штучний інтелект, блокчейн) і прогалини в регулюванні безпеки даних у секторі оборони [162]. Відсутність спеціальних стандартів для штучного інтелекту та блокчейну створює ризики для ефективності та безпеки.

Міжнародний досвід. У країнах НАТО та ЄС (Німеччина, Франція, Нідерланди) нормативна база поєднує загальні закони про електронний

документообіг із галузевими стандартами безпеки. Це забезпечує сумісність, гнучкість і баланс між інноваціями та захистом даних.

Пропозиції щодо вдосконалення. Запропоновано комплекс заходів, а саме: розроблення спеціального закону про електронний документообіг у секторі безпеки та оборони України, внесення відповідних змін до чинних актів, створення галузевих стандартів для штучного інтелекту та блокчейну, впровадження регуляторних "пісочниць" для тестування технологій. Рекомендується гармонізація з європейськими стандартами (NIS 2 Directive, GDPR) і НАТО для забезпечення інтероперабельності.

3. Технологічні рішення.

Концептуальна модель системи електронної взаємодії. Розроблено комплексну модель електронної взаємодії, яка синтезує шість підходів (технологічний, соціально-організаційний, функціональний, процесний, правовий, системний). Модель враховує повоєнні виклики, акцентуючи увагу на безпеці, адаптивності та інтероперабельності через сервісно-орієнтовану архітектуру (SOA), подібну до EIRA.

Інтеграція штучного інтелекту та блокчейну. Впровадження штучного інтелекту (зокрема локальних LLM, таких як Ollama, DeepSeek-R1) і блокчейну підвищує рівень автоматизації, достовірність і безпеку документообігу. Для забезпечення стійкості систем документообігу запропоновано використання нейромережевих моделей виявлення таргетованих атак на об'єкти критичної інфраструктури, що дозволяє завчасно ідентифікувати загрози та мінімізувати ризики компрометації даних. Інтеграція цих технологій сприяє вдосконаленню процесів прийняття рішень у сфері публічного управління. Технології NLP дозволяють структурувати дані, класифікувати документи та реагувати на запити, а блокчейн забезпечує цілісність і верифікацію. Контейнеризація (Docker Desktop) оптимізує розгортання систем, але потребує контрольованих середовищ для донавчання нейромережевих моделей.

Безпекові виклики. Ідентифіковано ризики штучного інтелекту (упередження, непередбачуваність) і блокчейну (юридичний статус документів,

інтеграція з існуючими системами). Запропоновано багаторівневу систему захисту: криптографія, багатофакторна автентифікація, моніторинг загроз, фізична сегментація мереж (за фінським досвідом).

Архітектура єдиної системи електронного міжвідомчого документообігу. Теоретичні моделі для електронного міжвідомчого документообігу у секторі оборони та безпеки України базуються на модульному принципі, федеративній інтеграції та "глибокій обороні". Запропоновано уніфікацію процесів, використання платформи «Трембіта» та впровадження хмарних технологій для масштабованості.

4. Перспективи подальших досліджень.

Інноваційні технології. Подальші дослідження мають зосередитися на потенціалі штучного інтелекту, блокчейну, квантових обчислень і обробки великих даних для посилення стійкості цифрової інфраструктури. Особлива увага приділена розробці спеціалізованих моделей штучного інтелекту для юридичних документів і гібридних систем із перевіркою людиною (Human-in-the-loop).

Соціально-економічні аспекти. Вивчення впливу цифрових трансформацій на внутрішньо переміщених осіб і маргіналізовані групи для забезпечення інклюзивності.

Глобальний внесок. Унікальний український досвід цифрової стійкості в умовах війни може стати основою для міжнародних стандартів захисту критичної інформаційної інфраструктури.

Таким чином успішне впровадження захищених систем електронної взаємодії та міжвідомчого документообігу в Україні вимагає комплексного підходу, що поєднує технологічні інновації, нормативно-правові реформи та організаційні зміни. Адаптація європейського досвіду, зокрема моделей Естонії, Німеччини, Фінляндії та Нідерландів, дозволить Україні подолати фрагментацію цифрової інфраструктури, підвищити стійкість до кіберзагроз і забезпечити інтероперабельність із європейськими системами. Запропонована модель «Цифрового стрибка» є стратегічним інструментом для повоєнної відбудови,

зміцнення національної стійкості та цифрової трансформації державного управління, зокрема в секторі безпеки й оборони України.

Ключові слова: державні механізми, публічне управління, електронний документообіг, штучний інтелект, блокчейн, кібербезпека, цифрова трансформація, нормативно-правове регулювання, інтероперабельність, об'єкт критичної інфраструктури, нейромережева модель, таргетована атака, прийняття рішень, електронне урядування, інформаційна безпека.

ABSTRACT

Nesterenko, V.O. State Mechanisms for Information Support of the Electronic Interagency Document Workflow System in the Defense Sector. – Qualification Scientific Work as a Manuscript.

Dissertation for the Degree of Doctor of Philosophy in Specialty 281 – Public Administration and Management (Field of Knowledge – 28 Public Administration and Management). – V.N. Karazin Kharkiv National University of the Ministry of Education and Science of Ukraine, Kharkiv, 2025.

The dissertation explores the legal and regulatory aspects of electronic document workflow within the state governance system of the national defense sector. It analyzes the current state of legal regulation in this field and identifies key gaps hindering the effective implementation of artificial intelligence and blockchain technologies in the document management systems of defense institutions.

The dissertation outlines pressing legal challenges associated with the introduction of artificial intelligence and blockchain in the defense sector’s electronic document workflow, including:

- the absence of a legal status definition for documents generated using AI algorithms;
- unclear mechanisms for distributing responsibility when using automated decision-making systems;

- a lack of specific data protection requirements for distributed ledgers and AI systems;
- the unresolved interoperability issues among electronic document systems across defense structures.

Particular attention is given to automation of document workflow processes, countermeasures against cyberattacks, and improvement of AI-based decision-making mechanisms, which ensure the resilience of critical information infrastructure in the defense sector.

It is argued that the implementation of the proposed measures will establish the legal framework necessary for the effective and secure adoption of AI and blockchain technologies in the defense sector's electronic document workflow. This will enhance the efficiency of administrative processes and ensure an adequate level of information protection. The dissertation identifies promising research directions related to the development of methodological approaches for legal risk assessment in the implementation of emerging technologies in defense document systems and examines the specifics of legal regulation for the use of quantum computing technologies in securing future electronic workflows.

To achieve the set goal, the dissertation offers a comprehensive development of theoretical and methodological principles and formulates practical recommendations aimed at creating and improving a secure electronic interagency communication and document management system within the public authorities of Ukraine. This approach provides scientific justification for the proposed solutions and considers the current challenges of digital transformation in public administration.

The research incorporates the context of digital transformation, post-war recovery challenges, and the strategic goals of European integration. It includes analysis of international practices and examines legal, organizational, and technological aspects of similar systems in leading countries. The integration of advanced technologies such as AI, blockchain, localized large language models, and containerization tools is justified as key factors for improving efficiency, cybersecurity, information security, and interoperability of digital solutions in public administration

and e-governance, with a focus on protecting critical infrastructure facilities. To ensure the resilience of document workflow systems, the dissertation proposes the use of neural network models for detecting targeted attacks on critical infrastructure facilities, enabling early threat identification and minimization of data compromise risks. Integration of these technologies contributes to improving decision-making processes in public administration.

Based on the conducted research, which covers international experience, legal frameworks, technological solutions, and the development of practical recommendations, the dissertation presents conclusions structured across key areas:

1. Comparative Analysis and Adaptation of International Experience.

Models of Electronic Interaction. A methodological framework for comparative analysis was developed based on eight criteria (technological architecture, security, interoperability, scalability, legal compliance, organizational coordination, innovation, economic efficiency), identifying improvement opportunities for Ukraine's electronic interaction system. Case studies include the EU (Estonia – X-Road, Netherlands – Digikoppeling, Germany – IT-Grundschutz, Finland – KEJO) and non-EU countries (Israel, Denmark, Australia, South Korea), revealing that decentralized architectures, standardized APIs, digital identities, and multi-layered security are key to success.

Adaptation to Ukrainian Realities. The proposed "Digital Leap" model combines elements from Estonian decentralization, Israeli critical infrastructure protection, Danish digital inclusion, Australian inter-level coordination, and South Korean innovation. This model is tailored to Ukraine's post-war context, accounting for limited resources, wartime challenges, and European integration needs.

Synergistic Effect. Interagency integration through electronic systems provides synergy in five areas: governance efficiency, transparency, citizen convenience, innovation stimulation, and national competitiveness. A comparative effect table demonstrates nonlinear outcomes exceeding the sum of individual improvements, especially in post-conflict reconstruction.

2. Legal and Regulatory Framework.

Fragmentation of Legislation. Analysis of Ukraine's current legal framework reveals fragmentation, insufficient adaptation to emerging technologies (AI, blockchain), and gaps in data security regulation within the defense sector. The absence of specific standards for AI and blockchain poses effectiveness and security risks.

International Experience. In NATO and EU countries (e.g., Germany, France, Netherlands), the legal framework combines general laws on electronic document management with sector-specific security standards. This ensures compatibility, flexibility, and a balance between innovation and data protection.

Recommendations for Improvement. Proposed measures include: drafting a specialized law on electronic document workflow in Ukraine's security and defense sector, amending existing acts, creating industry-specific standards for AI and blockchain, and implementing regulatory "sandboxes" for technology testing. Harmonization with EU (NIS 2 Directive, GDPR) and NATO standards is advised to ensure interoperability.

3. Technological Solutions.

Conceptual Model for Electronic Interaction. A comprehensive model was developed, integrating six approaches (technological, socio-organizational, functional, process-based, legal, and systemic). It addresses post-war challenges with a focus on security, adaptability, and interoperability, through a service-oriented architecture (SOA) similar to EIRA.

Integration of AI and Blockchain. The adoption of AI (including local LLMs such as Ollama, DeepSeek-R1) and blockchain enhances process automation, authenticity, and security in document workflows, while optimizing managerial decision-making under conditions of cyberattack countermeasures. NLP technologies support data structuring, document classification, and response automation, while blockchain ensures integrity and verification. Containerization (e.g., Docker Desktop) optimizes system deployment but requires controlled environments for model fine-tuning.

Security Challenges. Risks of AI (bias, unpredictability) and blockchain (legal status of documents, integration with legacy systems) were identified. A multi-level

protection system is proposed: cryptography, multi-factor authentication, threat monitoring, and physical network segmentation (following Finnish practices).

Architecture of a Unified Interagency Electronic Document Workflow System. Theoretical models for interagency electronic document workflow in Ukraine's security and defense sector are based on modularity, federated integration, and "defense in depth." Standardization of processes, the use of the «Trembita» platform, and cloud technologies are proposed to ensure scalability.

4. Future Research Perspectives.

Innovative Technologies. Future studies should explore AI, blockchain, quantum computing, and big data analytics to enhance the resilience of digital infrastructure. Special attention should be paid to developing specialized AI models for legal documents and hybrid human-in-the-loop systems.

Socio-Economic Aspects. Further research is needed on the impact of digital transformation on internally displaced persons and marginalized groups to ensure inclusivity.

Global Contribution. Ukraine's unique experience in maintaining digital resilience during wartime may serve as a foundation for international standards on critical information infrastructure protection.

Conclusion. The successful implementation of secure electronic interaction and interagency document management systems in Ukraine requires a comprehensive approach combining technological innovation, legal reform, and organizational change. Adapting European models – especially from Estonia, Germany, Finland, and the Netherlands – will help Ukraine overcome digital infrastructure fragmentation, increase cyber resilience, and ensure interoperability with European systems. The proposed "Digital Leap" model serves as a strategic tool for post-war recovery, national resilience strengthening, and the digital transformation of public administration, particularly in the security and defense sector.

Keywords: state mechanisms, public administration, electronic document workflow, artificial intelligence, blockchain, cybersecurity, digital transformation,

legal and regulatory framework, interoperability, critical infrastructure facility, neural network model, targeted attack, decision-making, e-governance, information security.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. Нестеренко В. О. Огляд створення та впровадження захищеної системи електронного документообігу Збройних Сил України // Електронне наукове видання "Публічне адміністрування та національна безпека". — 2020. — №1. *https://doi.org/10.25313/2617-572X-2020-1-5580*.

2. Орлов, О., Живило, Є., & Нестеренко, В. (2025). Нормативно-правові аспекти електронного документообігу в системі державного управління сектору оборони держави. Аспекти публічного управління, 13 (1), 106-113. https://doi.org/10.15421/152512.

3. Орлов, О., & Нестеренко, В. (2025). Використання штучного інтелекту в документообігу: перспективи та виклики. State Formation. No. 1 (37)/2025. https://periodicals.karazin.ua/db/article/view/27245/24168.

4. Орлов, О., Живило, Є., & Нестеренко, В. (2025). Принципові напрями розгортання захищеного документообігу на платформах штучного інтелекту. Theory and Practice of Public Administration 1 (80)/2025. http://doi.org/10.26565/1727-6667-2025-1-02.

5. Орлов, О., Живило, Ю., та Нестеренко, В. (2025). Електронна взаємодія органів державної влади в контексті цифрової трансформації в повоєнній Україні: де шукати резерви вдосконалення?. Актуальні проблеми державного управління , 1 (66), 273-296. https://doi.org/10.26565/1684-8489-2025-1-13.

6. Нестеренко В.О., Аналіз досвіду європейської спільноти держав із запровадження захищеної системи електронної взаємодії в органах державної влади. Суспільство та національні інтереси № 8(16) 2025 с.719. https://doi.org/10.52058/3041-1572-2025-8(16)

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Нестеренко В.О. Порядок здійснення діловодства та документування управлінської інформації в електронній формі в Міністерстві оборони України та Генеральному штабі Збройних Сил України. Публічне управління XXI століття: портал можливостей: зб. тез XX Міжнар. наук. конгресу. – Вид-во ХарРІ НАДУ “Магістр”, 2020. – С. 467-470.

8. Нестеренко В. О. Напрями організації взаємодії складових сектору безпеки і оборони держави в системі електронного міжвідомчого документообігу. Публічне у правління XXI століття: погляд у майбутнє: зб. тез

XXI Міжнар. наук. конгресу. – Вид-во ХарРІ НАДУ “Магістр”, 2021. – С.494-497.

9. Нестеренко В.О., Нагорний О.А. Теоретичні засади Державної політики щодо створення, впровадження та функціонування захищеної системи електронного міжвідомчого документообігу сфери оборони Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: тези доповідей XXIX міжнародної науково-практичної конференції MicroCAD-2021, 18-20 травня 2021р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ «ХПІ».с. 145.

10. Нестеренко В.О., Перспективи та виклики впровадження захищеного ШІ-орієнтованого СЕДО в Збройних Силах України. Публічне управління XXI століття: основні виклики післявоєнної відбудови : зб. наук. матер. XXV Міжнар. наук. конгресу [Електронний ресурс]. – Харків : ХНУ імені В. Н. Каразіна, 2025. (PDF 716 с.) с. 315 ISBN 978-966-285-798-6. URI https://ekhnuir.karazin.ua/handle/123456789/22470.

Акти впровадження результатів:

1. АКТ впровадження результатів наукових досліджень пов’язаних з супроводженням захищеної системи електронного документообігу Міністерства оборони України та Збройних сил України в Головному управлінні підготовки Збройних Сил України від 15.01.2020 №348/121.

2. АКТ впровадження результатів дисертаційного дослідження під час розробки КСЗІ (комплексної системи захисту інформації) захищеної СЕДО (системи електронного документообігу) та розробки Порядку введення в експлуатацію модулів КСЗІ АРМ (автоматизованих робочих місць) захищеної СЕДО 33102567.62022.001.И2.2 в Головному управлінні зв’язку та інформаційних систем Генерального штабу Збройних Сил України від 22.01.2020 №308/51/137.

3. АКТ впровадження результатів виконаної дослідно-конструкторської роботи по ДКР шифр “СЕДО-М” в Воєнно-науковому управлінні Генерального штабу Збройних Сил України від 19.05.2020 №323/1097.

4. Витяг із протоколу засідання методичної ради Центру оперативних стандартів і методики підготовки Збройних Сил України щодо ведення результатів проведених наукових досліджень пов’язаних з супроводженням захищеної СЕДО-М, в частині що стосується розміщення військових публікацій з усіх сфер військової публікації Генерального штабу Збройних Сил України та Збройних Сил України від 23.02.2020 №1.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Стрімкий розвиток цифрових технологій і зростання складності глобальних викликів у сфері безпеки підкреслюють важливість створення захищених і ефективних систем електронного міжвідомчого документообігу, особливо у сфері оборони. В Україні цифрова трансформація, необхідність повоєнного відновлення та європейська інтеграція актуалізують потребу в удосконаленні державних механізмів забезпечення інформаційної безпеки таких систем. Війна в Україні виявила вразливості критичної інформаційної інфраструктури: за даними Державної служби спеціального зв’язку та захисту інформації України, кількість кібератак на системи державного управління зросла на 40% у 2022–2024 роках. Особливу увагу приділено захисту об'єктів критичної інфраструктури сектору оборони від таргетованих атак із застосуванням нейромережевих моделей виявлення загроз, що забезпечує стійкість систем електронного документообігу в умовах кібербезпеки та інформаційної безпеки. Водночас стратегія цифровізації Європейського Союзу та стандарти кібербезпеки НАТО вимагають впровадження інтероперабельних, безпечних та інноваційних рішень у державному управлінні, зокрема в оборонному секторі.

Інтеграція інноваційних технологій, таких як штучний інтелект (ШІ), блокчейн, нейромережеві моделі, локальні великі мовні моделі (LLM) і контейнеризація, відкриває нові можливості для підвищення ефективності, кібербезпеки, інформаційної безпеки та інтероперабельності систем електронного документообігу в контексті цифрової трансформації та електронного урядування. Проте відсутність комплексних теоретичних засад, уніфікованих нормативно-правових підходів і практичних методологій для впровадження цих технологій в оборонному секторі України створює значні виклики. Наявні системи, такі як Єдина система електронного документообігу (ЄСЕМД), стикаються з проблемами масштабованості, кібербезпеки та відповідності стандартам ЄС і НАТО. Це зумовлює потребу в системному дослідженні державних механізмів забезпечення захищеної електронної

взаємодії між відомствами, особливо в оборонній сфері, де конфіденційність і стійкість є критично важливими. Актуальність дослідження посилюється необхідністю подолання правових, етичних і технічних бар'єрів на шляху впровадження інноваційних технологій, забезпечення інклюзивності та відповідності міжнародним нормам у контексті повоєнного відновлення.

Стан наукової розробки проблеми. Проблема інформаційного забезпечення систем електронного міжвідомчого документообігу в державному управлінні активно досліджується як в Україні, так і на міжнародному рівні. Зарубіжні вчені, такі як П. Данліві та Х. Маргеттс, розробили концепцію цифрового урядування (Digital Era Governance), яка підкреслює необхідність інтеграції технологій для підвищення ефективності публічної адміністрації. Дослідження Дж. Хартлі та М. Шваба акцентують на синергетичних ефектах цифрової взаємодії, але не пропонують конкретних моделей для країн у кризових умовах. У контексті оборони, праці НАТО (зокрема, стандарти STANAG) та європейських дослідників (наприклад, проекти DESI та eIDAS) висвітлюють питання кібербезпеки та інтероперабельності, однак їхній фокус обмежується розвиненими економіками.

В Україні дослідження електронного документообігу представлені працями О. Карпенка, В. Дрешпака та Ю. Журавльової, які аналізують нормативно-правові аспекти цифровізації державного управління. Окремі роботи, зокрема О. Литвиненка, розглядають кібербезпеку в оборонному секторі, але не охоплюють інтеграцію ШІ, блокчейну чи локальних великих мовних моделей. Проблеми ЄСЕМД частково досліджені в працях Київської школи економіки, де наголошується на технічних і організаційних обмеженнях системи. Водночас комплексні дослідження, що поєднують теоретичні, правові та технологічні аспекти впровадження інноваційних технологій у захищений документообіг оборонного сектору в умовах війни та повоєнного відновлення, залишаються недостатньо розробленими. Це створює науковий пробіл, який дане дослідження прагне заповнити шляхом систематизації міжнародного

досвіду, аналізу нормативної бази та розробки нової архітектури документообігу.

Зв'язок роботи з науковими програмами, планами, темами. Тему дисертації визначено відповідно до основних положень Законів України "Про захист інформації в інформаційно-телекомунікаційних системах" затверджений Указом Президента України від 5 липня 1994 року № 80/94-ВР зі змінами, "Про електронні документи та електронний документообіг" затверджений Указом Президента України від 22.05.2003 року № 851-IV зі змінами, "Про електронну ідентифікацію та електронні довірчі послуги" затверджений Указом Президента України 18.12.2024 року від № 2155-VIII, Постанови Кабінету Міністрів України № 606 від 08.09.2016 року "Деякі питання електронної взаємодії електронних інформаційних ресурсів", № 1142 від 04.10.2024 року "Деякі питання створення та функціонування електронної системи", № 1411 від 05.12.2024 року "Про реалізацію експериментального проєкту", наказу Міністерства юстиції та Міністерства фінансів № 2040/5/327 від 05.07.2024 року який визначає порядок електронної інформаційної взаємодії між Єдиним державним реєстром юридичних осіб, фізичних осіб – підприємців та громадських формувань і інформаційними системами Державної податкової служби України, наказів Міністерства цифрової трансформації та Адміністрації Держспецзв'язку які регламентують порядок ведення реєстру сертифікатів відкритих ключів, а також стандарти та технічні специфікації для засобів криптографічного захисту інформації. ca.gp.gov.ua.

Дисертаційну роботу виконано на кафедрі публічної політики навчально-наукового інституту «Інститут державного управління» Харківського національного університету імені В. Н. Каразіна. Результати дисертаційного дослідження були розроблені та реалізовані у відповідності до тематик дослідно-конструкторських робіт та наукових досліджень пов'язаних з супроводженням захищеної системи електронного документообігу сектору оборони та безпеки (Додаток):

– Центральний науково-дослідний інститут Збройних Сил України та

Науковий центр зв’язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут (м. Київ). В дослідно-конструкторській роботі шифр “СЕДО-М”, особистий внесок – обґрунтовано організацію формування єдиного захищеного інформаційного середовища електронних документів органів військового управління, установ, військових частин Збройних Сил України та інших складових сил оборони держави. Удосконалено спеціальне програмне забезпечення захищеної СЕДО, шляхом розширення їх функціональних можливостей. Сформульовано порядок обробки інформації з обмеженим доступом у захищеній СЕДО, а також визначено склад та технічні характеристики захищеної СЕДО.

– Головне управління зв’язку та інформаційних систем Генерального штабу Збройних Сил України (м. Київ). В ході супроводження дослідно-конструкторської роботи шифр “СЕДО-М”, особистий внесок – визначено порядок створення та функціонування, введення в експлуатацію модулів КСЗІ АРМ захищеної СЕДО призначених для використання в структурних підрозділах органів військового управління МО України, ГШ ЗС України, а також порядок здійснення електронної взаємодії між органами державної влади.

– Головне управління підготовки Збройних Сил України (м. Київ). В ході супроводження захищеної “СЕДО” Міністерства оборони України та Збройних сил України , особистий внесок – розроблені навчальні план-програми для здійснення підготовки на курсах підвищення кваліфікації керівників та спеціалістів структурних підрозділів Міністерства оборони України, Генерального штабу Збройних Сил України, органів військового управління, військових частин та установ Збройних Сил України (військовослужбовці, державні службовці третьої-сьомої категорій та особи, призначені (зараховані до кадрового резерву для призначення) на відповідні посади).

– Центр оперативних стандартів і методик підготовки Збройних Сил України (м. Житомир). В ході супроводження захищеної “СЕДО” Міністерства оборони України та Збройних сил України , особистий внесок – апробовано Методику перевірки функціональних можливостей оновленого СПЗ захищеної

“СЕДО” (за окремими складовими). Визначено алгоритм та порядок здійснення реєстрації з наданням відповідного позначення проектам військових публікацій та розміщенням в захищеному СЕДО затверджених (або введених в дію) військових публікацій (керівних документів, навчально-методичних матеріалів) за всіма сферами військової діяльності Генерального штабу та Збройних Сил України.

Метою дослідження є розробка державних механізмів інформаційного забезпечення для створення та вдосконалення захищеної системи електронного документообігу в органах публічного управління України в умовах цифрової трансформації, електронного урядування та європейської інтеграції. Дослідження спрямоване на оптимізацію процесів прийняття рішень та забезпечення кібербезпеки об'єктів критичної інфраструктури, систематизацію міжнародного досвіду, аналіз нормативно-правових і технологічних аспектів, а також обґрунтування підходів до інтеграції інноваційних технологій (штучного інтелекту, блокчейну, локальних великих мовних моделей і контейнеризації) для забезпечення ефективності, безпеки та інтероперабельності систем у секторі державного управління, зокрема безпеки й оборони.

Для досягнення поставленої мети визначено такі **завдання**:

Провести порівняльний аналіз показників електронної взаємодії та цифрової трансформації в Україні та країнах ЄС і НАТО для виявлення резервів покращення.

Систематизувати досвід країн ЄС у впровадженні захищених систем електронної взаємодії (СЕВ), включаючи нормативно-правову базу, технологічні рішення та організаційні механізми.

Дослідити правове регулювання та практичні підходи до застосування інноваційних технологій (ШІ, блокчейн) у документообігу військових відомств країн-членів НАТО.

Проаналізувати чинну нормативно-правову базу, що регулює електронний документообіг у системі державного управління, зокрема в секторі оборони.

Визначити правові проблеми, колізії та етичні аспекти, пов’язані з впровадженням технологій ШІ і блокчейну в електронний документообіг.

Розробити пропозиції щодо вдосконалення нормативно-правового забезпечення для інтеграції інноваційних технологій у захищені системи документообігу.

Дослідити синергетичний ефект від електронної взаємодії органів державної влади та розробити методологічну модель його досягнення в умовах обмежених ресурсів і повоєнного відновлення.

Проаналізувати сучасні науково-технічні підходи до використання ШІ, зокрема локально розгорнутих великих мовних моделей, а також технологій контейнеризації на основі віртуалізованих середовищ для розгортання у системах електронного документообігу.

Розробити концептуальну модель багаторівневої архітектури захищеного документообігу на основі локальних великих мовних моделей і контейнеризованої інфраструктури.

Оцінити технічні, функціональні та безпекові аспекти проекту ЄСЕМД, включаючи вимоги до архітектури, механізми захисту інформації та виклики інтеграції.

Визначити ключові напрями вдосконалення системи електронної взаємодії з урахуванням повоєнного періоду, європейської інтеграції, кібербезпеки та захисту критичної інформаційної інфраструктури.

Ідентифікувати безпекові ризики, пов’язані з використанням ШІ та локальних великих мовних моделей у документообігу, і запропонувати методологію їх мінімізації.

Сформулювати практичні рекомендації щодо розгортання та налаштування захищених систем документообігу на базі ШІ та блокчейну.

Обґрунтувати напрями удосконалення ЄСЕМД, включаючи технічні, безпекові та організаційні аспекти, і оцінити перспективи впровадження змін.

Визначити перспективні напрями подальших досліджень у галузі застосування інноваційних технологій для захищеного документообігу.

Об’єктом дослідження є механізми інформаційного забезпечення державного управління України.

Предметом дослідження є державні механізми інформаційного забезпечення системи електронного міжвідомчого документообігу сфери оборони.

Методи дослідження. У дослідженні застосовується міждисциплінарний методологічний підхід, який поєднує якісні, кількісні та моделювальні методи для аналізу й удосконалення захищених систем електронного документообігу. Використовуються такі методи:

Порівняльний аналіз. Проведено бенчмаркінг показників електронної взаємодії та цифрової трансформації в Україні, країнах ЄС і НАТО для виявлення найкращих практик і резервів покращення. Проаналізовано нормативно-правові бази, технологічні рішення та організаційні механізми в країнах із розвиненим цифровим урядуванням, таких як Естонія та Фінляндія.

Нормативно-правовий аналіз. Систематизовано чинну нормативно-правову базу України, що регулює електронний документообіг у державному управлінні, зокрема в оборонному секторі, для виявлення правових прогалин, колізій та етичних аспектів, пов’язаних із застосуванням ШІ та блокчейну.

Аналіз витрат і вигод. Оцінено економічні та операційні ефекти від інтеграції інноваційних технологій у системи документообігу з урахуванням обмежених ресурсів у повоєнний період.

Сценарне моделювання. Розроблено прогнозні моделі для оцінки синергетичних ефектів електронної міжвідомчої взаємодії та визначення оптимальних конфігурацій захищених архітектур документообігу.

Системний аналіз. Досліджено технічні, функціональні та безпекові аспекти ЄСЕМД, включаючи вимоги до архітектури, механізми захисту інформації та виклики інтеграції.

Кейс-аналіз. Проведено поглиблене вивчення міжнародного досвіду (зокрема, застосування ШІ у документообігу військових відомств НАТО та блокчейн-ініціатив у цифровому урядуванні ЄС) для адаптації рішень до умов України.

Технологічне експериментування. Виконано практичну оцінку інструментів на основі ШІ і платформ контейнеризації для розробки та тестування концептуальної багаторівневої архітектури документообігу.

Експертні опитування та інтерв'ю. Зібрано якісні дані від представників державних органів, оборонного сектору та ІТ-фахівців для валідації запропонованих моделей і рекомендацій.

Цей комплексний підхід забезпечує всебічний аналіз теоретичних, правових і технологічних аспектів, що дозволяє розробити обґрунтовані рекомендації для вдосконалення систем документообігу в оборонному секторі України.

Наукова новизна. Наукова новизна дослідження полягає в розробці комплексного підходу до створення державних механізмів інформаційного забезпечення захищених систем електронного міжвідомчого документообігу в оборонному секторі України з урахуванням інноваційних технологій і контексту повоєнного відновлення. Основні елементи новизни, що відповідають завданням дослідження, включають:

Вперше:

– розроблено концептуальну багаторівневу архітектуру захищеного електронного документообігу в системі міжвідомчої взаємодії сфери оборони, що базується на технологіях штучного інтелекту. Особливістю запропонованої архітектури є інтеграція локально розгорнутих великих мовних моделей, що дозволяє забезпечити автономність, стійкість до зовнішніх впливів та відповідність вимогам інформаційної безпеки державного рівня. Архітектура розроблена з урахуванням специфіки оборонного сектору, де критично важливими є такі чинники, як захист державної таємниці, стійкість до кібератак, підтримка автономного функціонування в умовах обмеженого доступу до зовнішніх мереж, а також можливість інтеграції з уже існуючими міжвідомчими платформами. Таким чином, запропонована архітектура створює основу для побудови сучасної системи електронного документообігу у сфері оборони, що відповідає вимогам національної безпеки, сприяє посиленню координації між

суб’єктами сектору безпеки і оборони та забезпечує високий рівень інституційної надійності в процесах прийняття управлінських рішень.

– сформульовано практичні рекомендації щодо розгортання та налаштування систем захищеного електронного документообігу в межах міжвідомчої взаємодії сфери оборони із застосуванням технологій локального розміщення програмних компонентів, зокрема моделей штучного інтелекту великого масштабу. Запропоновано та обґрунтовано застосування технологічного підходу, що базується на розгортанні компонентів штучного інтелекту в ізольованому середовищі з використанням контейнерних платформ. Особлива увага приділена питанням міжвідомчої сумісності, що дозволяє інтегрувати запропоновані рішення у загальнодержавну систему документообігу із збереженням цілісності, правомірності та секретності обміну інформацією. Вказані практичні заходи орієнтовані на впровадження інноваційних технологій у національні механізми цифрового управління оборонною сферою та створюють основу для ефективної трансформації наявних інформаційних систем із урахуванням принципів стійкості, оперативності й безперервності. Таким чином, розроблені рекомендації формують стратегічно важливу складову державної політики у сфері інформаційного забезпечення безпеки та оборони, сприяючи підвищенню технологічної самодостатності, інформаційного суверенітету та кіберстійкості національного оборонного простору.

Удосконалено:

– методологію оцінки синергетичних ефектів електронної взаємодії державних органів у системі міжвідомчого документообігу, що функціонує в межах сектора безпеки й оборони. Запропонована методологія враховує специфіку повоєнного контексту, зокрема високий рівень вимог до інформаційної безпеки, необхідність оперативного прийняття рішень, підвищену динаміку міжвідомчої координації, а також обмеженість матеріально-технічних і кадрових ресурсів у процесі відновлення державного управління. Таким чином, удосконалена методологія дозволяє не лише кількісно оцінювати ефективність впровадження електронного документообігу у сфері оборони, а й формулювати

стратегічні орієнтири для побудови національної системи електронної взаємодії державних органів у повоєнний період, забезпечуючи її відповідність принципам інформаційної безпеки, оперативності та міжвідомчої узгодженості.

Дістали подальшого розвитку головні напрями, що забезпечують зміцнення національних механізмів електронного міжвідомчого документообігу в оборонній сфері, з урахуванням викликів воєнного та повоєнного періодів, міжнародних стандартів, а також зростаючої ролі штучного інтелекту та децентралізованих технологій:

– нормативно-правові підходи до інтеграції штучного інтелекту та технології розподіленого реєстру (блокчейн) у систему електронного документообігу вдосконалено шляхом розробки пропозицій щодо усунення чинних правових колізій, мінімізації етичних ризиків і забезпечення відповідності правовим, технічним та етичним стандартам Європейського Союзу та Організації Північноатлантичного договору. Сформовано напрямки гармонізації національного законодавства з міжнародними нормами у сфері регулювання цифрового суверенітету та кібербезпеки.

– дослідження безпекових ризиків, пов’язаних із впровадженням штучного інтелекту та локалізованих великих мовних моделей у процесах автоматизованого документообігу, поглиблено завдяки розробці спеціалізованої методології оцінки та мінімізації загроз. Методологія враховує динаміку кіберзагроз, властиву як активній фазі воєнного протистояння, так і періоду постконфліктного відновлення, зокрема ризики несанкціонованого доступу, маніпуляції даними, втрати цілісності або ідентичності документів.

– напрями вдосконалення єдиної системи електронного міжвідомчого документообігу шляхом комплексного аналізу технічних, організаційних та безпекових аспектів її функціонування. Запропоновано концепцію розширення системи на основі гнучкої архітектури, яка підтримує інтероперабельність між різними органами державної влади, модульність, захищений обмін інформацією, адаптацію до нових типів загроз, а також впровадження інноваційних

технологій, зокрема, інтелектуальних агентів, динамічного маршрутизаційного планування, та криптографічних протоколів нового покоління.

Практичне значення одержаних результатів полягає у тому, що розроблені науково-теоретичні положення, узагальнення та методико-прикладні рекомендації можуть бути використані органами публічної влади для формування та реалізації ефективних механізмів інформаційного забезпечення в умовах сучасних безпекових викликів, а також для створення інституцій оновленої системи публічного управління, орієнтованої на цифрову трансформацію та національні інтереси у сфері оборони.

В цілому, результати дослідження сприяють практичному посиленню спроможностей держави у сфері інформаційної взаємодії органів влади, забезпечуючи надійне функціонування критично важливих інформаційних систем навіть в умовах високої невизначеності та деструктивних впливів.

Апробація результатів дисертації. Результати дисертаційного дослідження оприлюднені на міжнародних та всеукраїнських науково-практичних конференціях, форумах, конгресах, на засіданнях круглих столів. Зокрема, апробація проходила на XX міжнародному науковому конгресі: «Публічне управління XXI століття: портал можливостей» (м. Харків, 2020 р.), XXI міжнародному науковому конгресі: «Публічне управління XXI століття: погляд у майбутнє» (м. Харків, 2021 р.), XXIX міжнародній науково-практичній конференції MicroCAD-2021 «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» (м. Харків, 2021 р.), XXV міжнародному науковому конгресі «Публічне управління XXI століття: основні виклики післявоєнної відбудови» (м. Харків, 2025 р.)

Публікації. Основні положення дисертації опубліковано у 9 наукових працях загальним обсягом 3,29 авторських аркушів, зокрема у 5 статтях у фахових виданнях з державного управління загальним обсягом 3,15 авторських аркушів, з яких 2,82 авт. арк. належать дисертанту, у 4 тезах доповідей у збірниках конференцій загальним обсягом 0,47 авторських аркуші.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, із 10 підрозділами, висновків, списку використаних джерел і додатків.

Перший розділ “Запровадження електронної взаємодії органів державної влади в умовах розвитку електронного урядування: зарубіжний і вітчизняний досвід” присвячено обґрунтуванню теоретико-методологічних засад електронної взаємодії органів державної влади в умовах цифрової трансформації державного управління. Сформовано системне уявлення про сучасні підходи до запровадження електронного міжвідомчого документообігу, зокрема в оборонній сфері. У межах цього розділу здійснено комплексне дослідження фундаментальних понять і категорій, що визначають суть електронної взаємодії в публічному управлінні, її роль у забезпеченні ефективності, прозорості, безперервності та безпеки управлінських процесів. Розділ систематизує наукові підходи до розуміння електронної взаємодії, узагальнює базові визначення, принципи, функції та компоненти таких систем у контексті української цифрової трансформації.

Метою другого розділу “Сучасні підходи до формування механізмів інформаційного забезпечення системи єдиного захищеного інформаційного середовища електронних документів складових сектору оборони держави” є теоретико-прикладне обґрунтування сучасних підходів до формування ефективних механізмів інформаційного забезпечення єдиного захищеного інформаційного середовища електронних документів в межах сектору оборони держави. У розділі розглядаються ключові аспекти нормативно-правового, технологічного та організаційного характеру, які впливають на розвиток безпечного документообігу між складовими національного оборонного сектору. Таким чином, даний розділ виконує прикладну функцію, спрямовану на поєднання теоретичних підходів і практичних рішень у сфері формування надійної, технологічно стійкої та нормативно врегульованої системи інформаційного забезпечення електронного документообігу в секторі безпеки й оборони України. Отримані результати створюють основу для розробки цілісної

моделі державної політики та механізмів її реалізації, що будуть подані у наступному розділі дисертаційного дослідження.

Призначення третього розділу “Напрями розвитку та удосконалення електронного міжвідомчого документообігу сфери оборони” полягає у розробці стратегічних, організаційно-технічних та нормативно-правових напрямів розвитку та удосконалення системи електронного міжвідомчого документообігу в секторі оборони України, з урахуванням сучасних цифрових викликів, передового міжнародного досвіду та перспектив впровадження інноваційних технологій, зокрема штучного інтелекту. Саме третій розділ виконує функцію трансформаційного проектування: він поєднує аналіз існуючих інструментів з баченням майбутнього розвитку систем електронного міжвідомчого документообігу, орієнтованого на технологічну стійкість, інформаційну безпеку та оперативну ефективність оборонного управління. Результати цього розділу можуть бути покладені в основу державної політики цифрової трансформації сектору безпеки й оборони, з урахуванням викликів воєнного часу, міжнародних зобов’язань та довгострокової стратегії інтеграції до євроатлантичного простору.

Основний зміст дисертації викладено на 156 (сто п’ятдесят шести) сторінках друкованого тексту. Робота містить 5 (п’ять) таблиць, 7 (сім) рисунків, 3 (три) діаграми та 5 (п’ять) додатків. Список використаних джерел налічує 239 найменувань, з яких 94 (39%) англійською мовою.

РОЗДІЛ 1. ЗАПРОВАДЖЕННЯ ЕЛЕКТРОННОЇ ВЗАЄМОДІЇ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ В УМОВАХ РОЗВИТКУ ЕЛЕКТРОННОГО УРЯДУВАННЯ: ЗАРУБІЖНИЙ І ВІТЧИЗНЯНИЙ ДОСВІД

1.1. Підходи до сутності та визначення електронної взаємодії органів державної влади за умов цифрової трансформації в Україні.

Електронна взаємодія органів державної влади в умовах цифрової трансформації є ключовим елементом побудови ефективної, прозорої та зручної для громадян системи управління. Особливої актуальності це питання набуває в контексті повоєнної відбудови України, де цифрова модернізація стає одним із пріоритетних напрямів розвитку держави. Електронна взаємодія передбачає використання цифрових технологій для обміну інформацією, надання послуг, координації дій та прийняття рішень між різними урядовими структурами, що особливо важливо в умовах обмежених ресурсів та необхідності швидкої реконструкції.

У сучасному світі цифрова трансформація є визначальним фактором розвитку будь-якої держави, і Україна, попри військові виклики, не є винятком. Вона охоплює процес автоматизованого обміну інформацією між різними урядовими структурами за допомогою сучасних технологічних засобів. Це сприяє підвищенню ефективності, прозорості та підзвітності державного управління, а також забезпечує доступ громадян до адміністративних послуг у цифровому форматі та дозволяє забезпечити швидкий та ефективний обмін даними, що є критично важливим для координації процесів відбудови. Одним з елементів електронної взаємодії є електронне урядування – важливий інструмент демократизації суспільства та покращення якості державних послуг. Електронна взаємодія передбачає впровадження уніфікованих стандартів обміну даними, посилення кібербезпеки та створення механізмів прозорого моніторингу функціонування електронних платформ [1]. Особливої ваги в повоєнний період

набуває питання захисту цифрової інфраструктури від кібератак та забезпечення безперервності роботи критичних державних систем.

На початкових етапах інформатизації суспільств і зокрема державного управління основна увага приділялася впровадженню інформаційно-комунікаційних технологій у ключові адміністративні процеси. На етапі "визначення завдань" запроваджуються інформаційні системи для збору та статистичного аналізу даних. На етапі "підготовки до прийняття управлінських рішень" та "прийняття рішень" застосовуються інформаційно-аналітичні системи, які забезпечують обґрунтованість управлінських дій. На етапах "доведення рішення до адресатів", "організація виконання" та "контроль виконання рішень" активно використовуються системи електронного документообігу. Наступна активна фаза нормотворчої діяльності в сфері електронного урядування спрямована на надання адміністративних послуг у цифровій формі через веб-портали та мобільні інтернет-сервіси. Розвиток електронного урядування розглядається як ключовий фактор підвищення конкурентоспроможності держави на міжнародній арені та невід'ємний елемент європейської інтеграції України.

Можна з упевненістю констатувати, що цифрова трансформація є одним із головних пріоритетів державної політики України. Реалізація цієї трансформації стала можливою завдяки низці стратегічних законодавчих ініціатив, які сприяють розвитку цифрових технологій та інтеграції їх у різні сфери суспільного життя. Зокрема, важливими етапами стали ухвалення Закону України «Про електронні документи та електронний документообіг» у 2003 році, що заклало основу для розвитку електронної взаємодії, а також прийняття розпоряджень Кабінету Міністрів України, таких як Концепція електронного розвитку урядування та Стратегій здійснення цифрового розвитку, які визначають напрямки цифрових трансформацій і цифровізації в країні. Ці ініціативи є важливими кроками для досягнення ефективного та прозорого управління в умовах цифрової ери [60].

Незважаючи на значний прогрес, розвиток електронної взаємодії в Україні

стикається з низкою викликів, особливо в контексті повоєнної відбудови. Серед основних проблем можна виділити недостатнє фінансування, пошкодження цифрової інфраструктури внаслідок військових дій, технічну відсталість окремих органів влади, труднощі з інтеграцією різних інформаційних систем та платформ, а також недостатній рівень цифрової грамотності населення. Усе це створює значні бар'єри для ефективної реалізації цифрових ініціатив. Таким чином, постає питання, як в умовах поточної ситуації в Україні найбільш ефективно реалізувати поставлені плани, узагальнено названі «Цифровим стрибком», та де шукати резерви для покращення електронної взаємодії органів державної влади в повоєнний період.

Проблеми електронної взаємодії органів державної влади – це міждисциплінарна сфера, яка залучає науковців, експертів та практиків з усього світу. При цьому особливої актуальності ці питання набувають в контексті відбудови країни після військових дій, коли ефективне використання цифрових технологій може значно прискорити процеси відновлення.

У світовому контексті та безпосередньо в Україні питання цифрових трансформацій та електронного урядування досліджувалися низкою провідних науковців та експертів. Серед них варто виділити Джейн Фаунтін (Jane E. Fountain) – відому американську дослідницю, професора Гарвардського університету, авторку концепції "технологічного детермінізму" та важливих досліджень у сфері електронного урядування. Її праця «Building the Virtual State» є однією з ключових у цій галузі. Даррелл Вест (Darrell M. West) – американський політолог і фахівець з цифрової політики, автор книги «Digital Government: Technology and Public Sector Performance», досліджував вплив технологій на державне управління. Мануель Кастельс (Manuel Castells), іспанський соціолог, дослідник інформаційного суспільства, у своїй праці «The Rise of the Network Society» аналізує роль інформаційних технологій у трансформації державного управління.

Слід визнати, що значний внесок у дослідження електронної взаємодії органів державної влади в умовах цифрової трансформації також зробили і

українські науковці. О. Баранов [9] дослідив правові аспекти соціальної та цифрової трансформації, що є особливо важливим для формування правового поля електронної взаємодії. Д. Досин, В. Литвин, Ю. Нікольський та В. Пасічник [32] розробили теоретичні основи інтелектуальних систем, базованих на онтологіях, що може бути застосовано для підвищення ефективності міжвідомчої взаємодії. О. Карпенко запропонував механізми формування та реалізації сервісно-орієнтованої державної політики в Україні, що є важливим аспектом розвитку електронних послуг. Наприклад, дослідження [67] щодо цифрових компетенцій як умови формування якості людського капіталу мають особливе значення для підготовки кадрів у сфері цифрової трансформації. Г. Андрощук [3] проаналізував аспекти цифрової трансформації в країнах ЄС, що є цінним для гармонізації українського підходу з європейськими стандартами.

Українська національна платформа Форуму громадянського суспільства Східного партнерства у своєму дослідженні “Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному?” аналізує загальні тенденції та передумови цифрового розвитку України. На даній платформі було розміщено огляд цілей, які були визначені Міністерством цифрової трансформації до 2024 року, а також розглянуто важливі передумови для ефективної синхронізації роботи органів виконавчої влади в процесі цифрової трансформації [124].

У проведених дослідженнях В. Луценко та Т. Пікуля була розглянута існуюча проблематика правового забезпечення цифрової трансформації в Україні, а також проаналізовано етапи досягнення органами державної влади в сфері цифровізації, зокрема впровадження додатку «Дія» [74]. О. Попов досліджував дискурсне поле цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. У своїх наукових статтях він детально розкрив стан наукових розробок проблем цифрової взаємодії органів публічної влади та електронного урядування в Україні [90].

Проте, незважаючи на значний обсяг досліджень, питання резервів для покращення електронної взаємодії органів державної влади в умовах повоєнної

відбудови України залишається недостатньо вивченим. Особливо це стосується аспектів забезпечення стійкості цифрової інфраструктури, швидкого відновлення електронних сервісів після руйнувань, інтеграції з європейськими стандартами та системами, а також створення моделі ефективної електронної взаємодії в умовах обмежених ресурсів. Ці питання потребують глибшого дослідження та розробки практичних рекомендацій.

В цілому у роботі було застосовано комплексний методологічний підхід, що поєднує кілька взаємодоповнюючих методів наукового пізнання для всебічного аналізу електронної взаємодії органів державної влади в умовах цифрової трансформації та повоєнної відбудови України.

– **Монографічний метод** застосовано для детального вивчення окремих аспектів та прикладів електронної взаємодії. Цей метод дозволив глибоко проаналізувати конкретні кейси впровадження цифрових рішень в Україні, зокрема платформу «Дія», системи електронного документообігу та інші проєкти цифрової трансформації. Монографічний аналіз конкретних прикладів дозволив виявити практичні проблеми та успішні рішення в галузі електронної взаємодії.

– **Абстрактно-логічний метод** використаний для розробки теоретичних моделей та концепцій електронної взаємодії. За допомогою цього методу було сформульовано ключові поняття, розроблено концептуальну модель електронної взаємодії та визначено логічні взаємозв’язки між різними підходами до розуміння даного феномену (технологічним, соціально-організаційним, функціональним, правовим).

– **Порівняльний метод** застосовано для зіставлення українського та міжнародного досвіду цифрової трансформації. Цей метод дозволив порівняти показники електронної взаємодії в Україні з аналогічними показниками країн ЄС та інших держав, що успішно впровадили електронне урядування. Порівняльний аналіз дав можливість виявити найкращі практики та адаптувати їх до українських реалій повоєнної відбудови.

– **Метод моделювання** використаний для розробки комплексної моделі

досягнення синергетичного ефекту від електронної взаємодії. На основі теоретичних концепцій та емпіричних даних було створено модель, що враховує особливості цифрової інфраструктури в умовах відбудови країни та визначено ключові фактори успіху електронної взаємодії.

Інформаційною базою дослідження стали нормативно-правові акти України, стратегічні документи у сфері цифровізації, наукові праці вітчизняних та зарубіжних дослідників, аналітичні звіти міжнародних організацій, статистичні дані щодо розвитку електронного урядування в Україні та світі, а також матеріали проектів цифрової трансформації, що реалізуються в Україні.

Метою підрозділу є дослідження теоретичних та практичних підходів до побудови ефективної електронної взаємодії органів державної влади за умов цифрової трансформації у повоєнній Україні та виявлення резервів для її покращення. Для досягнення поставленої мети визначено такі ***завдання***:

1) провести порівняльний аналіз показників електронної взаємодії та цифрової трансформації в Україні та країнах ЄС для виявлення потенційних резервів покращення та адаптації успішних міжнародних практик до українських реалій;

2) дослідити синергетичний ефект від електронної взаємодії органів державної влади та розробити методологічну модель його досягнення в умовах обмежених ресурсів та необхідності швидкої відбудови цифрової інфраструктури;

3) визначити ключові напрями вдосконалення системи електронної взаємодії з урахуванням викликів повоєнного періоду, європейської інтеграції та потреби в забезпеченні кібербезпеки і захисту критичної інформаційної інфраструктури;

4) розробити практичні рекомендації щодо пошуку та активації резервів для покращення електронної взаємодії органів державної влади в Україні, спрямовані на підвищення ефективності державного управління та якості послуг для громадян і бізнесу.

Електронна взаємодія органів державної влади в умовах цифрової

трансформації та повоєнної відбудови в Україні є ключовим елементом побудови ефективної, прозорої та зручної для громадян системи управління. Використовуючи системний підхід до аналізу даного феномену, можна визначити електронну взаємодію органів державної влади як систему організованого обміну інформацією, документами та даними між різними органами влади за допомогою цифрових технологій, що забезпечує ефективну координацію, швидкість прийняття рішень, прозорість та доступність державних послуг для громадян і бізнесу.

Електронна взаємодія передбачає створення єдиного технологічного й інституційного середовища, де органи влади можуть обмінюватися даними, документами та інформацією в режимі реального часу на одній платформі [75]. Зазначені процеси повинні відбуватися в одному цифровому середовищі, надійно захищеному від зовнішнього несанкціонованого втручання та кібератак, що особливо актуально в умовах підвищених безпекових загроз у повоєнний період.

На основі абстрактно-логічного методу та систематизації різних підходів до розуміння електронної взаємодії, мною розроблено комплексну концептуальну модель електронної взаємодії органів державної влади, що враховує специфіку повоєнної відбудови України (рисунок 1) [238].

Представлена структура інтегрує різні підходи до розуміння електронної взаємодії, які можна систематизувати наступним чином. З точки зору *технологічного підходу,* електронна взаємодія розглядається як сукупність технологій та інфраструктури, які забезпечують обмін інформацією між органами влади. Акцент робиться на використанні сучасних цифрових рішень, таких як хмарні технології, штучний інтелект та блокчейн, для підвищення ефективності управління. В контексті повоєнної відбудови особливого значення набуває впровадження рішень, що забезпечують швидке відновлення та резервування даних, а також децентралізоване зберігання критичної інформації.

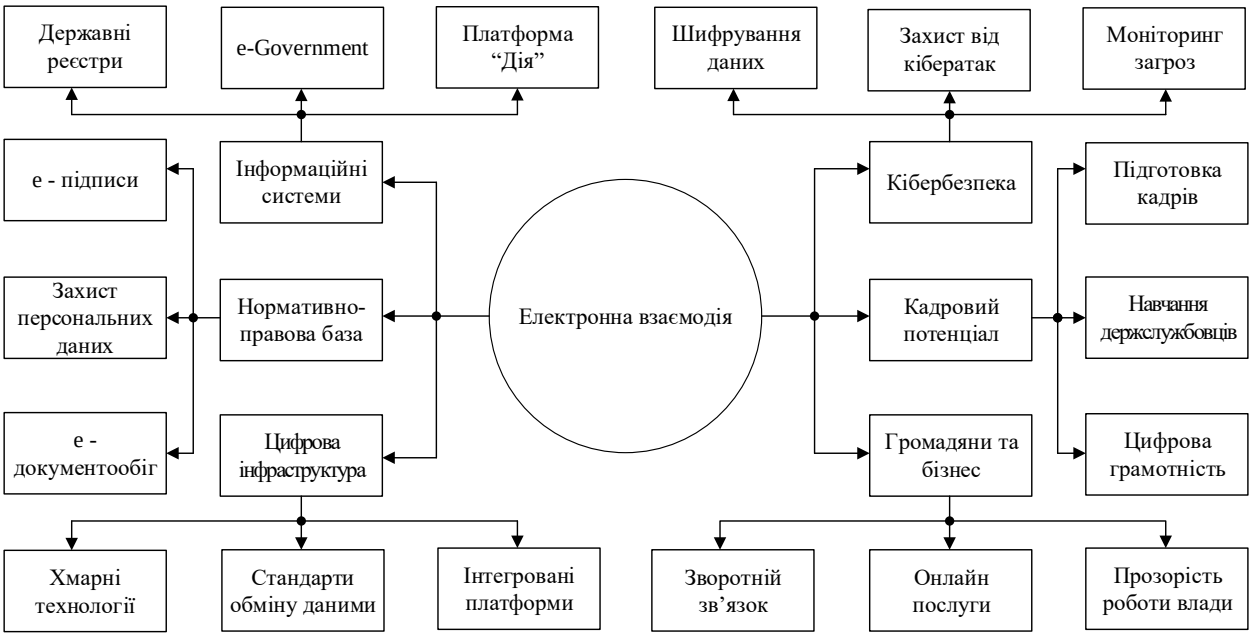


Рисунок 1. Узагальнена структура електронної взаємодії

В свою чергу *соціально-організаційний підхід* акцентує увагу на організаційних аспектах електронної взаємодії, зокрема на міжвідомчій координації та стандартизації процесів. Важливим елементом є створення єдиних стандартів обміну даними, що дозволяє уникнути сегментації/мікросегментації інформаційних систем. З соціальної точки зору, електронна взаємодія розглядається як інструмент підвищення якості життя громадян. Вона сприяє забезпеченню відкритості державного управління, зменшенню корупції та розширенню можливостей для участі громадян у прийнятті рішень. В умовах повоєнної відбудови цей підхід особливо важливий для забезпечення ефективної комунікації з громадянами та залучення їх до процесів відновлення.

Функціональний підхід акцентує увагу на конкретних функціях, які виконуються через електронну взаємодію. Відповідно до цього підходу, електронна взаємодія органів державної влади – це процес безпаперового обміну документами, даними та інформацією, що забезпечує координацію, контроль і управління між урядовими установами. Перевагами цього підходу є, насамперед, успадкованість та інтеграція систем (наприклад, Єдиний державний реєстр

фізичних осіб, ЄДРПОУ), стандартизація форматів документів і використання технічних протоколів для безпечного обміну даними. В умовах повоєнної відбудови функціональний підхід дозволяє зосередитися на пріоритетних функціях держави, які потребують першочергового відновлення та розвитку.

Процесний підхід вивчає електронну взаємодію як сукупність процедур і алгоритмів, які реалізуються для досягнення конкретних результатів. Процесна модель включає такі етапи як: ідентифікація потреби у взаємодії; формування запиту або передача документації; отримання відповіді чи обробленого результату; документування результатів взаємодії. Прикладом четвертого етапу є співпраця між Державною фіскальною службою та Міністерством соціальної політики під час виплати допомоги громадянам.

Правовий підхід фокусується на правових аспектах електронного урядування в Україні. З моменту проголошення незалежності у 1991 році в Україні значно змінилися адміністративні процеси в органах державної влади завдяки впровадженню інформаційно-комунікаційних технологій у сфери державної політики, інформатизації та електронного урядування. Важливим є узгодження національного законодавства про електронне урядування з європейськими стандартами, зокрема в контексті гармонізації нормативно-правової бази з вимогами ЄС. Саме правовий підхід акцентує увагу на нормативно-правових аспектах електронної взаємодії, а саме: регулювання порядку обміну даними; встановлення стандартів безпеки та конфіденційності; визначення прав та обов’язків учасників процесу. В контексті повоєнної відбудови правовий підхід набуває особливого значення для розробки спеціального законодавства щодо відновлення цифрової інфраструктури та забезпечення безперервності державних послуг.

Системний підхід розглядає електронну взаємодію органів державної влади як складну систему стало функціонуючих активів, що включають технічно розгалужену інфраструктуру (сервери, мережі тощо) [97], інформаційні ресурси та сервіси (реєстри, бази даних), а також людський фактор, який, у свою чергу, поділяється на адміністраторів систем і користувачів. Цей підхід враховує

взаємозв’язок між усіма елементами системи для забезпечення її ефективного функціонування та стійкості, що надзвичайно важливо в умовах повоєнної відбудови, коли різні елементи системи можуть бути пошкоджені або функціонувати з обмеженнями.

Таким чином, на основі інтеграції різних підходів можемо сформулювати комплексне визначення електронної взаємодії органів державної влади як системи організованого обміну інформацією, документами та даними між різними органами влади за допомогою цифрових технологій, яка охоплює широкий спектр процесів, включаючи обмін електронними документами, подання звітів у цифровому форматі, надання адміністративних послуг онлайн та інші форми комунікації між державними інституціями, громадянами та бізнесом, що функціонує в умовах підвищених безпекових вимог та орієнтована на швидку адаптацію до викликів повоєнного періоду.

Узагальнення підходів до визначення електронної взаємодії органів державної влади наведено на рисунку 2.

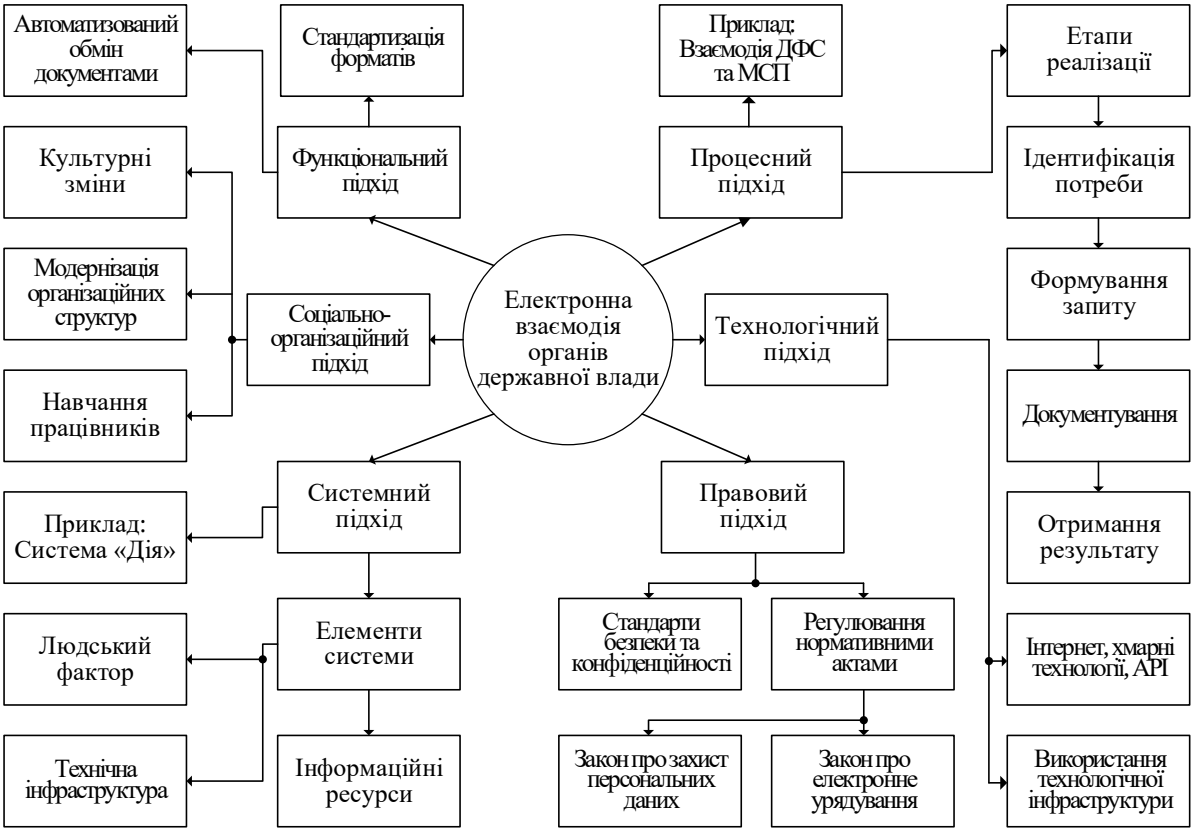


Рис. 2. Узагальнення підходів до визначення електронної взаємодії органів державної влади

Для глибшого розуміння потенційних резервів удосконалення електронної взаємодії в Україні доцільно провести порівняльний аналіз різних моделей електронної взаємодії, що успішно функціонують у світі.

В рамках цього дослідження я розробив методологічну основу такого порівняння, яка дозволяє врахувати як кількісні показники, так і якісні характеристики електронної взаємодії (Таблиця 1).

Таблиця 1. Методологічна структура порівняльного аналізу моделей електронної взаємодії в різних країнах

Критерій порівняння	**Ключові індикатори**	**Методи оцінки**	**Значимість для повоєнної відбудови**
Архітектурна модель	- централізована/ децентралізована - наявність резервування - масштабованість - модульність	- експертна оцінка - технічний аудит - структурний аналіз	висока – визначає стійкість системи до руйнувань та швидкість відновлення
Інституційна структура	- рівень координації - наявність спеціального органу координації - чіткість розподілу відповідальності - гнучкість	- інституційний аналіз - експертне опитування - аналіз нормативних документів	середня – забезпечує ефективність управління в умовах кризи
Нормативно-правова база	- повнота законодавства - гармонізація з міжнародними стандартами - наявність спеціальних норм для кризових ситуацій - адаптивність	- правовий аналіз - порівняльний аналіз законодавства - експертні оцінки	висока – створює правове підґрунтя для швидкого відновлення
Технологічні рішення	- інтероперабельність - кібербезпека - використання інновацій - відповідність стандартам	- технічний аудит - бенчмаркінг - функціональне тестування	дуже висока – визначає фактичну можливість функціонування в складних умовах

Фінансова модель	- джерела фінансування - ефективність витрат - стійкість у кризових умовах - залучення міжнародної допомоги	- фінансовий аналіз - аналіз вартості життєвого циклу - порівняльний аналіз витрат	висока – критична для забезпечення ресурсів на відбудову
Залучення стейкхолдерів	- рівень залучення громадян - партнерство з бізнесом - міжнародна співпраця - зворотний зв'язок	- соціологічні дослідження - аналіз кейсів - експертні інтерв'ю	середня - забезпечує легітимність та підтримку
Кадровий потенціал	- цифрова грамотність - наявність спеціалістів з кібербезпеки - програми навчання - мотиваційні механізми	- оцінка компетенцій - аналіз ринку праці - опитування працівників	висока - визначає можливість ефективного використання технологій
Інноваційність	- використання новітніх технологій - швидкість впровадження інновацій - гнучкість до змін - R&D інвестиції	- аналіз інноваційних проєктів - порівняльні дослідження - експертні оцінки	середня - забезпечує конкурентоспроможність у довгостроковій перспективі

В цілому використовуючи цю методологічну структуру, стало можливим здійснити порівняльний аналіз моделей електронної взаємодії в Україні та семи країнах, які демонструють різні підходи до цифрової трансформації.

– *Естонська модель: X-Road як еталон міжвідомчої взаємодії.* Естонія вважається одним із світових лідерів цифрової трансформації державного управління. Основою естонської моделі є платформа X-Road, що забезпечує безпечний обмін даними між різними інформаційними системами. Ключовою особливістю X-Road є децентралізована архітектура, де дані зберігаються в різних системах, але можуть бути доступні через єдиний інтерфейс. Це

забезпечує високий рівень стійкості системи до кібератак та технічних збоїв. У якості успішного прикладу для України можна навести таке: під час масштабної кібератаки на Естонію у 2007 році, коли були атаковані урядові сайти, банки та медіа, децентралізована архітектура X-Road дозволила зберегти основні функції електронного урядування. Після цієї атаки Естонія впровадила додаткові заходи безпеки, включаючи "цифрові посольства" – сервери з резервними копіями даних, розміщені в інших країнах. В умовах повоєнної відбудови України естонський досвід є надзвичайно цінним. Децентралізована архітектура, подібна до X-Road, може забезпечити безперервність надання державних послуг навіть при фізичному пошкодженні інфраструктури в окремих регіонах. Крім того, створення "цифрових посольств" може бути ефективним рішенням для забезпечення збереження критично важливих даних.

– *Сінгапурська модель: централізований підхід до цифрового управління.* Сінгапур реалізує високоцентралізовану модель електронного урядування з єдиним порталом державних послуг (SingPass) та інтегрованою системою міжвідомчої взаємодії. Ключовою особливістю сінгапурської моделі є високий рівень координації всіх цифрових ініціатив та стратегічне планування на державному рівні. У якості успішного прикладу для України можна навести таке: під час пандемії COVID-19 Сінгапур зміг за лічені дні розгорнути цифрові рішення для відстеження контактів (TraceTogether) та управління карантинними заходами, що було можливим завдяки високому рівню цифрової готовності та централізованому управлінню. Але слід визнати, що централізована модель Сінгапуру виявила вразливість до проблем приватності даних, що викликало занепокоєння щодо надмірного спостереження за громадянами. Враховуючи зазначене, для України доцільно адаптувати окремі елементи сінгапурської моделі, зокрема в частині стратегічного планування, централізованого управління та координації цифрових ініціатив, що дозволить підвищити ефективність національної політики у сфері кібербезпеки та цифрової трансформації. Однак, враховуючи європейський вектор розвитку та важливість захисту приватності, необхідно знайти баланс між централізацією та захистом

персональних даних.

– *Данська модель: орієнтація на користувача та цифрова інклюзія.* Данія фокусується на створенні сервісно-орієнтованої моделі електронного урядування з акцентом на потреби користувачів. Основою цієї моделі є принцип «digital by default» (цифровий за замовчуванням), згідно з яким всі державні послуги надаються в цифровому форматі, але з забезпеченням альтернативних каналів для вразливих груп населення. Впровадження єдиного цифрового поштового ящика для комунікації з державними органами (Digital Post) дозволило значно скоротити адміністративні витрати та підвищити ефективність. При цьому для людей похилого віку та осіб з обмеженими можливостями були створені спеціальні програми цифрової підтримки. Але для України, в умовах повоєнної відбудови особливо важливо забезпечити інклюзивність цифрових послуг, враховуючи потреби внутрішньо переміщених осіб, людей з інвалідністю та інших вразливих груп. Данський досвід може бути корисним для розробки інклюзивної стратегії цифрової трансформації.

– *Ізраїльська модель: кібербезпека як пріоритет.* Ізраїль, який часто стикається з безпековими викликами, розробив модель електронної взаємодії з особливим акцентом на кібербезпеку. Ключовими елементами ізраїльської моделі є Національне кіберуправління, яке виконує функції координації всіх аспектів кібербезпеки, а також здійснює стратегічне управління розвиненою екосистемою кібербезпекових стартапів та інновацій. У якості успішного прикладу для України можна навести те, що ізраїльська програма «Щит» забезпечує захист критичної інформаційної інфраструктури, включаючи енергетичний сектор, водопостачання та транспорт. Під час хвилі кібератак на енергетичні об’єкти у 2016 році ця система продемонструвала високу ефективність. В умовах підвищених безпекових загроз ізраїльський досвід захисту критичної інфраструктури може бути надзвичайно цінним для України. Особливо важливим є створення спеціалізованих структур з кібербезпеки та розвиток державно-приватного партнерства у цій сфері.

– *Південнокорейська модель: інновації та швидка адаптація.*

Південна Корея відома своєю здатністю швидко впроваджувати інновації в державне управління. Модель електронної взаємодії в цій країні характеризується високим рівнем технологічного розвитку, широким використанням мобільних технологій та активною підтримкою інновацій на державному рівні. Під час пандемії COVID-19 Південна Корея впровадила систему “смарт-карантину”, яка поєднувала дані мобільних операторів, кредитних карт та відеоспостереження для ефективного відстеження контактів. Це дозволило країні уникнути масштабних локдаунів при збереженні контролю над поширенням вірусу. Проте неуспішний аспект такий – це як досвід: швидке впровадження інновацій іноді призводило до проблем з приватністю та надмірного збору даних. З цього Україна може перейняти південнокорейський підхід до швидкого впровадження інновацій, особливо в умовах, коли необхідно швидко відновлювати цифрову інфраструктуру. Однак важливо знайти баланс між інноваційністю та захистом приватності.

– *Австралійська модель: федералізм і координація.* Австралія, будучи федеративною державою, розробила модель електронної взаємодії, яка балансує повноваження федерального центру та штатів. Ключовим елементом австралійської моделі є Агентство цифрової трансформації, яке встановлює стандарти та координує цифрові ініціативи на різних рівнях. Хорошим прикладом є впровадження системи єдиної ідентифікації myGovID, яка забезпечила доступ до широкого спектра державних послуг як на федеральному рівні, так і на рівні окремих штатів через єдиний обліковий запис. Система була розроблена з урахуванням високих стандартів безпеки та захисту приватності. Проте початкові етапи впровадження електронної взаємодії в Австралії характеризувалися фрагментацією та дублюванням функцій між різними рівнями влади. Але в контексті децентралізації, яка активно впроваджується в Україні, австралійський досвід координації цифрових ініціатив між різними рівнями влади може бути доволі корисним.

– *Індійська модель: масштаб і доступність.* Індія, бувши найбільшою демократією світу, розробила унікальну модель електронної взаємодії,

орієнтовану на забезпечення доступності державних послуг для свого численного та різноманітного населення. Основою індійської моделі є Програма цифрової Індії (Digital India) та система біометричної ідентифікації Aadhaar. Система Aadhaar, яка охоплює понад 1,3 мільярда людей, дозволила забезпечити доступ до державних послуг та соціальних програм для найбідніших верств населення, які раніше були виключені з системи через відсутність документів. Але все ж таки масштабне впровадження цифрових технологій в умовах цифрового розриву призвело до проблем з доступністю для сільського населення та людей з низьким рівнем цифрової грамотності. Для нас індійський досвід демонструє важливість забезпечення доступності цифрових послуг для всіх верств населення, особливо в умовах повоєнної відбудови, коли цифровий розрив може посилитися [145, 224].

– *Український досвід: платформа «Дія» як основа національної моделі.* Україна активно розвиває власну модель електронної взаємодії, центральним елементом якої є платформа «Дія». Ця платформа поєднує функції цифрового документообігу, надання електронних послуг та цифрової освіти. Під час повномасштабного вторгнення у 2022 році платформа «Дія» продовжувала функціонувати та навіть розширила свої можливості, забезпечуючи доступ до критично важливих послуг, таких як реєстрація внутрішньо переміщених осіб та оформлення допомоги. Це стало можливим завдяки використанню хмарних технологій та резервному копіюванню даних. Але слід відзначити недостатню інтеграцію з системами місцевого самоврядування та відсутність повноцінної системи електронної взаємодії між усіма органами влади.

Отже, на основі проведеного аналізу міжнародних моделей електронної взаємодії можна виокремити ключовий провідний досвід для вдосконалення української моделі в умовах повоєнної відбудови, зокрема в напрямах:

1) **Підвищення стійкості інфраструктури** через впровадження децентралізованої архітектури на зразок естонської X-Road та створення “цифрових посольств” для зберігання критичних даних.

2) **Посилення кібербезпеки** з використанням ізраїльського досвіду

захисту критичної інфраструктури та створення спеціалізованих структур з кібербезпеки.

3) **Забезпечення цифрової інклюзії** за данською моделлю, особливо для вразливих груп населення, приміром внутрішньо переміщених осіб та людей з інвалідністю.

4) **Вдосконалення координації** між різними рівнями влади за австралійським зразком, особливо в контексті децентралізації та посилення ролі місцевого самоврядування.

5) **Стимулювання інновацій** з використанням південнокорейського досвіду швидкого впровадження технологічних рішень в умовах кризи.

6) **Розвиток цифрових компетенцій** за індійською моделлю масштабних програм цифрової грамотності, адаптованих до потреб різних верств населення.

7) **Інтеграція з європейськими системами** в контексті євроінтеграції України, забезпечуючи сумісність українських цифрових рішень із стандартами ЄС.

У цілому, електронна взаємодія органів державної влади в умовах цифрової трансформації та повоєнної відбудови здатна забезпечити потужний синергетичний ефект, що проявляється в посиленні ефективності управлінських рішень завдяки інтеграції технологій, узгодженості дій різних інституцій і взаємозв'язку даних. Такий ефект досягається тоді, коли окремі елементи цифрової системи не просто функціонують ізольовано, а працюють у взаємодії.

Синергетичний ефект – це той результат, коли спільна робота двох або більше елементів системи призводить до значно більшого результату, ніж проста сума їхніх окремих дій. Іншими словами, це ефект, який виникає, коли інтеграція та взаємодія створюють додаткові переваги. Основні характеристики синергетичного ефекту наступі (див. табл. 2.):

– синергетичний ефект перевищує суму окремих зусиль. Приклад, якщо два органи влади інтегрують свої системи, загальний результат може бути в кілька разів більшим, ніж просто сума їхніх окремих покращень;

– синергетичний ефект поширюється на всю систему, створюючи нові

можливості та переваги [136]. Приклад, інтеграція податкової служби та реєстру нерухомості може призвести до створення нових сервісів для громадян;

– синергетичний ефект створює додаткові переваги, які неможливо досягти окремими зусиллями. Приклад, якщо податкова служба, реєстраційний орган та соціальні служби інтегрують свої системи, це дозволяє автоматизувати процеси, уникнути дублювання даних та створити нові сервіси для громадян. Загальний результат буде значно більшим, ніж просто сума окремих покращень.

Таблиця 2. Порівняння на прикладі електронної взаємодії

Аспект	**Ефект взаємодії**	**Синергетичний ефект**
Результат	Лінійний (сума окремих зусиль)	Нелінійний (перевищує суму окремих зусиль)
Вплив	Локальний (обмежується конкретними сферами)	Глобальний (поширюється на всю систему)
Мультиплікативність	Відсутня	Присутня (створює додаткові переваги)
Приклад	Покращення роботи одного відомства завдяки електронному документообігу	Інтеграція систем різних відомств (створення нових сервісів для громадян)

В умовах повоєнної відбудови синергетичний ефект електронної взаємодії органів державної влади має особливе значення, оскільки дозволяє досягти максимальних результатів при обмежених ресурсах. Проаналізуємо ключові аспекти синергетичного ефекту в контексті повоєнної цифрової трансформації України:

1) **Підвищення ефективності державного управління.** Йдеться про електронну взаємодію, яка підвищує ефективність державного управління, зменшуючи дублювання функцій та бюрократичні бар'єри. Обмін даними в реальному часі не тільки пришвидшує прийняття рішень, але й скорочує час на узгодження. Наприклад, інтеграція бази даних Міністерства соціальної політики з реєстром внутрішньо переміщених осіб та електронними системами Пенсійного фонду дозволила автоматизувати процес призначення та виплати

допомоги переселенцям. Це скоротило час призначення допомоги з кількох тижнів до кількох днів, зменшило навантаження на працівників соціальних служб та підвищило точність даних.

2) **Прозорість та підзвітність.** Відкритість органів влади та доступність даних для громадськості знижують ризики корупції та підвищують довіру до держави.. Наприклад, система електронних закупівель ProZorro, інтегрована з реєстрами бенефіціарних власників компаній, податковою системою та реєстром судових рішень, створила ефективний механізм запобігання корупції у сфері державних закупівель. Завдяки цій інтеграції система автоматично виявляє потенційні конфлікти інтересів та блокує сумнівні тендери. За даними досліджень, це дозволило заощадити понад 6% бюджетних коштів, що в умовах обмежених ресурсів повоєнного періоду є критично важливим.

3) **Зручність для громадян і бізнесу.** Третім аспектом є зручність для громадян і бізнесу, що є важливим елементом електронної взаємодії. Громадяни можуть отримувати державні послуги онлайн, без необхідності відвідувати установи, що стосується як отримання довідок, так і участі в електронному голосуванні. Наприклад, інтеграція додатку «Дія» з базами даних МВС, Міграційної служби, Міністерства освіти та науки, Міністерства охорони здоров’я дозволила створити “цифрові документи”, які юридично рівнозначні фізичним оригіналам. В умовах повоєнного періоду, коли багато громадян втратили документи внаслідок руйнувань чи вимушеного переміщення, ця інтеграція набуває критичного значення, дозволяючи людям продовжувати отримувати послуги та підтверджувати свою особу.

4) **Інноваційність та адаптивність.** Цифрова трансформація безпосередньо сприяє підвищенню інноваційності, стимулюючи впровадження передових технологій, таких як штучний інтелект, блокчейн та великі дані. Це дозволяє автоматизувати складні процеси, прогнозувати тенденції та ухвалювати обґрунтовані рішення. Відповідно, поєднання супутникових даних, технологій машинного навчання та кадастрових систем дозволило створити автоматизовану систему оцінки пошкоджень інфраструктури та житлового фонду. Ця система

допомагає оперативно приймати рішення щодо пріоритетів відбудови та оцінювати необхідні ресурси. На мою думку, такий підхід дозволив би на 40% прискорити процес відновлення та підвищити ефективність використання коштів на 25%.

5) **Підвищення конкурентоспроможності держави.** Останній важливий аспект – це підвищення конкурентоспроможності держави. Ефективна електронна взаємодія робить державу привабливою для інвестицій і міжнародного співробітництва, що зміцнює її економічну стабільність [160]. Створення єдиної системи інвестиційних проєктів, інтегрованої з системами митниці, податкової служби та місцевого самоврядування, дозволило суттєво спростити процедури для іноземних інвесторів. Це особливо важливо для залучення фінансування на відбудову пошкодженої інфраструктури в постраждалих регіонах. За оцінками експертів, така інтеграція дозволила скоротити час започаткування інвестиційного проєкту втричі, що є критичним фактором у конкуренції за обмежені міжнародні інвестиційні ресурси.

Аналізуючи поточний стан електронної взаємодії органів державної влади в Україні з критичної перспективи, необхідно визнати, що попри значні досягнення, особливо в створенні окремих цифрових сервісів, існують фундаментальні проблеми, які потребують негайного вирішення для успішної повоєнної відбудови.

1) Цифрова трансформація України, попри значні досягнення останніх років, стикається з комплексом фундаментальних викликів, які потребують системного переосмислення в контексті повоєнної відбудови. Досвід війни став своєрідним стрес-тестом для цифрової інфраструктури держави, виявивши як її сильні сторони, так і критичні вразливості. Аналізуючи поточну ситуацію, я змушений констатувати, що фрагментованість цифрової архітектури залишається наріжним каменем, який суттєво обмежує потенціал електронної взаємодії органів влади. Міністерство цифрової трансформації, фокусуючись на розвитку успішної платформи «Дія», не змогло подолати проблему “цифрових сілосів”, коли системи різних відомств – Міністерства юстиції, судової влади,

місцевого самоврядування – функціонують автономно, без належного обміну даними. Така дезінтеграція в умовах обмежених ресурсів повоєнного періоду є непростимою розкішшю, що вимагає створення національної архітектури електронної взаємодії за принципом “децентралізованої інтеграції”, коли дані зберігаються розподілено, але доступні через уніфіковані протоколи, забезпечуючи як технічну сумісність, так і стійкість до фізичних пошкоджень та кібератак.

2) Екзистенційною проблемою для української цифрової екосистеми є її недостатня стійкість до безпекових загроз. Військовий досвід продемонстрував вражаючу відданість українських ІТ-фахівців, які часто героїчними зусиллями забезпечували неперервність роботи критичних державних систем. Однак, слід визнати, що системний підхід до забезпечення кіберстійкості все ще відсутній. Більшість державних інформаційних систем функціонують без адекватного резервування, центри обробки даних залишаються вразливими до фізичних ударів, а нормативно-правова база з кібербезпеки фрагментована й не відповідає викликам сучасності. Парадоксально, але саме ця критична ситуація відкриває для України унікальне вікно можливостей – стати піонером у створенні “військово-стійкої” цифрової інфраструктури з багаторівневою системою захисту, що включає географічно розподілені центри обробки даних, міжнародне резервування через “цифрові посольства”, альтернативні канали зв’язку та архітектуру нульової довіри як фундаментальний принцип кібербезпеки.

3) Одним із найменш артикульованих, але критично важливих викликів залишається цифровий розрив між центральними та місцевими органами влади. В умовах децентралізації та зростання ролі громад у відбудові, це стає не просто технічною проблемою, а питанням національної єдності та ефективності управління. Численні територіальні громади, особливо віддалені чи постраждалі від бойових дій, не мають необхідних технічних можливостей, фінансових ресурсів та кадрового потенціалу для впровадження сучасних цифрових рішень. Існуючі платформи для місцевого самоврядування, такі як «Розумне місто» чи «Трембіта», залишаються фрагментарними та недостатньо інтегрованими з

національними системами. Створення комплексної програми “Цифрова громада” з типовими хмарними рішеннями, регіональними центрами підтримки, програмами навчання та механізмами цільового фінансування дозволить не лише подолати цей розрив, але й перетворити місцеві громади на активних учасників цифрової трансформації держави.

4) Європейський вектор розвитку України ставить перед нами амбітне завдання – інтеграцію національних цифрових систем з європейськими стандартами та платформами. Незважаючи на прийняття законодавчих актів, спрямованих на гармонізацію з європейським правом, практична імплементація відбувається повільно, створюючи бар’єри для повноцінної інтеграції. Паралельно, суспільний виклик недостатньої цифрової грамотності (53% українців з базовими цифровими навичками проти 58% в ЄС) посилюється для вразливих категорій населення та внутрішньо переміщених осіб. Перед Україною відкривається стратегічна перспектива стати “цифровим мостом” між ЄС та іншими регіонами, для чого необхідна прискорена інтеграція з європейськими цифровими ініціативами, включаючи імплементацію регламенту eIDAS, інтеграцію з EU Digital Gateway та формування національної системи цифрового включення з диференційованими програмами навчання, мережею центрів підтримки та спеціальними програмами для вразливих груп. Така комплексна трансформація не просто вирішить поточні проблеми, але й закладе фундамент для інноваційного розвитку України як цифрової держави в повоєнний період.

Аналіз сучасного стану цифрової трансформації в Україні та порівняння з провідними міжнародними моделями електронної взаємодії дозволяє сформулювати комплексні рекомендації для повоєнної відбудови української цифрової екосистеми. Особливого значення набуває нормативно-правовий та інституційний вимір, який створює фундамент для всих інших аспектів реформування. У короткостроковій перспективі необхідним є розроблення та прийняття Закону України «Про стійку цифрову інфраструктуру» – аналог, який можна порівняти з естонським Digital Continuity Act, але з фокусом на військову

стійкість. Цей закон має визначити не лише стандарти електронної взаємодії, але й механізми забезпечення безперервності критичних державних функцій в умовах надзвичайних ситуацій. Створення Національної ради з цифрової відбудови при Кабінеті Міністрів України дозволить уникнути “цифрової феодалізації”, коли кожне відомство розвиває власні системи без належної координації. Цікавою паралеллю тут може служити фінська модель Digital and Population Data Services Agency, яка централізовано координує цифровий розвиток держави, але з акцентом на громадські потреби, а не технології як такі. Удосконалення нормативної бази має супроводжуватися розробкою системи моніторингу та оцінки ефективності електронної взаємодії за прикладом Індексу цифрової економіки та суспільства (DESI) ЄС, але адаптованого до українських реалій повоєнного відновлення з додатковими показниками стійкості та безпеки.

Технологічні та інфраструктурні резерви покращення електронної взаємодії потребують нестандартних рішень, що враховують обмеженість ресурсів та підвищені ризики пошкодження фізичної інфраструктури. Замість традиційного підходу створення централізованих потужних дата-центрів, що є уразливими до точкових ударів, ефективнішою може стати модель “цифрової мережевої оборони” – системи географічно розподілених мікро-дата-центрів із синхронізацією даних у реальному часі. Яскравим прикладом може бути ізраїльська Cyber Dome Initiative, яка поєднує розподілену інфраструктуру з централізованим моніторингом. Особливу увагу варто приділити впровадженню національної платформи електронної взаємодії за принципом “єдиного вікна”, подібної до естонської X-Road, але з додатковими функціями автоматичної реконфігурації при пошкодженні окремих компонентів системи. Нетрадиційним, але перспективним рішенням може стати використання технології “мобільних дата-центрів” на базі контейнерів, які можуть швидко переміщуватися в безпечні локації при загрозі фізичного знищення. У середньостроковій перспективі стратегічне значення матиме створення “цифрових посольств” – резервних копій критичних державних даних, розміщених на території дружніх країн, за прикладом Естонії, яка розмістила свої цифрові резервні копії на серверах у

Люксембурзі. Україна могла б створити систему дзеркалювання даних у кількох країнах ЄС одночасно, забезпечуючи максимальну стійкість.

Резерви у сфері кібербезпеки набувають критичної важливості в умовах України, яка фактично знаходиться на передовій глобальної кібервійни. Впровадження архітектури нульової довіри (Zero Trust Architecture) як базового принципу кібербезпеки державних систем – не просто технічне рішення, а фундаментальна зміна філософії захисту. На відміну від традиційного підходу "захищеного периметра", Zero Trust передбачає постійну верифікацію кожного запиту незалежно від його джерела. Інноваційним підходом може стати створення "кіберполігонів" – спеціалізованих середовищ для тестування стійкості державних систем до кібератак, подібних до ізраїльського CyberGym або південнокорейського K-Shield. Але Україна може піти далі, інтегруючи цей підхід із програмами Bug Bounty – винагородами для "білих хакерів", які знаходять вразливості в державних системах, що успішно практикується в США через платформу HackerOne. В умовах обмежених ресурсів це дозволить залучити світову спільноту фахівців з кібербезпеки до посилення захисту українських систем. Створення національної системи підготовки фахівців з кібербезпеки має ґрунтуватися не на традиційній академічній моделі, а на інтенсивних програмах типу "кіберрезервістів", коли IT-фахівці з приватного сектору проходять спеціалізоване навчання і можуть бути оперативно мобілізовані для реагування на масштабні кібератаки, подібно до естонської Cyber Defence League.

Питання цифрових компетенцій та цифрового включення представляє собою соціально-гуманітарний вимір цифрової трансформації, критично важливий для забезпечення її інклюзивності. Традиційні програми цифрової освіти часто не враховують специфічні потреби різних груп населення, особливо в умовах повоєнного відновлення. Інноваційним підходом могло б стати створення "цифрових хабів виживання" – центрів, де громадяни можуть не просто навчитися користуватися електронними послугами, але й отримати навички використання цифрових технологій для вирішення критичних життєвих

ситуацій: від відновлення втрачених документів до пошуку житла чи роботи. Прикладом може служити сінгапурська програма SG Digital Office, адаптована до військових реалій. Особливу увагу варто приділити внутрішньо переміщеним особам, для яких доступ до цифрових послуг часто є єдиним способом взаємодії з державою. Створення мережі мобільних центрів цифрової підтримки на базі автобусів, контейнерів чи фургонів, обладнаних комп'ютерами та інтернет-зв'язком, дозволить забезпечити доступ до цифрових послуг навіть у віддалених чи постраждалих районах – подібний підхід успішно застосовується в Індії через програму Digital Village. У середньостроковій перспективі розвиток персоналізованих програм цифрового навчання з елементами гейміфікації та адаптивних сценаріїв дозволить масштабувати цифрову освіту на все населення України.

Міжнародна інтеграція української цифрової інфраструктури становить стратегічний напрямок, що забезпечує як технічну взаємодію з європейськими системами, так і політичну підтримку на шляху цифрової відбудови. Забезпечення технічної сумісності українських цифрових ідентифікаторів з європейською системою eIDAS дозволить громадянам України користуватися цифровими сервісами ЄС, а європейцям – українськими. Цікавим підходом може стати концепція "цифрового шенгену" – середовища, де цифрові документи та ідентифікатори визнаються автоматично без додаткових процедур підтвердження [113]. Замість традиційного підходу поступової гармонізації законодавства та технічних стандартів, Україна могла б запропонувати ЄС модель "спільного цифрового простору" – платформи, де європейські та українські державні сервіси інтегруються на рівні користувацького інтерфейсу, забезпечуючи безшовний досвід для громадян. Середньострокова стратегія позиціонування України як "експериментального майданчика" для інноваційних цифрових рішень ЄС дозволить залучити додаткові ресурси та експертизу, перетворюючи виклик повоєнної відбудови на можливість для прискореного інноваційного розвитку.

Отже, враховуючи проведені вище дослідження можливо зробити наступні

висновки:

1) На основі застосування системного, монографічного, абстрактно-логічного, порівняльного методів і методу моделювання було розроблено комплексну концептуальну модель електронної взаємодії, що синтезує шість ключових підходів – технологічний, соціально-організаційний, функціональний, процесний, правовий і системний – з урахуванням особливостей повоєнної відбудови. Це дозволило сформулювати авторське визначення електронної взаємодії як цілісної системи організованого обміну інформацією між органами державної влади, що працює в умовах підвищених вимог до безпеки та забезпечує гнучку адаптацію до викликів повоєнного періоду.

2) Синергетичний ефект електронної взаємодії. Встановлено, що в умовах повоєнної відбудови синергетичний ефект електронної взаємодії органів державної влади набуває особливого значення, оскільки дозволяє досягти нелінійних результатів при обмежених ресурсах. Запропонована порівняльна таблиця ефектів взаємодії та синергетичного ефекту демонструє, що міжвідомча інтеграція в п’яти ключових аспектах (підвищення ефективності управління, забезпечення прозорості, зручність для громадян, стимулювання інноваційності та підвищення конкурентоспроможності держави) призводить до глобальних позитивних змін, що перевищують суму окремих покращень.

3) Розроблена методологічна структура порівняльного аналізу моделей електронної взаємодії за вісьмома критеріями дозволила ідентифікувати ключові резерви для покращення української моделі на основі досвіду провідних країн. Особливу цінність для повоєнної України становлять: естонська модель децентралізованої архітектури та «цифрових посольств»; ізраїльський досвід захисту критичної інфраструктури; данська модель цифрової інклюзії; австралійська модель координації між різними рівнями влади; південнокорейський підхід до інновацій. Систематизація цих елементів у контексті української специфіки дозволяє запропонувати інтегровану модель «Цифрового стрибка», адаптовану до умов повоєнної відбудови.

4) Здійснений критичний аналіз поточного стану електронної взаємодії

в Україні виявив п’ять фундаментальних проблем: фрагментованість цифрової інфраструктури, недостатню стійкість до безпекових загроз, розрив між центральними та місцевими органами влади, недостатню інтеграцію з європейськими системами та недостатній рівень цифрових компетенцій [51]. На основі цього аналізу запропоновано комплексні практичні рекомендації з короткостроковою (1-2 роки) та середньостроковою (3-5 років) перспективами реалізації, що охоплюють нормативно-правові, інституційні, технологічні, безпекові та освітні аспекти.

5) Цифрова трансформація та електронна взаємодія органів державної влади є не лише технологічним процесом, але й стратегічним елементом національної стійкості України. Це проявляється у забезпеченні безперервності державного управління, швидкому відновленні критичних послуг, підвищенні прозорості, ефективній координації відбудови та адаптивності до змінних умов. Імплементація запропонованої моделі «Цифрового стрибка», що ґрунтується на принципах стійкості, інклюзивності, випереджаючого розвитку та європейської інтеграції, дозволить Україні не лише ефективно відбудуватися після війни, але й здійснити якісний прорив у сфері державного управління.

6) Перспективи подальших досліджень пов’язані з вивченням потенціалу новітніх технологій (штучного інтелекту, блокчейну, квантових обчислень) у контексті посилення стійкості цифрової інфраструктури в умовах підвищених безпекових загроз, а також проведенням аналізу соціально-економічних впливів цифрових трансформацій на різні групи населення, особливо на внутрішньо переміщених осіб у повоєнний період. Унікальний український досвід цифрової стійкості в умовах війни та повоєнної відбудови має потенціал стати значущим внеском у глобальну безпекову архітектуру та міжнародні стандарти захисту критичної інформаційної інфраструктури.

1.2. Аналіз досвіду європейської спільноти держав із запровадження захищеної системи електронної взаємодії в органах державної влади

Запровадження захищених систем електронної взаємодії (СЕВ) в органах державної влади є ключовим елементом цифрової трансформації, що сприяє підвищенню ефективності, прозорості та безпеки публічного управління. У результаті глобальних викликів, таких як зростання кіберзагроз і потреба в інтеграції державних сервісів, країни Європейського Союзу (ЄС) розробили передові моделі СЕВ, які базуються на стандартах інтероперабельності, кібербезпеки та захисту даних. Виходячи з цього, аналіз європейського досвіду є доволі актуальним для України, яка прагне вдосконалити власну систему електронного міжвідомчого документообігу в секторі безпеки і оборони.

Метою цього підрозділу є систематизація досвіду країн ЄС у впровадженні захищених СЕВ, оцінка ключових підходів, викликів і можливостей для їх адаптації в Україні. Звідси випливає необхідність розглянути нормативно-правову базу, технологічні рішення, а також організаційні механізми, які забезпечують функціонування СЕВ у європейських державах. На основі цього аналізу будуть сформульовані рекомендації для України з урахуванням її специфіки, зокрема в контексті воєнного стану.

Європейський Союз створив комплексну нормативно-правову базу, яка регулює запровадження СЕВ у державному секторі. У результаті прийняття **Регламенту (EU) 2016/679 (GDPR)** забезпечено захист персональних даних, що є основою для безпечного обміну інформацією між органами влади [**Error! Reference source not found.**]. Таким чином, GDPR встановлює єдині стандарти обробки даних, що сприяють довірі до СЕВ.

Ще одним ключовим документом є **Директива (EU) 2016/1148 (NIS Directive)**, яка визначає заходи для забезпечення високого рівня безпеки мереж і інформаційних систем [**Error! Reference source not found.**]. Звідси випливає, що країни ЄС зобов’язані впроваджувати стандарти кібербезпеки, які захищають СЕВ від зовнішніх загроз. У 2022 році Директива була оновлена до **NIS 2**

Directive (EU) 2022/2555, що розширює вимоги до кібербезпеки та координації між державами-членами [161]. Виходячи з цього, можливо зробити висновок, що ЄС приділяє значну увагу гармонізації нормативних актів для забезпечення безпечної електронної взаємодії.

Відповідно, **Регламент (EU) 2019/881 (Cybersecurity Act)** посилює роль Європейського агентства з кібербезпеки (ENISA) у розробці сертифікаційних схем для інформаційних систем [**Error! Reference source not found.**]. У підсумку, ці документи створюють правову основу для впровадження СЕВ, яка є обов'язковою для всих країн-членів ЄС. Таким чином ми бачимо, що нормативна база ЄС є гнучкою, але водночас суворою, що забезпечує баланс між інноваціями та безпекою.

Технологічна основа СЕВ у країнах ЄС базується на концепції інтероперабельності, яка визначена в **Новій європейській рамці взаємодії (New European Interoperability Framework, EIF)** [**Error! Reference source not found.**]. У результаті впровадження EIF країни ЄС розробили стандарти для обміну даними, такі як **European Interoperability Reference Architecture (EIRA)** [**Error! Reference source not found.**]. З цього випливає, що EIRA забезпечує єдину архітектуру для СЕВ, дозволяючи різним системам ефективно взаємодіяти.

Ключовим інструментом є сервісно-орієнтована архітектура (SOA), яка широко застосовується в країнах ЄС. Наприклад, у Нідерландах стандарт **Digikoppeling** забезпечує безпечний обмін даними між органами влади через API [**Error! Reference source not found.**]. Таким чином, SOA дозволяє створювати масштабовані та гнучкі системи, які адаптуються до нових викликів. Виходячи з цього, як висновок, необхідно зазначити, що технологічна стандартизація є основою успіху європейських СЕВ.

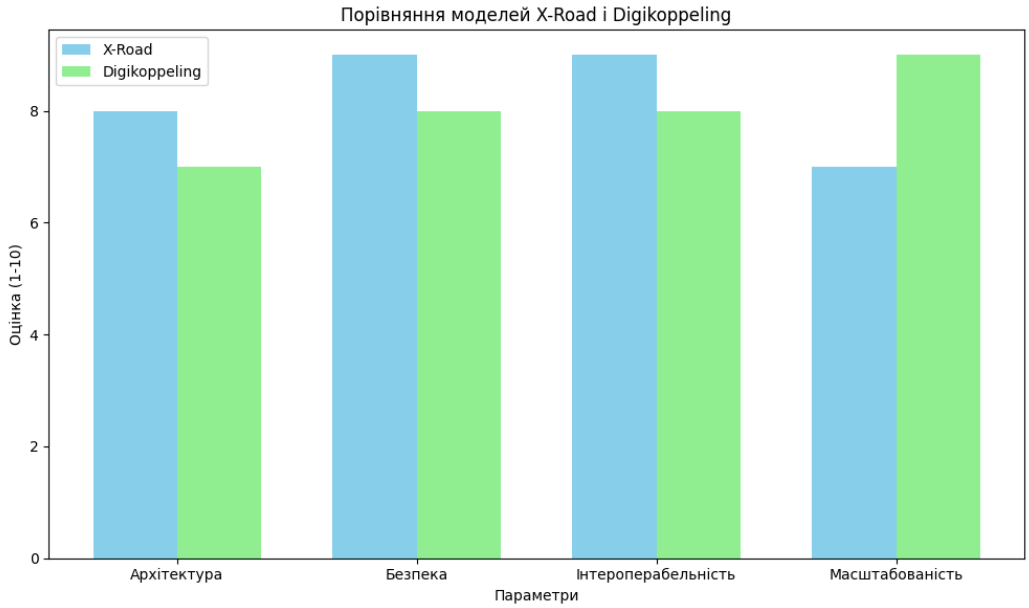
У процесі розробки національної СЕВ важливо враховувати міжнародний досвід країн, які досягли значного прогресу у впровадженні безпечних та масштабованих цифрових рішень. Зокрема, моделі X-Road (Естонія) та

Digikoppeling (Нідерланди) слугують показовими прикладами різних підходів до організації державної цифрової взаємодії.

Діаграма 1 представляє порівняльний аналіз цих двох моделей за ключовими параметрами: архітектура, безпека, інтероперабельність та масштабованість. Такий аналіз дозволяє визначити сильні сторони кожної моделі та оцінити їхню потенційну придатність до адаптації в українських умовах, зокрема в контексті цифрової трансформації та повоєнної відбудови.

Опис: Діаграма порівнює ключові характеристики моделей X-Road (Естонія) та Digikoppeling (Нідерланди) за такими параметрами: архітектура, безпека, інтероперабельність, масштабованість. X-Road використовує децентралізовану архітектуру з шифруванням і цифровими підписами, тоді як Digikoppeling базується на централізованих API-протоколах. Графік ілюструє переваги та обмеження кожної моделі, підкреслюючи їхню адаптивність до потреб України.

*Джерело: На основі [**Error! Reference source not found.**, **Error! Reference source not found.**, **Error! Reference source not found.**].



Діаграма 1. Порівняння моделей X-Road і Digikoppeling

Крім того, у Франції **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** розробила **Référentiel Général de Sécurité (RGS)**, який

встановлює вимоги до безпеки інформаційних систем [**Error! Reference source not found.**]. У підсумку, RGS забезпечує захист даних у СЕВ, що є критично важливим для державних установ. Таким чином ми бачимо, що європейські країни поєднують технологічні інновації з суворими стандартами безпеки.

Досвід окремих країн ЄС.

Естонія: X-Road як модель СЕВ. Естонія є світовим лідером у впровадженні СЕВ завдяки платформі X-Road, яка забезпечує безпечний обмін даними між органами влади [**Error! Reference source not found.**, **Error! Reference source not found.**]. У результаті використання X-Road Естонія досягла високого рівня цифровізації державних послуг, включаючи електронний документообіг. Звідси випливає, що X-Road базується на децентралізованій архітектурі, яка мінімізує ризики кібератак.

Виходячи з цього, ключовими елементами X-Road є:

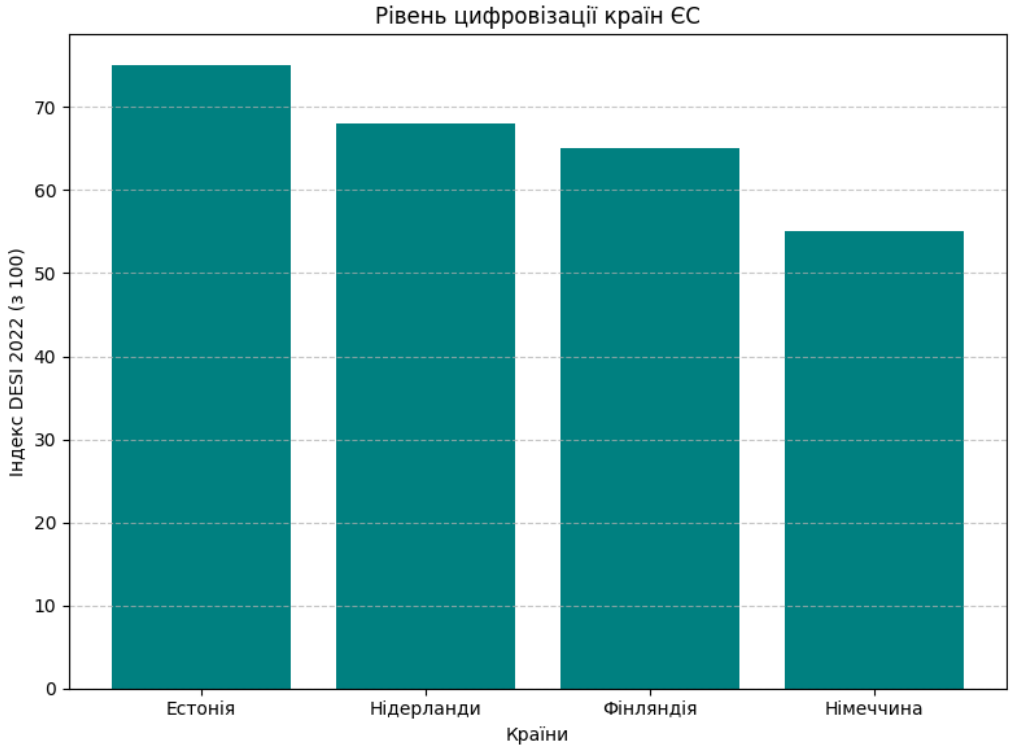
- **Безпека**: використання шифрування та цифрових підписів [**Error! Reference source not found.**].
- **Інтероперабельність**: єдиний протокол для всіх відомств [**Error! Reference source not found.**].
- **Масштабованість**: можливість інтеграції з міжнародними системами, наприклад, з Фінляндією [**Error! Reference source not found.**].

На основі цього можна стверджувати, що естонська модель є прикладом для країн, які прагнуть впровадити ефективну СЕВ. У підсумку, успіх Естонії пояснюється чіткою стратегією цифровізації, викладеною в **Digital Agenda 2020 for Estonia** [212].

У контексті оцінки ефективності впровадження цифрових державних сервісів доцільним є аналіз позицій європейських країн за ключовими показниками цифровізації. Індекс цифрової економіки та суспільства (DESI) щорічно вимірює рівень розвитку цифрових технологій у країнах ЄС, включаючи компоненти, що стосуються електронного урядування.

Діаграма 2 ілюструє рівень цифровізації державних послуг у чотирьох країнах ЄС – Естонії, Нідерландах, Німеччині та Фінляндії, за даними DESI 2022 року. Естонія демонструє найвищі показники завдяки системному впровадженню електронного уряду, тоді як Німеччина зіштовхується з викликами, пов'язаними з модернізацією застарілих ІТ-систем. Дана візуалізація дозволяє зрозуміти масштаби цифрового прогресу та актуальні бар'єри, що можуть бути враховані під час адаптації цифрових стратегій в Україні.

Опис: Стовпчикова діаграма показує рівень цифровізації державних послуг у країнах ЄС (Естонія, Нідерланди, Німеччина, Фінляндія).



Діаграма 2. Рівень цифровізації країн ЄС

Необхідно зазначити, що Естонія лідирує за показниками електронного урядування, тоді як Німеччина має нижчі показники через складність інтеграції застарілих систем. Діаграма підкреслює прогрес країн у впровадженні СЕВ.

Джерело: На основі [**Error! Reference source not found.**].

Німеччина: IT-Grundschutz і цифрова інфраструктура. Німеччина застосовує комплексний підхід до СЕВ через методологію **IT-Grundschutz, розроблену Bundesamt für Sicherheit in der Informationstechnik (BSI)** [**Error! Reference source not found.**, 153, **Error! Reference source not found.**]. У

результаті ця методологія забезпечує захист інформаційних систем від кіберзагроз, що є основою для СЕВ у державному секторі. З цього випливає, що Німеччина приділяє увагу стандартизації безпеки, зокрема через **Secure Information Sharing Architecture** [**Error! Reference source not found.**].

Таким чином, німецька модель СЕВ базується на:

- **Стандартизації**: єдині каталоги безпеки [**Error! Reference source not found.**].
- **Координації**: співпраця між федеральними та земельними органами [**Error! Reference source not found.**].
- **Інноваціях**: впровадження хмарних технологій у державних установах [**Error! Reference source not found.**].

Виходячи з цього, робимо висновок, що Німеччина демонструє ефективний баланс між безпекою та технологічним прогресом.

Фінляндія: KEJO та TUVE. Фінляндія використовує **KEJO** (систему спільного командного управління) для координації між органами безпеки [**Error! Reference source not found.**]. У результаті KEJO забезпечує оперативний обмін даними в реальному часі, що є критично важливим для сектору оборони. Звідси випливає, що Фінляндія інтегрує СЕВ із системами національної безпеки, зокрема через **TUVE (Secure Network Architecture)** [195].

На основі цього можна виділити особливості фінської моделі:

- **Безпека**: використання захищених мереж [161].
- **Інтеграція**: координація між цивільними та військовими відомствами [**Error! Reference source not found.**].
- **Стратегія**: чітке планування, викладене в **Security Strategy for Society** [**Error! Reference source not found.**].

Таким чином ми бачимо, що Фінляндія демонструє ефективний підхід до інтеграції СЕВ у сектор безпеки.

Нідерланди: DigiD і NL DIGIbeter. У Нідерландах СЕВ базується на **DigiD** (цифрова ідентичність) і **NL DIGIbeter** (цифрова урядова програма) [**Error! Reference source not found.**, **Error! Reference source not found.**]. У

результаті ці інструменти забезпечують безпечний доступ до державних сервісів і обмін даними між відомствами. З цього випливає, що Нідерланди активно використовують API через стандарт **Digikoppeling** [**Error! Reference source not found.**].

Відповідно, нідерландська модель характеризується:

- **Доступністю**: єдина цифрова ідентичність для громадян і установ [**Error! Reference source not found.**].
- **Гнучкістю**: використання API для інтеграції систем [**Error! Reference source not found.**].
- **Прозорістю**: чітка стратегія цифровізації [**Error! Reference source not found.**].

У підсумку, Нідерланди є прикладом країни, яка успішно поєднує технологічні та організаційні аспекти СЕВ.

Незважаючи на успіхи, країни ЄС стикаються з низкою викликів при впровадженні СЕВ:

1. **Кіберзагрози**: зростання атак на державні системи, що вимагає постійного оновлення стандартів безпеки [161].
2. **Інтероперабельність**: складність інтеграції застарілих систем із сучасними платформами [1].
3. **Фінансування**: високі витрати на модернізацію інфраструктури [231].
4. **Організаційні бар'єри**: опір змінам у державних установах [231].

У процесі впровадження СЕВ в країнах ЄС особливу увагу приділяють не лише технологічним аспектам, а й організаційним та кадровим складовим. Витрати на впровадження таких систем свідчать про необхідність збалансованого та міждисциплінарного підходу, який охоплює весь цикл цифрової трансформації.

Діаграма 3 відображає структуру витрат на впровадження СЕВ у країнах ЄС. Такий розподіл свідчить про пріоритетність технічної бази, водночас підкреслюючи важливість людського ресурсу та інституційної адаптації.

Діаграма 3. Структура витрат на впровадження СЕВ

В цілому інтеграція цих складових у межах єдиної політики цифрової трансформації дозволяє досягти системного ефекту та забезпечити стійкість функціонування публічних сервісів у динамічному середовищі.

Опис: Кругова діаграма ілюструє розподіл витрат на впровадження СЕВ у країнах ЄС: технологічна інфраструктура (50%), навчання персоналу (20%), кібербезпека (20%), організаційні зміни (10%). Діаграма підкреслює значні інвестиції в технології та необхідність балансу між різними аспектами.

Джерело: На основі [231].

Виходячи з цього, можна дійти обґрунтованого висновку, що успішне впровадження СЕВ вимагає комплексного підходу, який поєднує технологічні, правові та організаційні заходи. Таким чином, країни ЄС активно працюють над подоланням цих викликів через співпрацю з ENISA та впровадження єдиних стандартів.

Аналіз європейського досвіду відкриває можливості для вдосконалення СЕВ в Україні, особливо в секторі безпеки і оборони. У результаті вивчення

моделей Естонії, Німеччини, Фінляндії та Нідерландів можна запропонувати такі рекомендації:

1. **Інтероперабельність.** Впровадження єдиної архітектури на основі SOA, подібної до EIRA [**Error! Reference source not found.**].
2. **Кібербезпека.** Адаптація стандартів NIS 2 Directive для захисту СЕВ [161].
3. **Цифрова ідентичність.** Розвиток систем, аналогічних DigiD, для безпечного доступу до державних сервісів [**Error! Reference source not found.**].
4. **Стратегія.** Розробка чіткого плану цифровізації, подібного до Digital Agenda 2020 for Estonia [212].

З урахуванням проведеного аналізу європейських практик, зокрема моделей Естонії та Нідерландів, можна зробити науково обґрунтований висновок про доцільність адаптації їхнього досвіду в умовах України. У контексті збройної агресії та потреби в надійній координації між ключовими органами державної безпеки, Україна має всі підстави для створення захищеної СЕВ, орієнтованої на підвищену стійкість до кіберзагроз.

У зв’язку з цим доцільним є ініціювання пілотного проєкту із впровадження національної платформи, функціонально подібної до X-Road, яка забезпечить безпечний обмін даними між Міністерством оборони, Радою національної безпеки і оборони та іншими профільними органами. Такий підхід сприятиме підвищенню ефективності управлінських процесів у сфері оборони, а також закладе основу для подальшого розвитку національної цифрової інфраструктури в умовах воєнного стану.

У підсумку, європейський досвід демонструє, що успішне впровадження захищених СЕВ залежить від поєднання нормативно-правової бази, технологічних стандартів і організаційних механізмів. Таким чином ми бачимо, що країни ЄС, такі як Естонія, Німеччина, Фінляндія та Нідерланди, досягли значних результатів завдяки чітким стратегіям і стандартам безпеки. Виходячи з цього, робимо висновок, що Україна може адаптувати ці підходи, враховуючи власні виклики, зокрема в секторі безпеки і оборони. З цього випливає

необхідність розробки національної стратегії СЕВ, яка інтегруватиме європейські стандарти з локальними потребами.

1.3. Теоретичні засади державної політики щодо створення, впровадження та функціонування системи електронного міжвідомчого документообігу сфери оборони

Цифрова трансформація державного управління є одним із пріоритетних напрямів реформування публічного адміністрування в Україні. Особливої актуальності набуває впровадження електронного документообігу в сфері оборони, що дозволяє підвищити ефективність управлінських процесів, оперативність прийняття рішень та їх виконання, а також забезпечити захист інформації відповідно до сучасних викликів [61].

Електронний міжвідомчий документообіг у сфері оборони представляє собою складну соціотехнічну систему, що функціонує на перетині державного управління, оборонної політики, інформаційних технологій та кібербезпеки. Теоретичне осмислення засад державної політики щодо розвитку таких систем вимагає міждисциплінарного підходу та врахування специфіки функціонування органів військового управління.

Як зазначає Горбулін В.П., “інформаційні технології в оборонній сфері мають розглядатися не просто як технічний інструментарій, а як стратегічний ресурс забезпечення національної безпеки” [26, с. 45]. В умовах гібридних загроз та необхідності інтеграції з системами країн-партнерів по НАТО особливого значення набуває створення захищених систем електронного документообігу, що відповідають міжнародним стандартам.

Метою даного підрозділу є систематизація теоретичних засад державної політики у сфері створення, впровадження та функціонування системи електронного міжвідомчого документообігу сфери оборони, аналіз концептуальних підходів до побудови таких систем, а також обґрунтування

методологічних принципів їх розвитку в умовах цифрової трансформації сектору безпеки і оборони України.

Концептуальні основи електронного міжвідомчого документообігу формуються на перетині теорій державного управління, інформаційного менеджменту та кібербезпеки. Ключовим поняттям у цій сфері є “електронний документообіг”, який Матвієнко О.В. та Цивін М.Н. визначають як “сукупність процесів створення, оброблення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів” [76, с. 17].

Особливістю міжвідомчого документообігу в сфері оборони та безпеки є необхідність взаємодії різних органів військового управління, що мають власні електронно-комунікаційні системи і мережі, регламенти роботи і технічне обслуговування озброєння та військової техніки, а також оперативно-технічні вимоги до системи захисту інформації та кібербезпеки. Кураташвілі А.А. виділяє такі принципи побудови електронного міжвідомчого документообігу [68]:

1. Єдиності – формування єдиного інформаційного простору та уніфікованих правил роботи з документами;
2. Безперервності документообігу – забезпечення послідовного проходження документів через усі необхідні інстанції;
3. Паралельності – можливість одночасної роботи з документом різних учасників процесу;
4. Прозорості – можливість контролю стану документів у будь-який момент часу;
5. Захищеності – забезпечення інформаційної безпеки на всіх стадіях роботи з документами.

Згідно з дослідженням Лопушинського І.П., формування державної політики у сфері електронного документообігу відбувається на трьох рівнях [73]:

- Стратегічний рівень – визначення цілей, пріоритетів та напрямів розвитку систем електронного документообігу;

- Тактичний рівень – розробка конкретних механізмів впровадження та функціонування систем електронного документообігу;
- Операційний рівень – безпосередня реалізація процесів електронного документообігу в конкретних установах.

У контексті оборонної сфери особливої актуальності набуває врахування специфічних вимог до систем електронного документообігу, зокрема підвищених вимог до захисту інформації, здатності функціонувати в умовах обмеженого доступу до комунікаційних мереж, забезпечення інтероперабельності з інформаційними системами країн-партнерів, а також можливості оперативної адаптації до змін бойової обстановки.

Розвиваючи теоретичні засади електронного документообігу, Дубов Д.В. запропонував модель "цифрового суверенітету" в інформаційних системах оборонної сфери, яка передбачає баланс між використанням передових технологій та забезпеченням національної безпеки [36]. Ця модель включає:

- Технологічну автономність – використання програмного забезпечення з відкритим кодом або національних розробок;
- Інформаційну стійкість – здатність системи функціонувати в умовах інформаційних атак;
- Юридичну захищеність – нормативно-правове забезпечення функціонування системи;
- Кадрову незалежність – наявність кваліфікованих фахівців для обслуговування системи.

Згідно з дослідженнями Почепцова Г.Г., електронний документообіг слід розглядати не лише як технологічне явище, але й як елемент інформаційного протиборства в сучасних умовах [93]. Автор підкреслює, що системи електронного документообігу в оборонній сфері є потенційними об'єктами кібератак, тому їх архітектура має враховувати не лише функціональні, а й безпекові аспекти.

Теоретико-правові засади електронного документообігу в сфері оборони формуються під впливом міжнародного та національного законодавства. Основу

нормативно-правового забезпечення становлять загальні закони про електронні документи та спеціальні нормативні акти щодо функціонування інформаційних систем у сфері оборони.

Корж І.Ф. виділяє три рівні правового регулювання електронного документообігу в оборонній сфері [61]:

1. Загальне законодавство про електронні документи та електронний документообіг;
2. Спеціальне законодавство про захист інформації;
3. Відомчі нормативні акти, що регулюють особливості електронного документообігу в конкретних структурах.

Закон України “Про електронні документи та електронний документообіг” визначає основні принципи електронного документообігу та встановлює юридичний статус електронних документів [99]. Проте, як зазначає Баранов О.А., в оборонній сфері виникає необхідність додаткового регулювання з урахуванням специфіки інформації з обмеженим доступом [10].

Згідно з дослідженням Беланюк М.В., правове забезпечення електронного документообігу в сфері оборони повинно базуватися на принципах [13]:

- Законності – відповідність процесів документообігу вимогам законодавства;
- Достовірності – забезпечення автентичності та цілісності електронних документів;
- Конфіденційності – захист інформації від несанкціонованого доступу;
- Відповідальності – встановлення правових механізмів відповідальності за порушення правил документообігу;
- Стандартизації – дотримання єдиних технічних стандартів.

Ліпкан В.А. підкреслює важливість розробки спеціальних стандартів електронного документообігу для оборонної сфери, які б враховували вимоги міжнародних стандартів інформаційної безпеки та специфіку військового

управління [72]. Автор пропонує створення “нормативної матриці” електронного документообігу, яка включає:

- Базові стандарти (формати документів, протоколи обміну);
- Стандарти безпеки (шифрування, автентифікація, контроль доступу);
- Стандарти інтероперабельності (взаємодія різних систем);
- Галузеві стандарти (специфічні для оборонної сфери).

Важливим аспектом правового забезпечення електронного документообігу в оборонній сфері є врегулювання питань електронного підпису. Як зазначає Мельник Р.С., використання кваліфікованого електронного підпису має особливе значення для документів, що містять інформацію з обмеженим доступом, оскільки дозволяє забезпечити не лише цілісність документа, але й ідентифікацію особи, яка його підписала [77].

Згідно з дослідженням Бакалінської О.О., правове регулювання електронного документообігу в оборонній сфері стикається з такими викликами [6]:

- Необхідність гармонізації національного законодавства з міжнародними стандартами;
- Забезпечення балансу між відкритістю та захистом інформації;
- Регулювання міжвідомчої взаємодії в електронному середовищі;
- Адаптація загальних норм до специфіки військового управління.

Міжнародний досвід впровадження систем електронного документообігу в оборонній сфері. Теоретичне осмислення процесів впровадження систем електронного документообігу в оборонній сфері України неможливе без аналізу міжнародного досвіду, особливо країн-членів НАТО. Вивчення найкращих практик дозволяє уникнути типових помилок та адаптувати успішні моделі до національних умов.

Дослідження Романа В.І. показує, що в країнах НАТО електронний документообіг у військовій сфері розвивається за двома основними напрямами [107]:

1. Створення відомчих захищених систем документообігу для внутрішнього використання;

2. Розробка міжвідомчих платформ для обміну інформацією між різними структурами оборонного сектору.

Системи електронного документообігу в оборонній сфері США базуються на принципі “комплексного інформаційного середовища” (Joint Information Environment), що передбачає інтеграцію різних інформаційних систем на єдиній платформі з чітким розмежуванням доступу. Ця модель дозволяє забезпечити оперативність обміну інформацією при збереженні високого рівня захисту.

Аналіз систем електронного документообігу країн НАТО, виявив наступні ключові характеристики:

- Багаторівневий захист інформації з використанням криптографічних методів;
- Гнучка система управління доступом, заснована на рольовій моделі;
- Використання стандартизованих форматів документів для забезпечення інтероперабельності;
- Можливість функціонування в умовах обмеженої доступності мережевої інфраструктури;
- Інтеграція з системами підтримки прийняття рішень.

Важливим аспектом міжнародного досвіду є стандартизація систем електронного документообігу в рамках НАТО. Як зазначає Хорошко В.О., Альянс розробив специфікації NATO Information Exchange Gateway (IEG), що визначають вимоги до обміну інформацією між національними системами різних рівнів захисту [119]. Ці специфікації включають:

- Архітектурні рішення для побудови шлюзів обміну інформацією;
- Протоколи безпечної передачі даних;
- Механізми автентифікації та авторизації;
- Процедури аудиту та контролю.

Дослідження Богдановича В.Ю. показує, що в європейських країнах впровадження систем електронного документообігу в оборонній сфері відбувалося у кілька етапів [18]:

1. Автоматизація окремих процесів документообігу в межах одного відомства;
2. Створення відомчих систем електронного документообігу;
3. Інтеграція відомчих систем у єдиний інформаційний простір;
4. Забезпечення транскордонного обміну інформацією між системами різних країн.

Згідно з аналізом Турчинова О.В., успішність впровадження систем електронного документообігу в оборонних відомствах Великої Британії забезпечується чітким розподілом відповідальності між різними структурами [117]:

- Стратегічний рівень (Міністерство оборони) – визначення вимог та фінансування;
- Технічний рівень (спеціалізовані агентства) – розробка технічних рішень;
- Операційний рівень (військові підрозділи) – експлуатація та оцінка ефективності систем.

Цікавим для України є досвід країн Балтії, які здійснили цифрову трансформацію оборонного сектору в процесі інтеграції до НАТО. Як зазначає Петров В.В., ключовими факторами успіху в цих країнах стали [88]:

- Створення спеціалізованих центрів компетенції з питань електронного документообігу;
- Залучення приватного сектору до розробки технічних рішень;
- Поетапне впровадження з постійним моніторингом результатів;
- Комплексна програма навчання персоналу.

Теоретичні моделі архітектури системи електронного міжвідомчого документообігу. Теоретичні моделі архітектури систем електронного міжвідомчого документообігу в оборонній сфері формуються на перетині теорій

інформаційних систем, кібербезпеки та організаційного управління. Вони визначають концептуальні підходи до побудови таких систем з урахуванням специфіки оборонної сфери.

Згідно з дослідженням Дубова Д.В., архітектура системи електронного документообігу в оборонній сфері має будуватися за модульним принципом, що забезпечує гнучкість та масштабованість системи [39]. Автор виділяє такі основні модулі:

1. Модуль створення та редагування документів;
2. Модуль маршрутизації та контролю виконання;
3. Модуль зберігання та архівування;
4. Модуль безпеки та захисту інформації;
5. Модуль інтеграції з іншими системами;
6. Модуль аналітики та звітності.

Шевченко В.Л. пропонує багаторівневу модель архітектури системи електронного документообігу, що включає [129]:

- Рівень даних (сховища документів, бази даних);
- Рівень додатків (програмні компоненти для роботи з документами);
- Рівень бізнес-логіки (правила обробки документів, маршрути);
- Рівень інтерфейсів (засоби взаємодії користувачів з системою);
- Рівень безпеки (засоби захисту інформації).

Особливу увагу дослідники приділяють моделям безпеки в системах електронного документообігу оборонної сфери. Богданович В.Ю. пропонує використовувати модель “глибокої оборони” (Defense in Depth), яка передбачає створення кількох рівнів захисту [15]:

- Фізичний рівень (захист обладнання та носіїв інформації);
- Мережевий рівень (захист каналів передачі даних);
- Системний рівень (захист операційних систем та додатків);
- Рівень даних (шифрування та контроль цілісності документів);
- Організаційний рівень (регламенти та процедури безпеки).

Для міжвідомчої взаємодії пропонується використовувати сервіс-орієнтовану архітектуру (SOA), яка дозволяє організувати взаємодію різних систем через стандартизовані інтерфейси. Ця модель передбачає:

- Визначення набору сервісів для обміну документами;
- Створення реєстру сервісів для їх пошуку та використання;
- Розробку стандартів взаємодії між сервісами;
- Створення механізмів оркестрації сервісів для реалізації складних процесів.

Важливим аспектом архітектури систем електронного документообігу є забезпечення їх функціонування в умовах часткової або повної втрати зв'язку. За результатами досліджень Лєнкова С.В., для систем оборонної сфери доцільно використовувати розподілену архітектуру з асинхронною реплікацією даних, що забезпечує можливість автономної роботи окремих вузлів системи [70].

Згідно з концепцією "цифрового суверенітету", запропонованою Петровим В.В., архітектура системи електронного документообігу в оборонній сфері має базуватися на національних розробках або програмному забезпеченні з відкритим кодом, що дозволяє забезпечити незалежність від зовнішніх постачальників [87]. Автор пропонує створення "національної стеку технологій" для систем електронного документообігу, що включає:

- Операційні системи з відкритим кодом;
- Вітчизняні засоби криптографічного захисту;
- Національні формати електронних документів;
- Вітчизняні системи управління базами даних.

Інформаційна безпека в системах електронного документообігу оборонної сфери. Інформаційна безпека є одним з ключових аспектів функціонування систем електронного документообігу в оборонній сфері. Теоретичні засади забезпечення інформаційної безпеки таких систем формуються на основі загальних принципів кібербезпеки з урахуванням специфіки оборонного сектору.

Згідно з дослідженням Дубова Д.В., загрози інформаційній безпеці систем електронного документообігу в оборонній сфері можна класифікувати за такими категоріями [38]:

1. За джерелом виникнення:
   - Зовнішні (хакерські атаки, промислове шпигунство);
   - Внутрішні (зловмисні дії персоналу, недостатня кваліфікація);
2. За характером впливу:
   - Загрози конфіденційності (несанкціонований доступ до інформації);
   - Загрози цілісності (модифікація або знищення інформації);
   - Загрози доступності (порушення функціонування системи);
3. За спрямованістю:
   - Загрози інфраструктурі (серверам, мережам, робочим станціям);
   - Загрози програмному забезпеченню;
   - Загрози інформаційним ресурсам (документам, базам даних).

Хорошко В.О. підкреслює особливе значення криптографічного захисту інформації в системах електронного документообігу оборонної сфери [121]. Автор пропонує використовувати багаторівневу систему криптографічного захисту:

- Шифрування каналів зв’язку;
- Шифрування документів та їх метаданих;
- Захист електронних підписів;
- Захист процедур автентифікації та авторизації.

Важливим елементом забезпечення інформаційної безпеки є управління доступом до системи електронного документообігу. Згідно з дослідженням Лєнкова С.В., для систем оборонної сфери найбільш доцільною є комбінована модель управління доступом, що поєднує [69]:

- Мандатну модель (на основі рівнів доступу);
- Рольову модель (на основі функціональних ролей користувачів);
- Дискреційну модель (на основі визначених власником документа прав).

Крутов В.В. розробив концепцію “проактивної безпеки” систем електронного документообігу, яка передбачає не лише реагування на інциденти, але й прогнозування та запобігання загрозам [65]. Ця концепція включає:

- Постійний моніторинг стану системи;
- Аналіз потенційних вразливостей;
- Моделювання можливих атак;
- Автоматичне оновлення засобів захисту.

Особливе значення для систем електронного документообігу в оборонній сфері має забезпечення безперервності їх функціонування. Система повинна зберігати працездатність навіть в умовах кібератак або фізичного пошкодження інфраструктури. Для цього пропонується використовувати такі механізми:

- Географічно розподілене зберігання даних;
- Резервування каналів зв’язку;
- Автономний режим роботи окремих компонентів;
- Автоматичне відновлення після збоїв.

Згідно з концепцією Сніцаренка П.М., система електронного документообігу в оборонній сфері має функціонувати як “система систем”, що складається з компонентів різного рівня захищеності [110]. Взаємодія між цими компонентами здійснюється через спеціальні шлюзи, що забезпечують контроль інформаційних потоків та запобігають поширенню загроз.

Методологічні підходи до впровадження електронного документообігу. Теоретичне осмислення методологічних підходів до впровадження систем електронного документообігу в оборонній сфері дозволяє визначити оптимальні стратегії їх створення та впровадження з урахуванням специфіки військового управління [164].

Згідно з дослідженням Руснака І.С., процес впровадження систем електронного документообігу в оборонній сфері може базуватися на таких методологічних підходах [108]:

1. Системний підхід – розгляд електронного документообігу як елемента загальної системи управління;

2. Процесний підхід – аналіз та оптимізація процесів документообігу перед їх автоматизацією;

3. Проєктний підхід – організація впровадження як обмеженого в часі проєкту з чіткими цілями та ресурсами;

4. Ризик-орієнтований підхід – ідентифікація та управління ризиками впровадження.

Петров В.В. пропонує методологію “адаптивного впровадження”, яка передбачає поетапне введення системи в експлуатацію з можливістю коригування проєктних рішень на основі результатів попередніх етапів [86]. Ця методологія включає:

- Пілотне впровадження в окремих підрозділах;
- Аналіз результатів пілотного впровадження;
- Коригування архітектури та функціоналу системи;
- Поступове масштабування на всі структури.

Для оборонної сфери особливе значення має методологія забезпечення інтероперабельності систем електронного документообігу, яка має забезпечуватися на кількох рівнях:

- Технічний рівень – сумісність протоколів, форматів, інтерфейсів;
- Семантичний рівень – єдине розуміння змісту інформації;
- Організаційний рівень – узгодженість процесів та регламентів;
- Правовий рівень – узгодженість нормативної бази.

Важливим методологічним аспектом є підхід до управління змінами при впровадженні електронного документообігу. Дослідження Шевченка В.Л. показує, що в оборонних структурах часто спостерігається підвищений опір інноваціям, обумовлений специфікою організаційної культури [130]. Автор пропонує методологію “поступової трансформації”, яка передбачає:

- Залучення керівництва до процесу впровадження;
- Формування групи “агентів змін” серед персоналу;
- Проведення навчальних заходів на всіх рівнях організації;
- Демонстрацію швидких перемог для підвищення мотивації.

Згідно з дослідженням Толубка В.Б., впровадження систем електронного документообігу в оборонній сфері має базуватися на методології “паралельного супроводу”, яка передбачає одночасне функціонування паперового та електронного документообігу протягом перехідного періоду [115]. Це дозволяє:

- Зменшити ризики втрати інформації;
- Забезпечити плавний перехід до нових технологій;
- Виявити та усунути недоліки системи до повного переходу на електронний документообіг.

Сизов А.І. пропонує використовувати методологію “критичних факторів успіху” при впровадженні систем електронного документообігу в оборонній сфері [109]. Ця методологія передбачає визначення ключових факторів, які мають вирішальний вплив на успішність проєкту, та концентрацію ресурсів на їх забезпеченні. До таких факторів автор відносить:

- Підтримка вищого керівництва;
- Наявність кваліфікованої команди впровадження;
- Адекватне фінансування;
- Чіткі цілі та показники ефективності;
- Залучення користувачів до процесу розробки.

Методологія “сервісно-орієнтованого впровадження”, запропонована Мельником Р.С., передбачає розгляд системи електронного документообігу як набору сервісів, які можуть впроваджуватися незалежно один від одного [78]. Це дозволяє:

- Зосередитися на найбільш пріоритетних функціях;
- Отримати відчутні результати на ранніх етапах впровадження;
- Знизити ризики, пов'язані з масштабними змінами;
- Забезпечити гнучкість у виборі технічних рішень.

Інтеграція систем електронного документообігу з іншими інформаційними системами оборонної сфери. Теоретичні засади інтеграції систем електронного документообігу з іншими інформаційними системами оборонної сфери формуються на перетині теорій систем, інформаційного

менеджменту та кібербезпеки. Така інтеграція є необхідною умовою створення єдиного інформаційного простору оборонного відомства.

Іінтеграція інформаційних систем в оборонній сфері може здійснюватися за такими моделями:

1. Централізована модель – створення єдиної платформи, що об'єднує всі функції;
2. Федеративна модель – збереження автономності окремих систем з забезпеченням їх взаємодії;
3. Сервісна модель – надання доступу до функцій різних систем через єдиний інтерфейс.

Для оборонної сфери найбільш доцільною є федеративна модель, яка дозволяє зберегти специфіку окремих інформаційних систем при забезпеченні їх ефективної взаємодії.

При цьому Дубов Д.В. пропонує концепцію "інформаційного хабу" для інтеграції систем електронного документообігу з іншими інформаційними системами [41]. Ця концепція передбачає створення центрального компонента, що забезпечує:

- Маршрутизацію інформаційних потоків;
- Трансформацію даних між різними форматами;
- Управління правами доступу;
- Моніторинг та аудит взаємодії.

Важливим аспектом інтеграції є забезпечення семантичної сумісності різних систем. Згідно з дослідженням Шевченка В.Л., для цього необхідно створення єдиної онтології предметної області, що включає [131]:

- Уніфіковану термінологію;
- Стандартизовані класифікатори та довідники;
- Єдині метадані для опису документів;
- Правила інтерпретації інформації.

Для забезпечення технічної інтеграції необхідно використовувати стандартизовані інтерфейси та протоколи обміну даними:

– Інтеграція на рівні даних (обмін файлами, реплікація баз даних);

– Інтеграція на рівні додатків (API, веб-сервіси);

– Інтеграція на рівні бізнес-процесів (оркестрація процесів, бізнес-правила);

– Інтеграція на рівні користувацького інтерфейсу (єдиний портал).

Особливу увагу дослідники приділяють інтеграції систем електронного документообігу з системами підтримки прийняття рішень. Згідно з дослідженням Богдановича В.Ю., така інтеграція дозволяє [16]:

– Забезпечити осіб, що приймають рішення, повною та актуальною інформацією;

– Автоматизувати процеси підготовки аналітичних матеріалів;

– Відстежувати виконання прийнятих рішень;

– Зберігати історію прийняття рішень для подальшого аналізу.

Інтеграції систем електронного документообігу з системами управління організаційною структурою та персоналом дозволяє:

– Автоматично відображати зміни в організаційній структурі;

– Налаштовувати маршрути документів відповідно до актуальної структури;

– Забезпечувати доступ до документів відповідно до посадових обов’язків;

– Автоматизувати процеси підготовки та погодження кадрових документів.

Для оборонної сфери особливе значення має інтеграція систем електронного документообігу з системами оперативного управління. Згідно з дослідженням Толубка В.Б., така інтеграція має забезпечувати [113]:

– Оперативну передачу директивних документів;

– Контроль виконання наказів та розпоряджень;

– Документування оперативної обстановки;

– Забезпечення інформаційної підтримки прийняття рішень.

Оцінка ефективності функціонування системи електронного документообігу. Теоретичні засади оцінки ефективності функціонування систем електронного документообігу в оборонній сфері базуються на загальних підходах до оцінки інформаційних систем з урахуванням специфіки оборонного сектору. Дослідники пропонують різні моделі та методики такої оцінки.

Згідно з дослідженням Мельника Р.С., оцінка ефективності системи електронного документообігу повинна здійснюватися за такими групами показників [79]:

1. Функціональні показники – відповідність системи функціональним вимогам;
2. Технічні показники – продуктивність, надійність, масштабованість;
3. Економічні показники – вартість впровадження та експлуатації, економічний ефект;
4. Організаційні показники – вплив на процеси управління та прийняття рішень;
5. Безпекові показники – рівень захисту інформації, стійкість до загроз.

Шевченко В.Л. пропонує методику комплексної оцінки ефективності системи електронного документообігу, що базується на визначені інтегрального показника як зваженої суми часткових показників [133]. Автор виділяє такі часткові показники:

- Швидкість обробки документів;
- Час пошуку інформації;
- Рівень автоматизації рутинних операцій;
- Надійність збереження документів;
- Зручність використання системи;
- Рівень захисту інформації;
- Вартість експлуатації системи.

Для оборонної сфери особливе значення має оцінка впливу систем електронного документообігу на ефективність управлінських процесів. Цей вплив може оцінюватися за такими критеріями:

- Скорочення часу на підготовку та прийняття рішень;
- Підвищення обґрунтованості рішень;
- Зменшення кількості помилок у документах;
- Підвищення контрольованості виконання рішень;
- Покращення координації між різними структурами.

Дубов Д.В. пропонує методику оцінки інформаційної безпеки систем електронного документообігу, що базується на аналізі ризиків [42]. Ця методика включає:

- Ідентифікацію потенційних загроз;
- Оцінку вразливостей системи;
- Оцінку ймовірності реалізації загроз;
- Оцінку можливих наслідків;
- Визначення рівня прийнятного ризику;
- Оцінку ефективності захисних заходів.

Важливим аспектом оцінки ефективності є визначення економічного ефекту від впровадження системи електронного документообігу. Згідно з дослідженням Бакалінської О.О., цей ефект складається з [4]:

- Прямої економії (скорочення витрат на папір, друк, зберігання документів);
- Скорочення трудовитрат на роботу з документами;
- Підвищення швидкості прийняття рішень;
- Зменшення втрат від помилок та неефективних рішень;
- Зниження ризиків порушення конфіденційності інформації.

Лєнков С.В. пропонує використовувати методологію збалансованої системи показників (Balanced Scorecard) для оцінки ефективності систем електронного документообігу в оборонній сфері [71]. Ця методологія передбачає оцінку за чотирма перспективами:

- Фінансова перспектива (економічні показники);
- Перспектива внутрішніх процесів (оптимізація процесів документообігу);

– Перспектива навчання та розвитку (підвищення кваліфікації персоналу);

– Перспектива користувачів (задоволеність користувачів системою).

Для оцінки ефективності міжвідомчої взаємодії можна використовувати показники інтероперабельності систем електронного документообігу:

– Технічна інтероперабельність (сумісність технічних рішень);

– Семантична інтероперабельність (єдине розуміння інформації);

– Організаційна інтероперабельність (узгодженість процесів);

– Правова інтероперабельність (узгодженість нормативної бази).

Перспективи розвитку електронного міжвідомчого документообігу в сфері оборони. Отже, теоретичне осмислення перспектив розвитку електронного міжвідомчого документообігу в сфері оборони дозволяє визначити стратегічні напрями вдосконалення таких систем та адаптації їх до нових викликів цифрової епохи.

Згідно з дослідженням Горбуліна В.П., ключовими напрямами розвитку систем електронного документообігу в оборонній сфері є [27]:

1. Інтеграція з системами штучного інтелекту для автоматизації процесів аналізу інформації та підготовки проєктів рішень;

2. Впровадження технологій розподіленого реєстру (blockchain) для забезпечення цілісності та достовірності документів;

3. Розвиток мобільних технологій для забезпечення доступу до документів у польових умовах;

4. Використання хмарних технологій для підвищення доступності та масштабованості систем;

5. Впровадження технологій обробки великих даних (Big Data) для аналітичної обробки інформації.

Дубов Д.В. пропонує концепцію “когнітивного документообігу”, яка передбачає використання технологій штучного інтелекту для [40]:

– Автоматичної класифікації документів;

– Семантичного аналізу їх змісту;

– Виявлення логічних зв’язків між документами;

– Прогнозування потреб користувачів у інформації;

– Автоматичного формування аналітичних звітів.

Особливу увагу дослідники приділяють перспективам використання технології blockchain у системах електронного документообігу оборонної сфери. Згідно з дослідженням Шевченка В.Л., ця технологія дозволяє [132]:

– Забезпечити неможливість несанкціонованої модифікації або видалення документів;

– Створити розподілений журнал аудиту з фіксацією всіх дій з документами;

– Реалізувати механізми цифрового нотаріату;

– Забезпечити прозорість процесів електронного документообігу при збереженні конфіденційності інформації.

Сьогодні, для систем електронного документообігу в оборонній сфері особливого значення набуває розвиток технологій забезпечення стійкості до кібератак. Згідно з дослідженням Хорошка В.О., перспективними напрямами в цій сфері є [120]:

– Використання квантової криптографії для захисту каналів зв’язку;

– Впровадження біометричної автентифікації;

– Розвиток систем виявлення та запобігання вторгненням;

– Використання технологій гомоморфного шифрування, що дозволяють обробляти дані без їх розшифрування.

Важко переоцінити важливість розвитку систем електронного документообігу в контексті цифрової трансформації оборонного сектору України та його інтеграції до стандартів НАТО. Перш за все слід розвивати такі перспективні напрями:

– Гармонізація стандартів електронного документообігу з вимогами НАТО;

– Забезпечення інтероперабельності з системами країн-партнерів;

– Розвиток національних технологічних платформ;

- Впровадження сучасних методів управління інформацією.

Згідно з дослідженням Богдановича В.Ю., важливим напрямом розвитку систем електронного документообігу в оборонній сфері є інтеграція з системами підтримки прийняття рішень нового покоління, що базуються на технологіях штучного інтелекту та аналізу великих даних [17]. Це дозволить:

- Автоматизувати процеси збору та аналізу інформації;
- Виявляти приховані закономірності та зв'язки;
- Прогнозувати розвиток ситуації;
- Формувати варіанти рішень з оцінкою їх наслідків.

Також наголошується на необхідності розвитку "людського виміру" систем електронного документообігу. Це включає:

- Розвиток компетенцій персоналу у сфері інформаційних технологій;
- Формування культури інформаційної безпеки;
- Адаптацію систем до потреб та особливостей користувачів;
- Розвиток методів управління змінами при впровадженні нових технологій.

Підсумовуючи, необхідно зазначити шо проведене дослідження теоретичних засад державної політики щодо створення, впровадження та функціонування системи електронного міжвідомчого документообігу сфери оборони дозволяє сформулювати ряд важливих висновків:

1. Електронний міжвідомчий документообіг у сфері оборони є складною соціотехнічною системою, що функціонує на перетині державного управління, оборонної політики, інформаційних технологій та кібербезпеки. Теоретичні засади її розвитку формуються на основі міждисциплінарного підходу з урахуванням специфіки оборонної сфери.

2. Концептуальні основи електронного міжвідомчого документообігу базуються на принципах єдиності, безперервності, паралельності, прозорості та захищеності. Формування державної політики у цій сфері відбувається на стратегічному, тактичному та операційному рівнях з урахуванням специфіки оборонної сфери.

3. Нормативно-правове забезпечення електронного документообігу в сфері оборони формується на основі загального законодавства про електронні документи та спеціальних нормативних актів, що регулюють особливості функціонування інформаційних систем у сфері оборони. Важливим напрямом є розробка спеціальних стандартів, що враховують вимоги міжнародних стандартів інформаційної безпеки та специфіку військового управління.

4. Аналіз міжнародного досвіду впровадження систем електронного документообігу в оборонній сфері показує, що в країнах НАТО такі системи розвиваються за двома основними напрямами: створення відомчих захищених систем документообігу та розробка міжвідомчих платформ для обміну інформацією. Особливе значення має стандартизація систем електронного документообігу в рамках НАТО.

5. Теоретичні моделі архітектури систем електронного міжвідомчого документообігу в оборонній сфері базуються на модульному принципі та багаторівневій структурі. Для міжвідомчої взаємодії доцільно використовувати сервіс-орієнтовану архітектуру, яка дозволяє організувати взаємодію різних систем через стандартизовані інтерфейси.

6. Інформаційна безпека є ключовим аспектом функціонування систем електронного документообігу в оборонній сфері. Теоретичні засади забезпечення інформаційної безпеки таких систем базуються на моделі “глибокої оборони”, що передбачає створення кількох рівнів захисту: фізичного, мережевого, системного, даних та організаційного.

7. Методологічні підходи до впровадження систем електронного документообігу в оборонній сфері включають системний, процесний, проєктний та ризик-орієнтований підходи. Для оборонної сфери доцільно використовувати методологію “адаптивного впровадження”, яка передбачає поетапне введення системи в експлуатацію з можливістю коригування проєктних рішень.

8. Інтеграція систем електронного документообігу з іншими інформаційними системами оборонної сфери є необхідною умовою створення єдиного інформаційного простору. Така інтеграція може здійснюватися за

централізованою, федеративною або сервісною моделлю, при цьому для оборонної сфери найбільш доцільною є федеративна модель.

9. Оцінка ефективності функціонування систем електронного документообігу в оборонній сфері повинна здійснюватися за функціональними, технічними, економічними, організаційними та безпековими показниками. Важливим аспектом є оцінка впливу таких систем на ефективність управлінських процесів та забезпечення інформаційної безпеки.

10. Перспективними напрямами розвитку електронного міжвідомчого документообігу в сфері оборони є інтеграція з системами штучного інтелекту, впровадження технологій розподіленого реєстру, розвиток мобільних та хмарних технологій, використання технологій обробки великих даних. Особливе значення має розвиток систем у контексті цифрової трансформації оборонного сектору України та його інтеграції до стандартів НАТО.

Таким чином, теоретичні засади державної політики щодо створення, впровадження та функціонування системи електронного міжвідомчого документообігу сфери оборони формуються на перетині різних галузей знань та вимагають комплексного підходу з урахуванням специфіки оборонної сфери та сучасних тенденцій розвитку інформаційних технологій.

РОЗДІЛ 2. СУЧАСНІ ПІДХОДИ ДО ФОРМУВАННЯ МЕХАНІЗМІВ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ЄДИНОГО ЗАХИЩЕНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА ЕЛЕКТРОННИХ ДОКУМЕНТІВ СКЛАДОВИХ СЕКТОРУ ОБОРОНИ ДЕРЖАВИ

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

В умовах цифрової трансформації державного управління та загострення кібербезпекових викликів особливої актуальності набуває питання ефективної та захищеної організації електронного документообігу в секторі безпеки і 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 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.

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 [7]. Н. Грицяк та Л. Литвинова проаналізували особливості впровадження електронного урядування в Україні та його правові аспекти [28]. І. Клименко та К. Линьов розглядали технології електронного урядування з точки зору їх нормативного забезпечення [53].

Питання безпеки електронного документообігу в державних структурах висвітлено у працях В. Бурячка, В. Толубка, С. Толюпи [20]. Ці дослідники зосередили увагу на технічних та організаційних аспектах захисту інформації в електронно-комунікаційних системах державних органів. Л. Чистоклетов та С. Обрембальський досліджували специфіку інформаційної безпеки в умовах цифрового протистояння [127].

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 [63]. А. та С. Ільєнко, О. Яковенко , Є. Галич, та В. Павленко розглядали можливості імплементації технологій штучного інтелекту в системи кібербезпеки [49].

Специфіку функціонування електронно-комунікаційних систем у військовій сфері та оборонному секторі, положення, пов’язані із забезпеченням інформаційної безпеки та системами захисту інформації, яка циркулює на об’єктах інформаційної діяльності органів військового управління досліджено у колективній монографії [21], 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 [172], що зумовлює актуальність даного дослідження.

Метою підрозділу є аналіз 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:

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

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

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

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

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” [**Error! Reference source not found.**], “Про електронні довірчі послуги” [**Error! Reference source not found.**], “Про захист інформації в інформаційно-телекомунікаційних системах” [**Error! Reference source not found.**], “Про державну таємницю” [98].

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” [53, 101]. Окремі аспекти захисту інформації в оборонному секторі регламентуються положеннями Закону України “Про основи національної безпеки України” [103] та Стратегією кібербезпеки України [104].

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 реєстрах.

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 [19].

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 [106]. 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 [11].

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 [227].

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 [66]. 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 безпеки і оборони. Зокрема, у США Департамент оборони у 2020 році ухвалив “Стратегію розвитку штучного інтелекту у сфері оборони” (Defense Artificial Intelligence Strategy), яка визначає правові та етичні принципи застосування ШІ у військовій сфері, включаючи системи управління документами [232]. 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” (Ethics Guidelines for Trustworthy AI), які хоч і мають рекомендаційний характер, але закладають основи для гармонізації правового регулювання застосування ШІ

в державному управлінні країн-членів ЄС [204]. 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 [57]. 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 [228]. 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:

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.

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.

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.

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.

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.

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 [83].

Іншою складовою є використання месенджерів, для оперативного обміну службовою інформацією, що постає 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 використовуватись 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 діяльності створює ризики для інформаційної безпеки, витоку інформації та ускладнює документування управлінських рішень в цілому.

У результаті проведеного дослідження встановлено, що чинна нормативно-правова база, яка регулює електронний документообіг у системі державного управління сектором оборони України, характеризується фрагментарністю та недостатньою адаптованістю до викликів, пов'язаних із впровадженням новітніх технологій, зокрема штучного інтелекту та блокчейну [205]. 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.

Вкрай важливою необхідністю для ефективного впровадження ШІ в систему ЕДО сектору оборони є розробка та прийняття нормативно-правових актів, 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.

В цілому 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.

2.2. Використання штучного інтелекту в документообігу: перспективи та виклики

Сучасний документообіг у бізнесі, державних установах та наукових організаціях стикається зі значними викликами. Зокрема, це стосується обробки великих обсягів інформації, зростання вимог до швидкості та точності обробки даних, а також необхідності забезпечення безпеки та конфіденційності. В умовах зростаючої кількості документів традиційні методи обробки стають неефективними, вимагаючи значних людських ресурсів і часу.

Документообіг є важливим аспектом роботи будь-якої організації. Він забезпечує управління інформацією, підтримує прийняття рішень і відповідає за виконання нормативних вимог. Традиційно документообіг відрізняється високими витратами часу та ресурсів, а також схильністю до помилок через людський фактор. Тому в сучасних умовах стрімкого розвитку технологій виникає потреба в автоматизації цих процесів, що може значно підвищити ефективність роботи.

У цьому контексті штучний інтелект стає одним із ключових інструментів для автоматизації документообігу. Однак впровадження ШІ в документообіг стикається з кількома викликами, серед яких важливою складовою постає якість даних, конфіденційність та інтеграція з існуючими системами.

Перехід від традиційних систем документообігу до цифрових є складним завданням. Серед актуальних аспектів електронного урядування можна виділити концепцію безпаперового управління, що сприяє безперебійному обміну даними та ефективному оцифрованому робочому процесу. Життєвий цикл документа повинен бути безпечним, доступним для перевірки, захищеним від фальсифікацій і архівованим для майбутнього доступу.

Інтерес до використання технологій штучного інтелекту в електронному документообігу значно зріс упродовж останніх років, зокрема в контексті зростаючих потреб автоматизації та інтелектуального аналізу управлінських документів. Особливу увагу заслуговують інструменти обробки природної мови (*Natural Language Processing,* NLP), які відкривають нові можливості для автоматизованої інтерпретації текстової інформації, зокрема аналізу змісту договорів, службових записок, нормативних актів та інших управлінських документів.

У цьому контексті ефективним інструментом виступає технологія розпізнавання іменованих сутностей (*Named Entity Recognition*, NER), яка дозволяє здійснювати виокремлення та класифікацію значущих елементів тексту (осіб, організацій, дат, нормативних термінів тощо) у слабко структурованих документах. Застосування NER-технологій забезпечує перехід від традиційної автоматизації документообігу до глибокого інтелектуального аналізу, що є основою для розгортання високорівневих систем підтримки прийняття управлінських рішень. Такий підхід не лише підвищує якість витягнутої інформації, а й сприяє формуванню адаптивних моделей управління в межах цифрової трансформації державного сектору.

Необхідно зазначити, що задачу автоматизованого розпізнавання іменованих сутностей було сформульовано ще в 1996 році на конференції MUC-

6 [216, 24]. Вона передбачала знаходження в тексті таких даних, як власні імена, назви організацій, час, географічні назви, дати, грошові суми тощо. Однак практичні результати стали доступні лише з розвитком генеративного ШІ, зокрема завдяки створенню сучасних великих мовних моделей (*Large Language ModelL,* LLM), які демонструють високу ефективність.

Водночас існують проблеми, пов'язані з використанням LLM для автоматизації цих процесів. Дослідження показують, що хоча такі технології вже працюють досить ефективно, питання інтеграції та автоматизованого прийняття рішень залишаються відкритими.

Сьогодні розробка та впровадження системи керування електронними документами та записами (*Electronic document and records management system,* EDRMS) є одним із ключових аспектів розвитку електронного документообігу, особливо для органів державної влади, установ та організацій, де ефективне управління документами відіграє вирішальну роль у функціонуванні. Однак цей процес супроводжується низкою викликів, серед яких: забезпечення відповідності нормативним вимогам, гарантування безпеки даних та інтеграція з наявними інформаційними системами.

Попри думку дослідників Gelashvili T. та Pappel [198], які зазначають, що відсутність автоматизованих процесів прийняття рішень вказує на неможливість застосування штучного інтелекту в EDRMS, швидкий розвиток цієї технології відкриває нові перспективи. Використання ШІ для автоматизації процесів обробки документів та ухвалення рішень може значно підвищити ефективність таких систем.

Разом з тим, попри значні переваги EDRMS, їх впровадження потребує ретельного планування, фінансових ресурсів, організаційних змін та юридичного супроводу [237]. Важливими складовими успішної реалізації є навчання персоналу, розробка чітких регламентів роботи з електронними документами та постійний моніторинг ефективності системи.

Слід усвідомити, що подальший розвиток ШІ може значно підвищити ефективність цих систем, що, у свою чергу, підтверджує перспективність досліджень у цьому напрямку [122].

Таким чином, нині можна спостерігати глобальне застосування технологій електронного безпаперового документообігу, що об'єднує в єдиній мережі користувачів та сприяє забезпеченню швидкого обміну документами, оптимізує управлінську діяльність. Однак, всупереч активній цифровій трансформації процесів документообігу, в науковому дискурсі зберігається позиція, згідно з якою системи електронного документообігу не здатні повною мірою замінити традиційні паперові форми обміну документами [14]. Деякі дослідники наголошують, що електронні документи, попри їх функціональність, мобільність та швидкість обробки, не завжди можуть гарантувати належний рівень юридичної достовірності й автентичності, який забезпечується у паперовому документообігу через фізичні ознаки, підпис, печатки тощо.

Таким чином, можемо констатувати, що сьогодні більшість існуючих рішень зосереджені на окремих аспектах документообігу, тоді як комплексний підхід до інтеграції ШІ залишається недостатньо дослідженим. Науковий пробіл полягає у відсутності систематизованого підходу до використання ШІ що автоматизує всі етапи документообігу, включаючи не тільки створення, передачу, зберігання, обробку та архівування документів, але й автоматизацію процесу видобування інформації.

Метою підрозділу є всебічний аналіз сучасних науково-технічних підходів до використання технологій штучного інтелекту в системах електронного документообігу в сфері державного управління.

У межах цього дослідження здійснюється вивчення потенціалу інструментів ШІ для оптимізації процесів обробки, аналізу та захисту цифрових документів, а також ідентифікація ключових викликів, що супроводжують їх впровадження в нормативно-регламентоване середовище.

Особлива увага приділяється проблемам забезпечення юридичної достовірності електронних документів, інформаційної безпеки, етичних аспектів

використання інтелектуальних алгоритмів та правового регулювання таких технологій.

У межах досягнення поставленої мети запропоновано концептуальні підходи до інтеграції інноваційних ШІ-рішень у захищені системи документообігу, що сприятимуть підвищенню ефективності та надійності управлінських процесів в умовах цифрової трансформації публічного сектору.

Системи електронного документообігу мають значний потенціал для трансформації організацій у різних секторах, таких як фінанси, медицина, юриспруденція, ритейл та інші. Проте не всі установи використовують ці системи в повній мірі. Технології, що сприяють розвитку автоматизації, активно прогресують, надаючи нові можливості для державного управління та бізнесу.

Глобальний ринок систем управління електронними документами демонструє стабільне зростання, що підтверджує загальносвітову тенденцію до цифровізації управлінських процесів. У 2020 році його обсяг становив 3,68 мільярда доларів США, а до 2027 року прогнозується зростання до 9,48 мільярда доларів США. Така динаміка вказує на високий попит впровадження ефективних рішень для електронного документообігу, що ставить перед державними органами питання модернізації існуючих систем та введення передових технологій, зокрема AI, для оптимізації обробки даних [94, 128].

Інтеграція AI в документообіг дозволяє автоматизувати рутинні завдання, такі як введення даних, сортування документів, їх маршрутизація і архівування. У поєднанні з технологіями розпізнавання символів (*Optical character recognition,* OCR), ШІ здатен перетворювати скановані зображення на редагований текст, що значно прискорює обробку документів і знижує кількість помилок [62, 89].

Крім того, ШІ ефективно застосовується для аналізу великих обсягів даних, що дозволяє виявляти закономірності та здійснювати прогнозування, сприяючи прийняттю обґрунтованих управлінських рішень у реальному часі [56, 58, 111]. Методи Data Mining використовуються для обробки великих масивів даних, що дозволяє прогнозувати навантаження на сервери та кластеризувати

стан їх роботи [**Error! Reference source not found.**]. При цьому сталість надання електронних послуг та функціонування системи електронного документообігу допомагають органам влади швидко та ефективно реагувати на внутрішні та зовнішні виклики, забезпечуючи необхідну аналітику та підтримку для ухвалення обґрунтованих управлінських рішень [134], підвищуючи точність оцінки загроз і ризиків [59, 64, 116, 135].

Проте впровадження таких технологій супроводжується серйозними викликами, такими як забезпечення безпеки даних, збереження конфіденційності та необхідність дотримання міжнародних стандартів, таких як загальний регламент про захист даних (*General Data Protection Regulation,* GDPR). Ці фактори ставлять перед організаціями/установами нові етичні та технічні завдання, до яких необхідно підходити з усією відповідальністю [22].

За цих умов вкрай важливим аспектом в рамках забезпечення безпеки та конфіденційності даних є впровадження сучасних методів шифрування та аутентифікації. Це дозволяє значно зменшити ризики, пов’язані з потенційною втратою конфіденційної інформації або несанкціонованим доступом до неї. Відповідно, такі заходи сприяють підвищенню загального рівня захисту даних та зміцненню довіри до системи електронного документообігу [237].

Разом з цим існують певні ризики при використанні ШІ в системах мережевого управління, серед яких недостатня прозорість та відповідальність, ризик упереджень та дискримінації під час прийняття рішень. Для вирішення проблеми непрозорості алгоритмів AI в мережевому управлінні важливо впроваджувати моделі інтерпретованого штучного інтелекту, які дозволяють зрозуміти, як саме алгоритм приймає рішення.

Окрім того, відсутність єдиних прозорих стандартів і регулювань є серйозною перепоною для широкого застосування ШІ, оскільки це створює невизначеність щодо відповідальності та надійності таких систем. Тому, саме розробка і впровадження чітких нормативних вимог і стандартів є необхідним кроком для безпечного і ефективного використання AI в мережевому управлінні органів державної влади [126, 229].

Інтеграція ШІ в вже діючі системи електронного документообігу системи управління органів державної влади мають важливе значення для розвитку України, особливо в умовах війни, коли ефективність управління та обробки інформації стає критично важливою для забезпечення стабільності та функціонування державних інституцій [223, 30]. Україна займає друге місце за кількістю ШІ-компаній у Східній Європі, що свідчить про стрімкий розвиток цієї галузі в країні та її здатність швидко адаптувати новітні технології до реалій сучасного світу [30]. Використання AI в різних сферах, зокрема в електронному документообігу, розглядається як спосіб підвищення операційної ефективності та загальної якості обслуговування в IT-послугах, що дозволяє знизити витрати та підвищити швидкість прийняття рішень [43].

Слід зазначити, що в умовах активної цифровізації державного управління в Україні правова регламентація використання штучного інтелекту залишається недостатньо розробленою, що створює значні труднощі у впровадженні інноваційних технологій у систему електронного документообігу. Відсутність окремого законодавства, яке б комплексно регулювало використання ШІ в державному секторі, призводить до правових прогалин і невизначеності у правозастосовній практиці [58, 84, 85].

Більшість чинних нормативно-правових актів держави, які регулюють сферу електронного документообігу, мають загальний характер і не враховують специфіку інтеграції ШІ у державні процеси [30, 43, 55]. Це, у свою чергу, ускладнює стандартизацію процедур, знижує рівень довіри до автоматизованих рішень та стримує широкомасштабне впровадження інтелектуальних технологій.

Тому важливим елементом є необхідність адаптації національного законодавства до європейських стандартів, зокрема до регламентів про захист даних та про штучний інтелект (*Artificial Intelligence Act,* AI Act), які визначають вимоги до обробки персональних даних та регулюють використання ШІ. Зокрема у AI Act визначено такі сфери високого ризику для ШІ як:

- критична інфраструктура;

- приватні та державні послуги (охорона здоров’я, банківські послуги);
- працевлаштування;
- освіта та професійна підготовка;
- міграція та управлінні кордонами;
- правосуддя та демократичні процеси (наприклад, вибори);
- деякі системи правоохоронних органів.

Запровадження відповідних нормативних актів дозволить забезпечити баланс між технологічним прогресом та дотриманням прав людини, а також мінімізує ризики, пов’язані з автоматизованим прийняттям управлінських рішень [12, 23, 82, 111].

Для вирішення цієї проблеми необхідне розроблення окремого законодавчого акту, який визначатиме:

- Принципи та етичні норми використання ШІ в державному управлінні;
- Механізми контролю та підзвітності щодо роботи автоматизованих систем;
- Правові аспекти відповідальності у разі помилкових рішень, ухвалених на основі ШІ;
- Інструменти захисту персональних даних та збереження конфіденційної інформації.

Розробка чіткої нормативної бази для використання ШІ в системі електронного документообігу на всіх етапах механізму державного управління, що охоплюють усі органи, які беруть участь у виконанні функцій держави, сприятиме підвищенню ефективності управлінських процесів, забезпечить прозорість адміністративних процедур та посилить кібербезпеку державних інформаційних ресурсів.

З метою оптимізації адміністративних процесів, що сприятимуть підвищенню оперативності, ефективності та точності виконання функцій державних органів, пропонується розглянути методологію обробки документів. Вона передбачає впровадження чітко визначених етапів, що охоплюють усі

аспекти взаємодії з документами, від їх створення та зберігання до аналізу та обробки [12, 25].

Окрему увагу пропонується приділити інтеграції сучасних технологій, зокрема ШІ, для автоматизації та вдосконалення процесів документообігу, що дозволяє значно зменшити часові витрати на обробку інформації, підвищити точність рішень та забезпечити прозорість і підзвітність в управлінні державними ресурсами [80].

Необхідно зазначити, що методологія обробки документів у контексті механізмів державного управління має класичну структуру і складається з кількох ключових етапів, що забезпечують ефективне функціонування системи електронного документообігу. Передбачаючи інтеграцію технологій ШІ в системи електронного документообігу органів державної влади, процес виглядатиме наступним чином:

1. Завантаження документа – на цьому початковому етапі користувач передає текстові дані для подальшої обробки, що може включати різноманітні документи державного управління, такі як заяви, накази чи протоколи. Важливою є забезпечена доступність та прозорість цього етапу, що дозволяє знизити бюрократичні бар'єри.

2. Система документообігу – цей етап організовує ефективну маршрутизацію та обробку документів між різними органами та ланками державного управління. За допомогою автоматизації та цифрових рішень, система забезпечує належну організацію роботи з документами, що прискорює розгляд, ухвалення рішень та виконання функцій держави.

3. Попередня обробка документа – на цьому етапі відбувається очищення тексту від зайвих символів, форматування та підготовка даних до подальшого аналізу. Важливою частиною є забезпечення коректності та стандартизації даних, що дозволяє зберігати узгодженість і єдиний формат для подальших етапів обробки документів.

4. Аналіз тексту з використанням ШІ – застосовується для:

– Класифікації документів за типом (накази, протоколи, акти тощо), що дозволяє автоматично визначати категорію документа для подальшої обробки.

– Витягування ключових сутностей (NER), що дає змогу ідентифікувати важливі дані, такі як органи влади, особи, дати чи місця, що є критично важливими для ефективного функціонування державних процедур.

– Лематизації та токенізації тексту, що нормалізує документ для подальшого аналізу та порівняння.

– Синтаксичного аналізу, що дає змогу визначати граматичні структури та коректно інтерпретувати зміст документа.

– Аналізу логічних зв'язків, що дозволяє виявити зв'язки між різними частинами тексту, що може бути корисно для підготовки звітів, аналізу політик та забезпечення точності рішень.

5. Збереження результатів у базі даних – після обробки, класифікація та витягнуті сутності зберігаються в централізованому сховищі. Це дозволяє забезпечити прозорість і доступність даних для подальшого аналізу, що є важливим елементом у контексті цифровізації державних процесів.

6. Оптимізація пошуку – нормалізований текст індексується для забезпечення швидкого пошуку та аналізу документів у системі. Це дає змогу значно зменшити час на пошук необхідної інформації в документах, що є критичним для оперативності роботи державних органів.

В цілому запропоновані етапи складають ефективну методологію обробки документів, яка забезпечує не лише автоматизацію процесів, але й підвищення ефективності управлінських рішень через використання новітніх технологій ШІ.

Деталізуючи етапність наведеної методології (Рис.3) можна з впевненістю зазначити, що вона відображає процес обробки документів за допомогою штучного інтелекту та може бути адаптована до механізмів державного управління, зокрема в частині електронного документообігу, автоматизації класифікації та аналізу адміністративного листування.

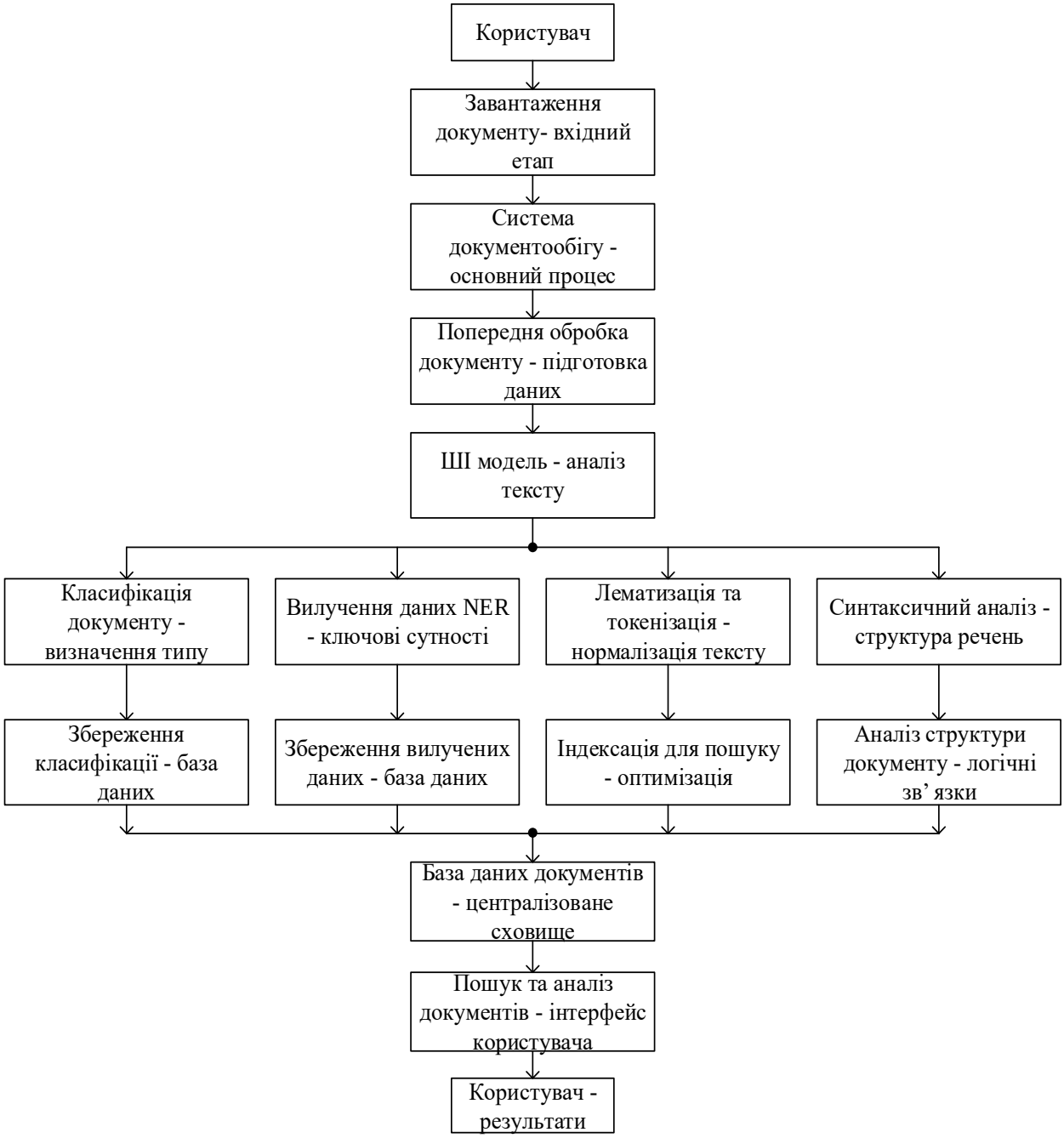


Рис. 3. – Методологія обробки документів у контексті механізмів державного управління

*Джерело: розробка автора.

Отже, процес обробки документів за допомогою штучного інтелекту включає:

Користувач – Державні службовці або громадяни, які завантажують документи (запити, довідки, накази, постанови тощо) з електронного кабінету.

Завантаження документу – Вхідний етап реєстрації офіційного документа в системі електронного документообігу (наприклад, СЕДО).

Система документообігу – Основний процес управління документами, який регулює їхнє зберігання, обробку та доступ.

Попередня обробка документу – Підготовка тексту для аналізу, яка може включати розпізнавання сканованих документів (OCR).

ШІ-модель – Використання технологій штучного інтелекту для аналізу адміністративного листування.

Класифікація документу – Визначення типу (закон, постанова, наказ, запит громадянина), що дозволяє автоматично спрямовувати документ до відповідного органу державної влади.

Вилучення даних NER – Визначення ключових сутностей, наприклад, назв організацій, імен посадовців, дат та географічних місць.

Лематизація та токенізація – Нормалізація тексту для подальшого аналізу та ефективного пошуку в базі даних.

Синтаксичний аналіз – Визначення структури речень та логічних зв’язків у тексті, що може допомагати в юридичній експертизі документів.

База даних документів – Централізоване сховище, яке дозволяє державним органам зберігати та швидко знаходити необхідні документи.

Пошук та аналіз документів – Інтерфейс для користувачів (державних службовців, громадян), який дозволяє швидко знаходити потрібні документи або робити аналітичні висновки.

Результати для користувача – Отримання інформації на основі запитів (наприклад, аналіз законодавчих актів, перевірка дотримання нормативів тощо).

З огляду на вищевикладене, слід зазначити, що система електронного документообігу, доповнена штучним інтелектом, дозволяє значно прискорити процес обробки звернень громадян. Алгоритми машинного навчання можуть автоматично класифікувати запити за тематикою, виявляти ключові дані (імена, дати, адреси) та спрямовувати їх до відповідних державних установ або

посадових осіб. Це, у свою чергу, скорочує час реагування, підвищує рівень обслуговування та мінімізує ризик людських помилок.

Окрім цього, ШІ дозволяє здійснювати автоматизований аналіз нормативно-правових актів для виявлення можливих суперечностей, дублювань або змін у законодавстві. Лінгвістичний аналіз та технології машинного навчання допомагають визначати невідповідності між законами та постановами, що сприяє узгодженості правової бази. Також автоматизовані системи можуть відстежувати зміни в законодавстві та оперативно інформувати зацікавлені державні органи.

Проведений аналіз вказує на те, що застосування ШІ значно оптимізує документообіг, оскільки системи можуть автоматично визначати тип документа (законодавчий акт, звернення, нормативний документ) та спрямовувати його до відповідного органу влади. Завдяки технологіям NLP забезпечується не лише правильна класифікація документів, але й аналіз їх змісту для точного розподілу завдань між відповідними структурами.

З точки зору державної політики, ці тенденції актуалізують потребу в забезпеченні відкритості та доступності інформації для громадян. Використання централізованих баз даних, які застосовують ШІ для індексації та швидкого пошуку документів, сприяє підвищенню рівня громадського контролю, зменшенню корупційних ризиків та зміцненню довіри до державних органів.

Водночас, поряд із перевагами, впровадження таких інновацій у системі державного управління може призвести до кібератак на сервери державних установ, витоку конфіденційної інформації, компрометацію облікових даних та маніпуляції з електронними підписами. Надалі державні інформаційні системи в цілому стануть привабливою мішенню для хакерів, зокрема з боку організованих кіберзлочинних угруповань та держав-агресорів, що прагнуть дестабілізувати функціонування владних структур.

З огляду на це, необхідно запроваджувати лише комплексний підхід до захисту інформаційних систем, що дозволить мінімізувати потенційні

кіберзагрози та забезпечити стабільне функціонування державних установ у цифровому середовищі.

Розглядаючи архітектуру програмного забезпечення системи обробки документів за допомогою штучного інтелекту (Рис. 4), слід відзначити, що вона базується на технологіях NLP. Дана структура включає кілька ключових модулів, кожен з яких виконує специфічні функції, зокрема попередню обробку документів, вилучення ключових сутностей (NER), класифікацію текстів, синтаксичний аналіз та лематизацію.

Завдяки такій модульній організації система здатна автоматично розпізнавати та аналізувати зміст документів, визначати їхню структуру, виділяти важливі елементи (імена, дати, організації) та зберігати отримані дані у відповідних базах. Це забезпечує швидкий пошук, оптимізацію документообігу та спрощує доступ до необхідної інформації.

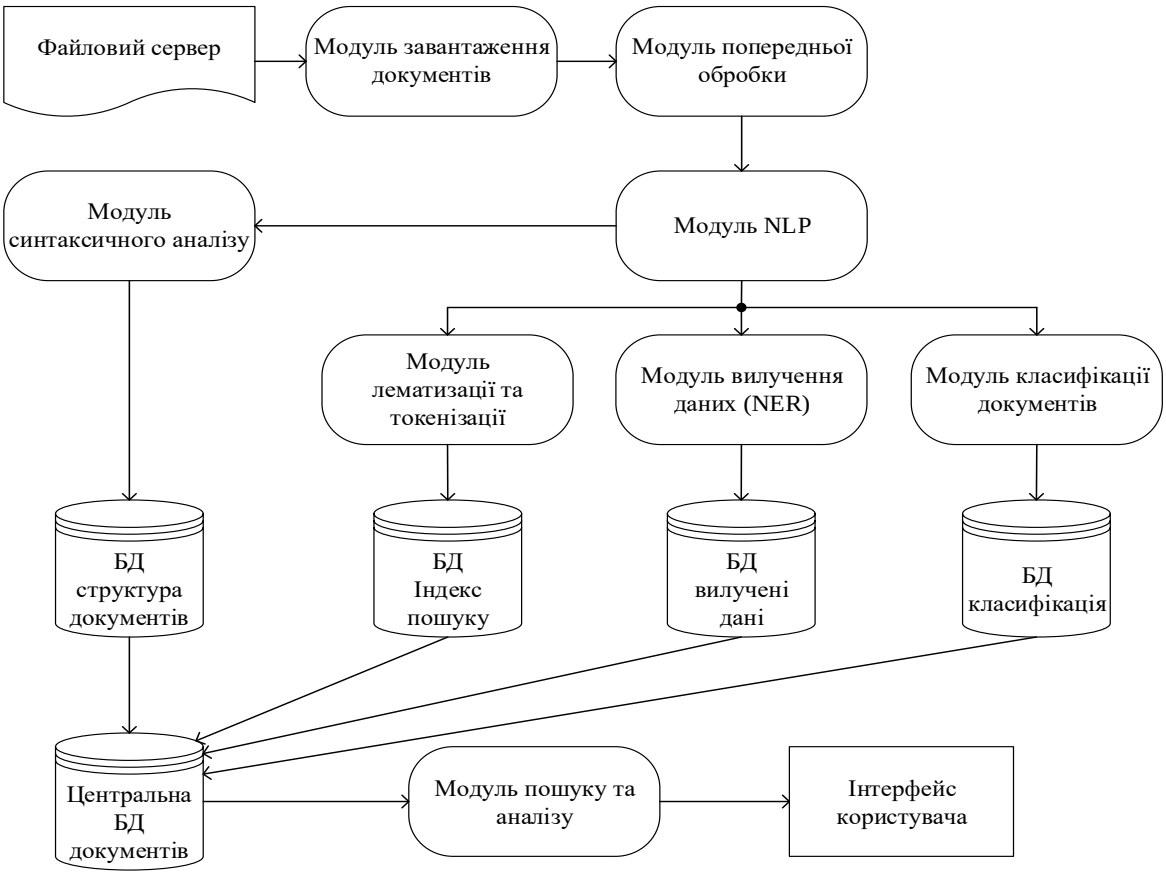


Рис. 4. – Структура архітектури програмного забезпечення системи електронного документообігу

*Джерело: розробка автора.

Використання NLP-моделі забезпечує високий рівень точності обробки текстових даних, що дозволяє автоматизувати процеси класифікації, аналізу та вилучення ключової інформації з документів. Це, в свою чергу, зменшує ризик людських помилок і значно скорочує час, необхідний для опрацювання великого обсягу текстової інформації.

Опис компонентів та їх роль в системі державного управління:

Файловий сервер

– Використовується для зберігання вхідних документів, таких як звернення громадян, нормативні акти, адміністративні накази.

– Забезпечує централізоване сховище офіційної документації.

Модуль завантаження документів

– Відповідає за завантаження документів у систему державного електронного документообігу.

– Може інтегруватися з електронними платформами подачі звернень та запитів.

Модуль попередньої обробки

– Виконує очищення та підготовку документів для подальшого аналізу.

– Наприклад, розпізнає текст із сканованих документів, усуває зайві символи та форматування.

Модуль NLP

– Основний компонент обробки тексту, який аналізує зміст документа, витягує ключові дані та проводить класифікацію.

– Використовується для автоматизації процесу аналізу документів у державних органах.

Модуль синтаксичного аналізу

– Досліджує структуру документа, визначає логічні зв’язки між його елементами.

– Допомагає у формуванні зв’язків між нормативними актами або у виявленні суперечностей.

Модуль лематизації та токенізації

– Нормалізує текст для подальшого аналізу, розбиває його на окремі слова та фрази.

– Оптимізує пошук документів за ключовими словами у державних архівах.

Модуль вилучення даних (NER)

– Використовується для виявлення ключових сутностей у документах (імена, назви установ, дати, місця).

– Може застосовуватися для автоматичного визначення відповідальних державних органів або категоризації звернень громадян.

Модуль класифікації документів

– Визначає тип документа (закон, наказ, звернення, звіт), що дозволяє автоматично спрямовувати його до відповідної структури.

– Дозволяє розподіляти документи між міністерствами, департаментами або окремими посадовцями.

Бази даних (класифікація, вилучені дані, індекс пошуку, структура документів)

– Використовуються для зберігання та обробки структурованої інформації про документи.

– Допомагають у швидкому доступі до необхідних даних державним службовцям.

Центральна база даних документів

– Основне сховище всіх оброблених документів, доступне для державних органів.

– Використовується для зберігання нормативних актів, законодавчих ініціатив, розпоряджень уряду та рішень місцевої влади.

Модуль пошуку та аналізу

– Дозволяє державним службовцям та громадянам знаходити необхідні документи за ключовими словами, датами, авторами.

– Підтримує аналітичні запити, наприклад, виявлення змін у законодавстві або аналіз публічних контрактів.

Інтерфейс користувача

– Фронтенд-система, через яку громадяни, юристи або державні службовці можуть взаємодіяти з базою документів.

– Може використовуватися для подачі запитів, отримання аналітики, перегляду офіційних документів.

У контексті державного управління така система може бути ефективним інструментом для оптимізації документообігу, підвищення ефективності роботи державних установ, прискорення розгляду запитів громадян та покращення якості адміністративних послуг. Крім того, її застосування сприятиме автоматизованому моніторингу нормативно-правових актів, що дасть змогу вчасно виявляти зміни у законодавстві, забезпечувати їхню узгодженість та оперативно реагувати на правові новації.

Таким чином, впровадження NLP-моделі у сфері державного управління сприятиме не лише підвищенню продуктивності та точності обробки документів, а й загальному вдосконаленню процесів управління, прозорості та доступності державних послуг.

Підсумовуючи, можна констатувати, що ШІ може стати потужним інструментом у сфері державного управління, сприяючи автоматизації рутинних процесів, покращенню аналізу даних та підвищенню ефективності прийняття рішень. Зокрема, впровадження штучного інтелекту у документообіг державних установ може значно прискорити обробку звернень громадян, автоматизувати класифікацію документів та забезпечити оперативний моніторинг нормативно-правових актів.

Однак, застосування ШІ потребує ретельного контролю, оскільки його алгоритми можуть містити упередження, а рішення, які він пропонує, не завжди відповідають правовим та етичним нормам. Тому важливо розвивати та використовувати ШІ з усвідомленням його можливостей і обмежень, дотримуючись етичних стандартів, принципів відкритості та підзвітності.

Враховуючи зазначене важливо звернути увагу на те, що для ефективного впровадження ШІ в державне управління необхідно розробляти відповідні

регуляторні механізми, що визначатимуть сфери його застосування, рівень відповідальності за ухвалені на його основі рішення та механізми запобігання можливим ризикам. Подальші дослідження мають бути спрямовані на пошук ефективних методів впровадження цих технологій у державні органи, розробку алгоритмів, що відповідають принципам правової визначеності та справедливості, а також удосконалення механізмів контролю за їхнім використанням.

В цілому збалансований підхід до розвитку ШІ дозволить не лише максимізувати користь від його застосування у державному управлінні, а й забезпечити безпеку та довіру громадян до цифрових інновацій.

Впровадження штучного інтелекту у системи електронного документообігу підвищує ефективність управління документами, автоматизуючи їхню обробку, аналіз і класифікацію. Технології NLP дозволяють швидко структурувати дані, ідентифікувати ключові сутності та оперативно реагувати на запити.

Однак, аналіз архітектури програмних рішень, що базуються на ШІ, супроводжується низкою викликів.

По-перше, це безпекові ризики, які включають збільшення кіберзагроз, витоків інформації та маніпуляцій даними. Це вимагає реалізації комплексних механізмів захисту, зокрема багатофакторної автентифікації, криптографічних методів шифрування та систем моніторингу безпеки.

По-друге, питання прогнозованості та надійності роботи ШІ залишається відкритим, оскільки сучасні генеративні моделі (LLM), що використовуються у документообігу, постійно донавчаються, що може призвести до непередбачуваності результатів їхньої роботи. Це викликає необхідність створення контрольованих середовищ для навчання ШІ та підготовки спеціальних моделей, орієнтованих на роботу для державних потреб.

По-третє, слід враховувати етичні та правові аспекти впровадження ШІ, адже автоматичне ухвалення рішень потребує чітко визначених механізмів підзвітності для уникнення дискримінації або некоректної обробки даних. Окрім

цього, нормативно-правова база для використання ШІ в державному управлінні має бути оновлена відповідно до міжнародних стандартів.

Четверте, ефективність ШІ у документообігу значно підвищується при його інтеграції з системами управління підприємствами (ERP), реєстрами державних органів, CRM-системами та аналітичними платформами, що дасть змогу створити єдину екосистему для роботи з документами та автоматизувати прийняття рішень.

Перспективи подальших досліджень прямо пов’язуються з необхідністю розвивати спеціалізовані моделі штучного інтелекту для обробки юридичних документів, нормативно-правових актів та запитів громадян, що відповідатимуть вимогам точності та правової визначеності. Важливим напрямом є створення гібридних систем, що поєднують автоматичний аналіз даних із можливістю перевірки рішень людиною (Human-in-the-loop), особливо для критично важливих документів. Також необхідно розробити стандарти кібербезпеки для захисту даних, оброблюваних штучним інтелектом, включаючи національні вимоги до криптографії та управління доступом. Вдосконалення нормативно-правового регулювання впровадження ШІ в державному управлінні має забезпечити його відповідність міжнародним стандартам цифрової безпеки та етики.

Зрештою, використання ШІ в електронному документообігу має значний потенціал для оптимізації процесів, підвищення швидкості обробки інформації та мінімізації людських помилок. Водночас успішне впровадження цієї технології потребує комплексного підходу, який враховує технічні, правові та етичні аспекти, а також забезпечення високого рівня захисту даних.

2.3. Принципи формування єдиного захищеного інформаційного середовища електронних документів складових сектору оборони держави

Досвід країн Європейського Союзу у сфері розбудови електронного урядування та створення захищених інформаційних середовищ для

електронного документообігу має особливе значення для формування відповідних систем в оборонному секторі України. Електронне урядування у європейських країнах еволюціонувало протягом останніх десятиліть від окремих інформаційних систем до комплексних рішень з електронної взаємодії, що функціонують на основі єдиних принципів та стандартів.

Європейський Союз визначив розвиток електронного урядування як один із пріоритетних напрямів становлення єдиного цифрового ринку. У результаті цієї політики було створено низку загальноєвропейських програм та ініціатив, спрямованих на розвиток електронної взаємодії між органами державної влади, зокрема у безпековому та оборонному секторах [176].

Ключовим документом у цьому контексті став "План дій розвитку електронного урядування ЄС 2016-2020", який окреслив базові принципи електронної взаємодії:

- "Digital by Default" (цифровий за замовчуванням) – передбачає пріоритетність впровадження цифрових каналів надання послуг та здійснення управлінських процесів;
- "Once Only Principle" (принцип єдиного введення даних) – забезпечує одноразове введення та багаторазове використання даних у різних інформаційних системах;
- "Inclusiveness and Accessibility" (інклюзивність та доступність) – гарантує рівний доступ усіх категорій користувачів до електронних сервісів;
- "Openness and Transparency" (відкритість та прозорість) – забезпечує відкритість даних та прозорість адміністративних процесів;
- "Cross-border by Default" (транскордонність за замовчуванням) – передбачає функціонування електронних сервісів незалежно від державних кордонів;
- "Interoperability by Default" (сумісність за замовчуванням) – забезпечує технічну, семантичну та організаційну сумісність інформаційних систем;
- "Trustworthiness and Security" (надійність та безпека) – гарантує захист даних та стійкість інформаційних систем до кіберзагроз [176].

Важливо зазначити, що останній принцип має особливе значення для оборонного сектору, оскільки забезпечує необхідний рівень захисту інформації з обмеженим доступом. Виходячи з цього, у 2016 році було прийнято Директиву ЄС з мережевої та інформаційної безпеки (NIS Directive), яка встановила єдині вимоги до захисту інформаційних систем критичної інфраструктури, включаючи системи оборонного призначення [183].

Відповідно до програми ISA² (Interoperability Solutions for European Public Administrations, Businesses and Citizens), що діяла протягом 2016-2020 років, було розроблено Європейську рамкову програму інтероперабельності (European Interoperability Framework, EIF), яка встановлює основні принципи забезпечення сумісності інформаційних систем публічного управління [178]. Ця програма стала логічним продовженням попередньої ініціативи ISA, що функціонувала у 2010-2015 роках і заклала основи для системної роботи з інтероперабельності європейських інформаційних систем.

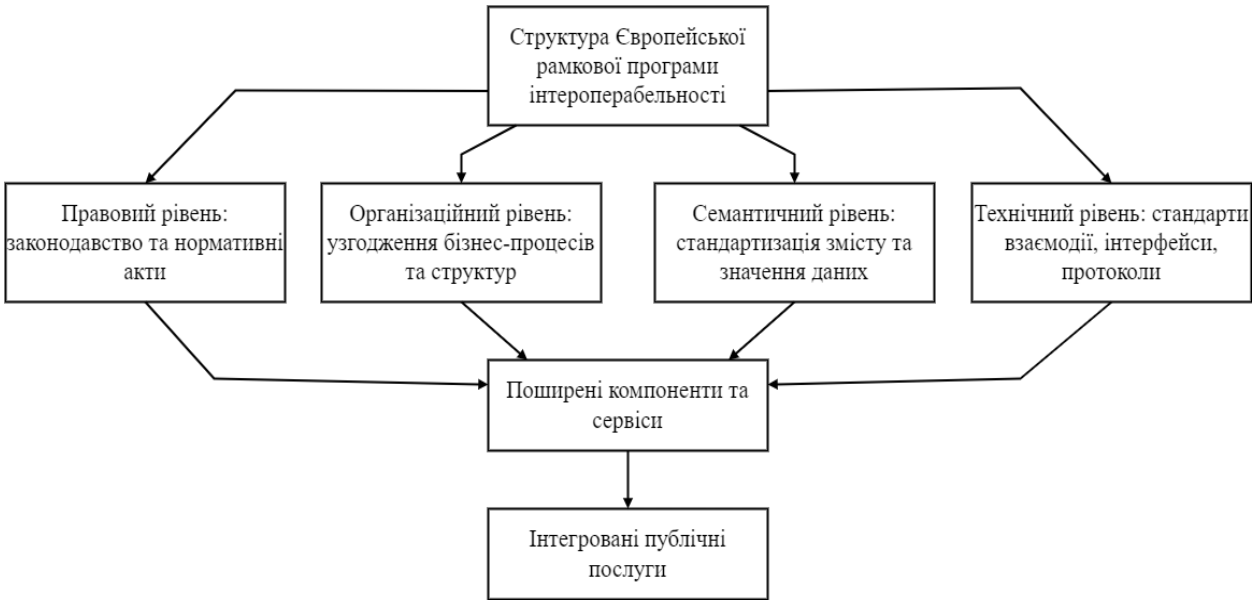


Рис. 5. Структурні рівні Європейської рамкової програми інтероперабельності [178]

Для забезпечення ефективної імплементації EIF було розроблено програму EIRA (European Interoperability Reference Architecture), яка визначає архітектурні блоки для створення інтероперабельних цифрових публічних послуг. В підсумку

це дозволило створити єдиний підхід до забезпечення сумісності інформаційних систем у різних секторах, включаючи оборонний [179].

Важливим аспектом загальноєвропейського підходу до електронної взаємодії є особлива увага до питань кібербезпеки. У 2019 році було прийнято Регламент ЄС щодо кібербезпеки (EU Cybersecurity Act), який запровадив систему сертифікації засобів захисту інформації та встановив вимоги до їх використання в критичній інфраструктурі [187]. Таким чином, було створено єдиний підхід до забезпечення безпеки інформаційних систем на європейському рівні.

Окрему увагу у європейських підходах приділено питанням захисту персональних даних. Загальний регламент про захист даних (General Data Protection Regulation, GDPR), що набув чинності у 2018 році, встановив єдині вимоги до обробки персональних даних, включаючи дані службовців оборонних відомств [185]. Звідси випливає необхідність впровадження спеціальних механізмів захисту персональних даних у системах електронного документообігу оборонного призначення.

Європейська оборонна агенція (European Defence Agency, EDA) розробила спеціалізовану програму кіберзахисту для оборонних відомств держав-членів ЄС, яка включає рекомендації щодо створення захищених інформаційних середовищ для електронного документообігу [112]. На її основі формуються національні стратегії кібербезпеки у сфері оборони та впроваджуються відповідні технічні рішення.

Таким чином, аналіз загальноєвропейських підходів дозволяє виокремити ключові принципи побудови захищених інформаційних середовищ:

1. Забезпечення інтероперабельності на всіх рівнях: правовому, організаційному, семантичному та технічному.
2. Пріоритетність безпеки та захисту даних.
3. Стандартизація форматів електронних документів.
4. Реалізація багаторівневої аутентифікації та авторизації.
5. Застосування технологій шифрування та цифрових підписів.

6. Впровадження механізмів контролю цілісності інформації.
7. Забезпечення неперервності функціонування інформаційних систем.
8. Регулярний аудит безпеки та тестування на проникнення.
9. Впровадження систем виявлення та запобігання вторгненням.
10. Формування культури інформаційної безпеки та підвищення компетентності персоналу.

Розглянемо досвід окремих країн ЄС у побудові захищених інформаційних середовищ для оборонного сектору.

Естонія: X-Road як основа електронної взаємодії. Досвід Естонії, яка є одним із світових лідерів електронного урядування, має особливе значення в контексті розробки захищених інформаційних середовищ. Основою естонської системи електронної взаємодії стала платформа X-Road, яка забезпечує захищений обмін даними між різними державними інформаційними системами, включаючи системи оборонного відомства [169].

Історія розвитку X-Road бере початок з 2001 року, коли було запроваджено першу версію системи, спрямовану на інтеграцію державних баз даних. Протягом наступних років система постійно вдосконалювалася і наразі представляє собою комплексне рішення для забезпечення захищеної взаємодії між різними інформаційними системами. У результаті еволюції X-Road, в системі було реалізовано принцип децентралізованої архітектури, що значно підвищило її стійкість до кібератак [234].

Ключовим елементом X-Road є система безпеки, яка базується на концепції “Security Server”, що забезпечує захищений обмін даними між різними інформаційними системами. Кожен учасник інформаційної взаємодії має власний “Security Server”, який відповідає за автентифікацію, авторизацію, шифрування та підписання повідомлень [171]. Відповідно, це дозволяє забезпечити високий рівень захисту інформації при її передачі між різними системами.

Виходячи з цього, можна виокремити ключові принципи побудови естонської системи:

– Децентралізований підхід до зберігання даних, що передбачає розподілене зберігання інформації без створення єдиної центральної бази даних

– Використання технології блокчейн для забезпечення цілісності даних, що унеможливлює їх несанкціоновану модифікацію

– Застосування багаторівневої системи аутентифікації, включаючи використання цифрових сертифікатів, смарт-карт та мобільної ідентифікації

– Використання електронних ID-карток для ідентифікації користувачів, що забезпечує високий рівень довіри до ідентифікаційних даних

– Забезпечення захищеного електронного обміну документами між цивільними та військовими структурами на основі єдиних стандартів та протоколів

– Застосування end-to-end шифрування при передачі даних, що забезпечує їх конфіденційність

– Використання технології часових міток для забезпечення неспростовності передачі документів

– Впровадження систем моніторингу та аудиту для контролю за доступом до інформаційних ресурсів

Особливістю естонської системи є реалізація принципу “безшовної інтеграції” різних інформаційних систем при збереженні автономності їх функціонування. З цього випливає можливість оперативної взаємодії між різними відомствами при збереженні необхідного рівня захисту інформації.

Система X-Road активно використовується у сфері оборони Естонії для забезпечення захищеного обміну даними між різними підрозділами оборонного відомства, а також для взаємодії з іншими державними органами. Таким чином, забезпечується оперативність прийняття рішень та ефективність управління обороннними ресурсами [174].

Окремий інтерес представляє досвід Естонії щодо впровадження системи цифрової стійкості (digital resilience), спрямованої на забезпечення безперервності функціонування державних інформаційних систем в умовах кібератак та інших надзвичайних ситуацій. Однією з ключових складових цієї

системи є технологія “data embassy” (посольство даних), яка передбачає зберігання резервних копій критичних державних інформаційних ресурсів на захищених серверах, розташованих за межами країни [214]. У результаті реалізації цього підходу значно підвищується стійкість інформаційних систем до різноманітних загроз, включаючи фізичне знищення інформаційної інфраструктури.

Німеччина: GSTOOL та IT-Grundschutz. Німеччина розробила комплексну систему стандартів та інструментів для забезпечення безпеки інформаційних систем державного управління, відому як IT-Grundschutz. У рамках цієї системи було створено спеціалізоване програмне забезпечення GSTOOL, яке широко використовується в оборонному секторі для оцінки ризиків та планування заходів із забезпечення інформаційної безпеки [150].

IT-Grundschutz представляє собою методику, розроблену Федеральним управлінням з інформаційної безпеки Німеччини (BSI), яка визначає стандартні заходи безпеки для типових сценаріїв використання інформаційних технологій. Методика охоплює технічні, організаційні, кадрові та інфраструктурні аспекти інформаційної безпеки [152]. Відповідно до цієї методики, процес забезпечення інформаційної безпеки включає п'ять основних етапів: ініціалізацію процесу, визначення об'єктів захисту, вибір заходів захисту, реалізацію заходів та підтримку процесу.

Особливістю німецького підходу є детальна каталогізація загроз та відповідних заходів безпеки. Каталог IT-Grundschutz включає понад 1000 рекомендацій щодо захисту різних компонентів інформаційних систем, що дозволяє системно підходити до забезпечення інформаційної безпеки [147]. В підсумку це забезпечує комплексний захист інформаційних систем на всіх рівнях.

Таким чином ми бачимо, що німецький підхід характеризується:

– Системністю та методичністю в оцінці інформаційних ризиків, що базується на детальному аналізі потенційних загроз та вразливостей

– Чіткою регламентацією процесів документообігу, включаючи визначення ролей та відповідальності всіх учасників процесу

– Реалізацією принципу розподілу прав доступу, що передбачає надання користувачам мінімально необхідних прав для виконання їх функціональних обов'язків

– Застосуванням спеціалізованих криптографічних алгоритмів для захисту інформації оборонного призначення, відповідно до рівня її конфіденційності

– Впровадженням стандартизованих процедур управління інцидентами інформаційної безпеки

– Регулярним проведенням незалежного аудиту безпеки інформаційних систем

– Систематичним навчанням персоналу з питань інформаційної безпеки

– Впровадженням принципу "security by design" при розробці нових інформаційних систем

У Німеччині також діє спеціалізована система електронного документообігу для оборонного сектору – SASPF (Standard-Anwendungs-Software-Produkt-Familie), яка забезпечує захищений обмін документами між різними підрозділами Бундесверу та іншими державними органами. Система базується на програмному забезпеченні SAP і адаптована до специфічних потреб оборонного відомства. З цього випливає можливість використання комерційних рішень для побудови захищених інформаційних середовищ за умови їх відповідної адаптації та сертифікації.

Особливу увагу в німецькому підході приділено забезпеченню безпеки систем електронного документообігу в умовах підвищеної загрози кібератак. Для цього впроваджено концепцію "Secure Information Sharing" (безпечний обмін інформацією), яка передбачає використання спеціальних технічних рішень для обміну документами між системами з різними рівнями захисту [148]. Таким чином, забезпечується можливість контрольованої передачі документів між різними контурами безпеки.

Фінляндія: TUVE та TORI. Фінляндія реалізувала проект TUVE (Turvallisuusverkko), спрямований на створення захищеної мережі комунікацій для органів державної влади, відповідальних за безпеку та оборону. Паралельно було впроваджено програму TORI, що забезпечує централізоване надання IT-послуг для державного сектору.

Проект TUVE був ініційований у 2009 році з метою створення надійної та захищеної мережевої інфраструктури для органів безпеки та оборони Фінляндії. Основними користувачами мережі є Міністерство оборони, Збройні сили, прикордонна служба, поліція, екстрені служби та інші критично важливі державні органи [194]. Виходячи з цього, можна стверджувати, що система орієнтована на забезпечення координації дій різних силових структур у кризових ситуаціях.

Архітектура TUVE базується на концепції ізольованої захищеної мережі, фізично відокремленої від інтернету та інших публічних мереж. Для зв'язку з зовнішніми мережами використовуються спеціальні шлюзи з багаторівневим захистом, що забезпечують контрольований обмін інформацією. Звідси випливає високий рівень захищеності інформації, що циркулює в мережі TUVE.

Основними принципами фінської системи є:

- Сегментація мереж відповідно до рівня секретності інформації, що передбачає фізичне та логічне розділення мереж з різними рівнями захисту.
- Застосування багаторівневого захисту (defense-in-depth), який включає комплекс організаційних, технічних та криптографічних заходів безпеки.
- Централізований моніторинг безпеки, що здійснюється спеціалізованим центром оперативного реагування на кіберінциденти (CERT).
- Використання шифрування для захисту каналів передачі даних, що забезпечує конфіденційність інформації під час її передачі.
- Впровадження механізмів безперервності функціонування, включаючи резервування критичних компонентів та каналів зв'язку.
- Застосування суворої автентифікації та авторизації користувачів.
- Регулярне тестування на проникнення та оцінка вразливостей.

- Використання сертифікованих засобів захисту інформації.

Програма TORI (Toimialariippumattomat tieto- ja viestintätekniset palvelut) була запроваджена як доповнення до TUVE і спрямована на централізацію та стандартизацію надання IT-послуг для державного сектору Фінляндії [192]. В підсумку це дозволило оптимізувати витрати на інформаційні технології та підвищити загальний рівень інформаційної безпеки.

У результаті впровадження цих систем Фінляндія значно підвищила рівень захищеності своїх інформаційних ресурсів, особливо у сфері оборони та національної безпеки. Досвід Фінляндії демонструє ефективність комплексного підходу до забезпечення інформаційної безпеки, що поєднує централізоване управління з децентралізованою реалізацією заходів безпеки.

Особливий інтерес представляє фінський досвід організації захищеного міжвідомчого документообігу в кризових ситуаціях. Для цього в рамках мережі TUVE впроваджено спеціалізовану систему KEJO, яка забезпечує оперативний обмін інформацією між службами екстреного реагування, правоохоронними органами та оборонними структурами [197]. Таким чином, забезпечується ефективна координація дій різних відомств при реагуванні на кризові ситуації.

Франція: RGS та комплексний підхід до захисту державних інформаційних систем. Франція розробила комплексну методологію забезпечення безпеки державних інформаційних систем, відому як Загальний регламент безпеки (Référentiel Général de Sécurité, RGS). Цей регламент встановлює єдині вимоги до безпеки інформаційних систем державних органів, включаючи оборонні відомства [138].

RGS базується на міжнародних стандартах інформаційної безпеки, зокрема на стандартах серії ISO 27000, але адаптований до специфічних потреб французької державної адміністрації. Регламент визначає три основні компоненти безпеки: функції безпеки, рівні гарантії та правила використання [137]. Виходячи з цього, для кожної інформаційної системи визначається необхідний рівень безпеки та відповідні заходи захисту.

Особливістю французького підходу є чітка класифікація інформаційних систем за рівнем критичності та відповідні вимоги до їх захисту. Для систем оборонного призначення передбачено найвищий рівень захисту з використанням сертифікованих засобів криптографічного захисту інформації [142]. Таким чином, забезпечується диференційований підхід до захисту інформаційних ресурсів залежно від їх важливості та конфіденційності.

Для захисту електронного документообігу у Франції широко застосовується система кваліфікованих електронних підписів, що базується на національній інфраструктурі відкритих ключів (PKI). Для цього створено систему акредитованих центрів сертифікації (Prestataires de Services de Certification Électronique, PSCE), які відповідають за випуск та управління цифровими сертифікатами [140]. У результаті це дозволяє забезпечити юридичну значущість електронних документів та їх захист від підробки.

У оборонному секторі Франції впроваджено спеціалізовану систему електронного документообігу SILRIA (Système d'Information Logistique pour le Réapprovisionnement Interarmées et les Achats), яка забезпечує захищений обмін документами між різними підрозділами збройних сил та оборонними підприємствами. Звідси випливає можливість створення єдиного інформаційного простору в оборонному секторі за умови застосування відповідних заходів безпеки.

Нідерланди: DigiD та Digikoppeling. Досвід Нідерландів у сфері електронної взаємодії державних органів представляє особливий інтерес завдяки впровадженню системи цифрової ідентифікації DigiD та стандарту обміну даними Digikoppeling [168]. Ці рішення забезпечують надійну ідентифікацію користувачів та захищений обмін даними між різними інформаційними системами.

Система DigiD (Digital Identity) була запроваджена у 2005 році і наразі є основним засобом електронної ідентифікації громадян при їх взаємодії з державними органами Нідерландів. Система підтримує різні рівні гарантії ідентифікації, включаючи базовий рівень (логін та пароль), середній рівень

(логін, пароль та SMS-код) та високий рівень (логін, пароль та електронний ID-card) [209]. Відповідно, для доступу до різних систем використовується відповідний рівень ідентифікації залежно від чутливості інформації.

Стандарт Digikoppeling визначає єдині протоколи та формати обміну даними між інформаційними системами державних органів Нідерландів. Стандарт базується на міжнародних протоколах (SOAP, WSDL, WS-Security) та забезпечує надійну автентифікацію, шифрування та підписання повідомлень [210]. В підсумку це дозволяє створити єдине захищене середовище для обміну електронними документами між різними відомствами.

Для оборонного сектору Нідерландів розроблено спеціалізовану систему електронного документообігу MULAN (Multi-Level Approved Network), яка забезпечує можливість роботи з документами різних рівнів секретності в єдиному інтерфейсі [167]. Таким чином, спрощується робота з документами при одночасному забезпеченні їх надійного захисту.

Цікавим аспектом нідерландського підходу є активне використання публічних API (Application Programming Interface) для організації взаємодії між інформаційними системами. Для цього створено єдиний реєстр API (API Register), який містить опис всіх доступних інтерфейсів та умови їх використання [166]. З цього випливає можливість гнучкої інтеграції різних систем при збереженні необхідного рівня безпеки.

Для більш детального розуміння європейських практик у сфері створення захищених інформаційних середовищ доцільно провести порівняльний аналіз підходів різних країн за ключовими параметрами (Таблиця 3).

Порівняльний аналіз європейських підходів до забезпечення безпеки інформаційних середовищ дозволяє виявити як спільні принципи, так і національні особливості. Виходячи з цього, можна зробити наступні висновки щодо основних тенденцій у цій сфері.

Таблиця 3. Порівняльний аналіз підходів країн ЄС до забезпечення безпеки інформаційних середовищ електронних документів в оборонному секторі

Країна	Основні технологічні рішення	Правова база	Особливості підходу до безпеки	Рівень інтегр-ї з цив. сист.	Методи криптогр. зах.	Відпов-сть станд. НАТО
Німеччина	IT-Grundschutz, GSTOOL, SASPF, SINA	Закони: про захист даних/безпеку IT-систем/BSI-Standards/	Систематична каталогізація загроз, методичність у впровадженні заходів безпеки, принцип “security by design”	Середній	ECC, AES-256, власні криптографічні алгоритми	Повна
Фінляндія	TUVE, TORI, KEJO	Закони: про управління інформаційною безпекою в державному секторі/електронні послуги	Фізична сегментація мереж, багаторівневий захист, централізоване управління безпекою	Обмежений	RSA, ECC, AES-256, OTP для особливо важливих даних	Повна
Франція	RGS, SILRIA, PSCE, SECOIA	Загальний регламент безпеки (RGS)/Закон про цифрову довіру	Диференційований підхід за рівнем критичності, національна система сертифікації засобів захисту	Середній	RSA, ECC, AES-256, власні криптографічні	Повна
Нідерланди	DigiD, Digikoppeling, MULAN	Закон про електронні підписи/захист даних	Публічні API з контрольованим доступом, багаторівнева аутентифікація	Високий	RSA, ECC, AES-256	Повна

*Джерело: розробка автора на основі [7-27]

По-перше, всі розглянуті країни дотримуються принципу багаторівневого захисту (defense-in-depth), який передбачає впровадження кількох незалежних рівнів безпеки. Таким чином, компрометація одного рівня захисту не призводить до компрометації всієї системи, що є особливо важливим для оборонного сектору.

По-друге, спостерігається тенденція до стандартизації та уніфікації підходів до інформаційної безпеки на європейському рівні. У результаті створюються єдині стандарти та протоколи, що забезпечують інтероперабельність інформаційних систем різних країн, зокрема в рамках НАТО.

По-третє, ключовою складовою безпеки електронного документообігу в оборонному секторі є надійна ідентифікація та автентифікація користувачів. Відповідно, всі розглянуті країни впроваджують багатофакторну аутентифікацію та використовують цифрові сертифікати для автентифікації користувачів та підписання документів.

По-четверте, важливим аспектом забезпечення безпеки є розмежування доступу до інформації за принципом “need-to-know” (необхідно знати). З цього випливає необхідність створення складних систем управління доступом, які враховують роль користувача, його приналежність до певного підрозділу, його рівень допуску та інші фактори.

По-п’яте, спостерігається тенденція до інтеграції систем електронного документообігу оборонного сектору з цивільними системами, але з дотриманням необхідних заходів безпеки. Звідси випливає необхідність створення спеціальних шлюзів та інтерфейсів, які забезпечують контрольований обмін інформацією між системами з різними рівнями захисту.

По-шосте, всі розглянуті країни приділяють значну увагу питанням навчання персоналу та формування культури інформаційної безпеки. Таким чином забезпечується мінімізація ризиків, пов'язаних із людським фактором, який часто є найслабшою ланкою в системі інформаційної безпеки.

По-сьоме, спостерігається тенденція до впровадження технологій блокчейн для забезпечення цілісності електронних документів та неспростовності їх передачі. В підсумку це дозволяє створити надійний аудиторський слід та запобігти несанкціонованій модифікації документів.

Окремо слід відзначити різний рівень інтеграції систем електронного документообігу оборонного сектору з цивільними системами. Естонія та

Нідерланди демонструють високий рівень інтеграції, що дозволяє забезпечити ефективну взаємодію між різними відомствами. Німеччина та Франція дотримуються більш консервативного підходу, забезпечуючи обмежену інтеграцію з дотриманням суворих заходів безпеки. Фінляндія демонструє найбільш консервативний підхід, забезпечуючи фізичне розділення мереж оборонного призначення та інших мереж.

Для оцінки ефективності заходів безпеки інформаційних середовищ у оборонному секторі країн ЄС доцільно провести аналіз рівня їх захищеності за ключовими параметрами. Для цього використаємо методику оцінки рівня зрілості процесів інформаційної безпеки, яка базується на моделі COBIT (Control Objectives for Information and Related Technology) [205].

Відповідно до цієї методики, рівень зрілості процесів інформаційної безпеки оцінюється за шкалою від 0 до 5, де:

0 – процес відсутній

1 – процес є початковим, хаотичним

2 – процес є повторюваним, але інтуїтивним

3 – процес є визначеним

4 – процес є керованим та вимірюваним

5 – процес є оптимізованим

У таблиці 4 представлено результати оцінки рівня зрілості процесів інформаційної безпеки в системах електронного документообігу оборонного сектору розглянутих країн.

Аналіз даних, представлених у таблиці 4, дозволяє зробити наступні висновки:

Естонія та Фінляндія демонструють найвищий середній рівень зрілості процесів інформаційної безпеки (4,75), що свідчить про високу ефективність їх підходів до забезпечення безпеки інформаційних середовищ у оборонному секторі. Особливо варто відзначити їх досягнення у сфері управління доступом, управління інцидентами, криптографічного захисту та аудиту.

Таблиця 4**.** Оцінка рівня зрілості процесів інформаційної безпеки в системах електронного документообігу оборонного сектору країн ЄС

Процес	Естонія	Німеччина	Фінляндія	Франція	Нідерланди
Управління доступом	5	5	5	5	4
Управління інцидентами	5	4	5	4	4
Управління вразливостями	4	5	4	4	4
Управління безперервністю	5	4	5	4	3
Криптографічний захист	5	5	5	5	4
Фізична безпека	4	5	5	4	4
Аудит та моніторинг	5	4	5	4	4
Навчання персоналу	5	4	4	4	4
Середній рівень	4,75	4,5	4,75	4,25	3,88

*Джерело: розробка автора на основі [7-27] та методики COBIT

Німеччина займає друге місце за середнім рівнем зрілості процесів (4,5), демонструючи особливо високі показники у сфері управління доступом, управління вразливостями, криптографічного захисту та фізичної безпеки. Виходячи з цього, можна стверджувати, що німецький підхід до каталогізації загроз та методичного впровадження заходів безпеки є досить ефективним.

Франція демонструє середній рівень зрілості 4,25, що також є високим показником. Особливо варто відзначити досягнення у сфері управління доступом та криптографічного захисту. Таким чином, французький підхід до диференціації заходів безпеки залежно від рівня критичності систем також є досить ефективним.

Нідерланди демонструють найнижчий серед розглянутих країн середній рівень зрілості процесів (3,88), що, втім, є досить високим показником. Варто відзначити, що найнижчий показник спостерігається у сфері управління безперервністю (3), що може бути пов’язано з високим рівнем інтеграції систем оборонного сектору з цивільними системами.

Варто також відзначити, що всі розглянуті країни демонструють високий рівень зрілості процесів управління доступом та криптографічного захисту, що

свідчить про ключову роль цих процесів у забезпеченні безпеки систем електронного документообігу в оборонному секторі.

Для візуалізації результатів аналізу рівня зрілості процесів інформаційної безпеки в розглянутих країнах представимо їх у вигляді пелюсткової діаграми (рис. 5).

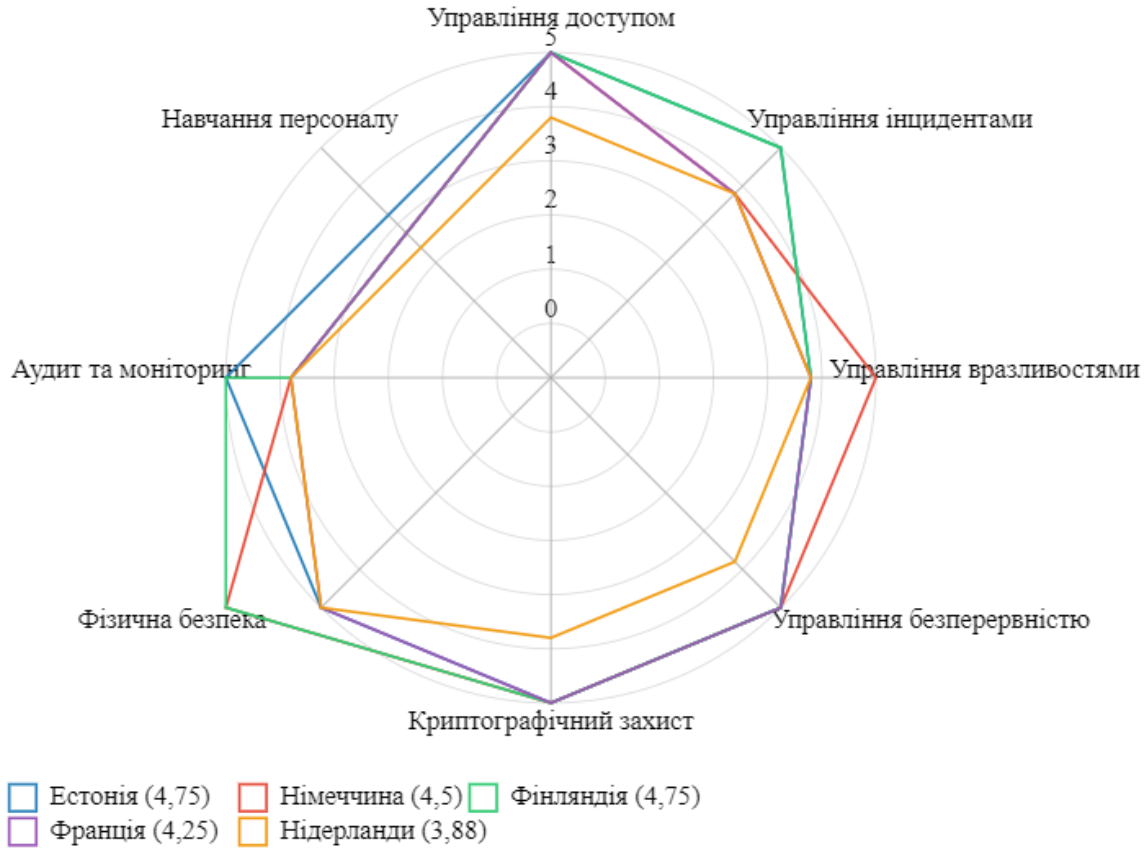


Рис. 5. Порівняння рівня зрілості процесів інформаційної безпеки в країнах ЄС

***Примітка**: Наведена візуалізація представлена у вигляді пелюсткової діаграми, де по осях розташовані процеси інформаційної безпеки, а значення відображають рівень зрілості кожного процесу в конкретній країні.*

Висновки та рекомендації щодо імплементації європейського досвіду в Україні. Проведений аналіз досвіду європейських країн у сфері створення захищених інформаційних середовищ для електронного документообігу в оборонному секторі дозволяє сформулювати ряд висновків та рекомендацій щодо його імплементації в Україні.

По-перше, досвід Естонії щодо впровадження децентралізованої архітектури системи електронної взаємодії X-Road та використання технології блокчейн для забезпечення цілісності даних може бути особливо цінним для України. Виходячи з цього, доцільним є впровадження аналогічної децентралізованої архітектури для системи електронної взаємодії в оборонному секторі України, що дозволить підвищити її стійкість до кібератак та забезпечити надійне функціонування в умовах військових дій.

По-друге, німецький досвід систематичної каталогізації загроз та методичного впровадження заходів безпеки може бути використаний для створення національної методики оцінки ризиків та забезпечення безпеки інформаційних систем оборонного сектору України. Відповідно, доцільним є розробка національного каталогу загроз та заходів безпеки, адаптованого до специфіки оборонного сектору України.

По-третє, фінський досвід фізичної сегментації мереж та багаторівневого захисту може бути особливо цінним для забезпечення безпеки систем електронного документообігу в умовах підвищеної загрози кібератак. Таким чином, доцільним є впровадження аналогічної архітектури в оборонному секторі України, що передбачає фізичне розділення мереж з різним рівнем секретності та створення захищених шлюзів для контрольованого обміну інформацією.

По-четверте, французький досвід диференційованого підходу до забезпечення безпеки інформаційних систем залежно від їх критичності може бути використаний для оптимізації витрат на інформаційну безпеку в оборонному секторі України. Звідси випливає необхідність розробки методики оцінки критичності інформаційних систем та відповідних вимог до їх захисту.

По-п’яте, нідерландський досвід використання публічних API для організації взаємодії між інформаційними системами може бути корисним для забезпечення гнучкої інтеграції систем електронного документообігу оборонного сектору з іншими державними інформаційними системами. У результаті це дозволить забезпечити ефективну взаємодію різних відомств при збереженні необхідного рівня безпеки.

Враховуючи проведений аналіз, можна сформулювати наступні рекомендації щодо імплементації європейського досвіду в Україні:

Розробка національної стратегії кібербезпеки оборонного сектору, яка враховуватиме кращі європейські практики та буде адаптована до специфіки національної системи безпеки та оборони.

Впровадження децентралізованої архітектури системи електронної взаємодії в оборонному секторі, що базується на принципах X-Road, з використанням технології блокчейн для забезпечення цілісності даних.

Розроблення національної методики оцінки ризиків та забезпечення безпеки електронно-комунікаційних систем та мереж оборонного сектору, що базується на принципах IT-Grundschutz, але враховує специфіку українського оборонного сектору.

Впровадження багаторівневої системи захисту електронно-комунікаційних систем та мереж оборонного сектору, що включає фізичну сегментацію мереж, багаторівневу автентифікацію та авторизацію, шифрування даних та контрольований обмін інформацією між системами з різними рівнями секретності.

Розроблення системи класифікації інформаційних систем за рівнем критичності та відповідних вимог до їх захисту, що дозволить оптимізувати витрати на інформаційну безпеку.

Впровадження системи публічних API для організації взаємодії між електронно-комунікаційними системами та мережами оборонного сектору та іншими державними інформаційними системами з контрольованим доступом та відповідними заходами безпеки.

Розроблення програми підвищення компетентності персоналу у сфері інформаційної безпеки, що включає регулярні навчання, тренінги та періодичну оцінку знань.

Впровадження системи незалежного аудиту безпеки інформаційних систем оборонного сектору для своєчасного виявлення та усунення вразливостей.

Створення системи управління безперервністю функціонування інформаційних систем оборонного сектору, що забезпечить їх надійну роботу в умовах кризових ситуацій.

Забезпечення відповідності національних стандартів інформаційної безпеки в оборонному секторі стандартам НАТО, що сприятиме інтероперабельності систем електронного документообігу України з відповідними системами країн-членів НАТО.

В цілому імплементація цих рекомендацій дозволить підвищити рівень захищеності інформаційних середовищ для електронного документообігу в оборонному секторі України, забезпечити їх відповідність кращим європейським практикам та стандартам НАТО, а також створити умови для ефективної взаємодії з відповідними системами країн-партнерів.

РОЗДІЛ 3. НАПРЯМИ РОЗВИТКУ ТА УДОСКОНАЛЕННЯ ЕЛЕКТРОННОГО МІЖВІДОМЧОГО ДОКУМЕНТООБІГУ СФЕРИ ОБОРОНИ

3.1. Загальні засади функціонування та використання системи електронної взаємодії органів виконавчої влади

Система електронної взаємодії органів виконавчої влади (СЕВ ОВВ) є центральним елементом інфраструктури електронного урядування в Україні. Її основною метою є автоматизація процесів документообігу, підвищення ефективності міжвідомчої взаємодії та забезпечення прозорості державного управління. У результаті впровадження СЕВ ОВВ вони отримують можливість створювати, обробляти, надсилати, зберігати та знищувати електронні документи з використанням кваліфікованого електронного підпису, що забезпечує їх юридичну значущість. Таким чином, СЕВ ОВВ відіграє ключову роль у модернізації державного управління, сприяючи цифровізації адміністративних процесів. Цей підрозділ роботи присвячений детальному аналізу нормативно-правових, організаційних, технічних і функціональних засад СЕВ ОВВ, а також оцінці її переваг, викликів і перспектив розвитку.

Нормативно-правова база СЕВ ОВВ. Функціонування СЕВ ОВВ ґрунтується на комплексній нормативно-правовій базі, яка регулює створення, впровадження та використання системи. Виходячи з цього, ключовими нормативними актами є:

1. **Закон України “Про електронні документи та електронний документообіг”** (2003) встановлює правові засади електронного документообігу, визначаючи порядок створення, використання та зберігання електронних документів. На основі цього закону забезпечується юридична значущість документів, створених у СЕВ ОВВ [46].
2. **Закон України “Про електронний цифровий підпис”** (2003, зі змінами) регулює використання кваліфікованого електронного підпису, який є

обов’язковим для документів у СЕВ ОВВ. З цього випливає, що підпис забезпечує автентичність і цілісність документів [**Error! Reference source not found.**].

3. **Постанова Кабінету Міністрів України від 18 липня 2012 року № 670** затверджує Положення про СЕВ ОВВ, яке визначає структуру, функції держателя, адміністратора та користувачів системи. Відповідно, цей документ є основою для організаційного функціонування системи [92].

4. **Постанова Кабінету Міністрів України від 17 січня 2018 року № 55** встановлює Регламент організації взаємодії органів виконавчої влади в електронній формі, що сприяє автоматизації міжвідомчого документообігу. Таким чином, уніфікуються процеси обміну інформацією [91].

5. **Наказ Міністерства юстиції України від 1 листопада 2012 року № 1600/5** затверджує Порядок роботи з електронними документами через СЕВ ОВВ, зокрема використання електронного підпису [81].

Звідси випливає, що нормативно-правова база забезпечує комплексний підхід до регулювання СЕВ ОВВ, створюючи умови для її ефективного функціонування. Виходячи з цього, робимо висновок, що чітке правове регулювання є передумовою для успішної реалізації системи в державному управлінні.

Організаційна структура та учасники СЕВ ОВВ. СЕВ ОВВ функціонує як державна телекомунікаційна система, що забезпечує електронну взаємодію між органами виконавчої влади, органами місцевого самоврядування та іншими установами, підключеними до системи. У результаті організаційна структура системи включає кілька ключових учасників:

- Утримувач системи – Міністерство цифрової трансформації України, яке відповідає за стратегічний розвиток, координацію та контроль функціонування СЕВ ОВВ. На основі цього забезпечується єдина державна політика у сфері цифровізації.
- Адміністратор системи – Державне підприємство «Дія», яке здійснює технічне адміністрування, забезпечує підтримку користувачів і захист

інформації. Таким чином, ДП «Дія» відіграє ключову роль у підтримці безперебійної роботи системи.

- Користувачі системи – посадові особи Секретаріату Кабінету Міністрів України, міністерств, центральних і місцевих органів виконавчої влади, Ради міністрів Автономної Республіки Крим та інших підключених установ. Відповідно, система охоплює широке коло суб'єктів державного управління.

Виходячи з цього, СЕВ ОВВ забезпечує єдиний цифровий простір для міжвідомчої взаємодії, що охоплює як центральні, так і місцеві органи влади. Таким чином ми бачимо, що організаційна структура системи є гнучкою та адаптованою до потреб різних рівнів державного управління.

Функціональні можливості СЕВ ОВВ. СЕВ ОВВ надає широкий спектр функціональних можливостей, спрямованих на автоматизацію документообігу та підвищення ефективності державного управління. Основними функціями є:

1. Створення та оброблення електронних документів із використанням кваліфікованого електронного підпису, що забезпечує їх юридичну значущість. У результаті документи, створені в системі, мають таку ж правову силу, як і паперові.
2. Надсилання, передавання та отримання документів між органами влади в електронній формі. З цього випливає, що система значно скорочує час обробки документів і знижує витрати на паперове діловодство.
3. Зберігання та знищення документів відповідно до вимог законодавства про архівну справу. Таким чином, забезпечується відповідність системи нормам архівного діловодства.
4. Контроль виконання управлінських рішень, включаючи акти та протокольні рішення Кабінету Міністрів України. На основі цього органи влади можуть ефективно відстежувати виконання завдань.

Звідси випливає, що СЕВ ОВВ є комплексною системою, яка охоплює всі етапи життєвого циклу електронного документа. Виходячи з цього, робимо висновок, що система сприяє оптимізації адміністративних процесів і підвищенню прозорості державного управління.

Технічна інфраструктура СЕВ ОВВ базується на сучасних інформаційно-комунікаційних технологіях (ІКТ), що забезпечують її надійність, масштабованість і безпеку. Основні технічні аспекти включають:

- Захист інформації. Комплексна система захисту інформації (КСЗІ) забезпечує конфіденційність, цілісність і доступність даних. У результаті СЕВ ОВВ відповідає вимогам нормативних документів із технічного захисту інформації, що підтверджується Атестатом відповідності КСЗІ ядра СЕВ ОВВ версії 2.0 від 20 грудня 2019 року [**Error! Reference source not found.**].
- Інтеграція з іншими системами. СЕВ ОВВ інтегрується з відомчими системами електронного документообігу, такими як FossDoc, що забезпечує єдиний інформаційний простір. Таким чином ми бачимо, що система є частиною ширшої екосистеми електронного урядування.
- Хмарні технології. Використання хмарного середовища дозволяє забезпечити доступність системи для всіх підключених користувачів, незалежно від їхнього технічного забезпечення. Відповідно, це сприяє інклюзивності системи.
- Захищені канали зв’язку. Для документів із конфіденційною інформацією може використовуватися Національна система конфіденційного зв’язку. З цього випливає, що система здатна адаптуватися до різних вимог безпеки.

Виходячи з цього, технічна інфраструктура СЕВ ОВВ є сучасною та відповідає викликам цифрової епохи. Таким чином, система забезпечує надійне та безпечне середовище для міжвідомчої взаємодії.

У результаті впровадження СЕВ ОВВ органи виконавчої влади отримують низку значних переваг:

1. **Підвищення ефективності.** Автоматизація документообігу скорочує час на обробку документів і знижує адміністративні витрати. На основі цього підвищується продуктивність роботи державних службовців.

2. **Прозорість і контроль.** Система забезпечує моніторинг виконання управлінських рішень, що сприяє прозорості діяльності органів влади. Звідси випливає, що СЕВ ОВВ сприяє підзвітності державного управління.

3. **Екологічність.** Перехід на електронний документообіг зменшує використання паперу, що відповідає принципам сталого розвитку. Таким чином, система сприяє екологічній модернізації державного управління.

4. **Доступність.** Хмарний інтерфейс СЕВ-СЕД дозволяє підключатися малим організаціям із обмеженим технічним ресурсом, наприклад, органам місцевого самоврядування. Відповідно, система є інклюзивною для всіх рівнів управління.

Незважаючи на переваги, впровадження та використання СЕВ ОВВ супроводжується певними викликами:

1. **Технічна готовність.** Не всі органи місцевого самоврядування мають достатню технічну базу для повноцінного використання СЕВ ОВВ. У результаті виникають труднощі з інтеграцією системи на місцевому рівні.

2. **Кваліфікація кадрів.** Недостатній рівень підготовки державних службовців у сфері ІКТ може ускладнювати впровадження системи. З цього випливає, що необхідне додаткове навчання персоналу.

3. **Стандартизація.** Відсутність уніфікованих форматів даних у деяких відомчих системах ускладнює міжвідомчий обмін. Виходячи з цього, робимо висновок, що потрібна подальша гармонізація стандартів.

4. **Інформаційна безпека.** Хоча система має КСЗІ, зростаючі кіберзагрози вимагають постійного вдосконалення заходів захисту. Таким чином, інформаційна безпека залишається ключовим викликом.

У підсумку, подальший розвиток СЕВ ОВВ пов’язаний із низкою стратегічних ініціатив, спрямованих на підвищення її ефективності та масштабованості. Зокрема, передбачається:

1. **Поглиблення інтеграції.** Розширення взаємодії СЕВ ОВВ з іншими державними інформаційними системами, такими як Єдиний державний портал

адміністративних послуг. На основі цього створюватиметься єдиний цифровий простір для всіх державних сервісів.

2. **Розширення доступу.** Залучення більшої кількості органів місцевого самоврядування до системи. Таким чином ми бачимо, що СЕВ ОВВ має потенціал охопити всі рівні державного управління.

3. **Впровадження нових технологій.** Використання технологій блокчейн для підвищення безпеки та прозорості документообігу. З цього випливає, що система може адаптуватися до новітніх технологічних трендів.

4. **Навчання кадрів.** Розробка програм підготовки державних службовців для ефективного використання СЕВ ОВВ. Відповідно, це сприятиме подоланню кадрових викликів.

Виходячи з цього, можливо зробити висновок, що СЕВ ОВВ має значний потенціал для подальшого розвитку, який сприятиме реалізації концепції електронного урядування в Україні.

У підсумку, система електронної взаємодії органів виконавчої влади є ключовим інструментом цифрової трансформації державного управління в Україні. На основі її функціональних можливостей забезпечується автоматизація документообігу, підвищення прозорості та ефективності міжвідомчої взаємодії. Таким чином ми бачимо, що СЕВ ОВВ відіграє важливу роль у модернізації адміністративних процесів і гарматування України до європейських стандартів електронного урядування. Проте, виходячи з цього, для реалізації її потенціалу необхідно подолати технічні, організаційні та кадрові виклики, а також продовжити вдосконалення нормативно-правової бази та технічної інфраструктури. З цього випливає, що СЕВ ОВВ залишатиметься пріоритетним напрямом розвитку цифрової держави.

3.2. Розробка проекту єдиної системи електронного міжвідомчого документообігу сфери оборони в електронно-комунікаційних системах різного призначення та різного рівня складності

Сучасні умови розвитку інформаційного суспільства та зростання загроз у сфері безпеки, зокрема в умовах гібридної війни, вимагають від оборонного сектору України впровадження інноваційних рішень для ефективного управління інформаційними потоками. Єдина система електронного міжвідомчого документообігу (ЄСЕМД) у сфері оборони покликана забезпечити оперативний, безпечний і стандартизований обмін документами між різними відомствами, такими як Міністерство оборони України, Генеральний штаб Збройних Сил України, Державна служба спеціального зв'язку та захисту інформації та іншими структурами. Така система має інтегрувати електронно-комунікаційні системи різного призначення (військові, адміністративні, логістичні) та рівня складності (від локальних до національних) [138], забезпечуючи їх сумісність і захист даних.

Актуальність розробки ЄСЕМД зумовлена необхідністю підвищення оперативності прийняття рішень, зниження бюрократичних витрат і забезпечення високого рівня інформаційної безпеки. За даними Національного інституту стратегічних досліджень, цифрова трансформація оборонного сектору є одним із пріоритетів України в умовах інтеграції до європейського цифрового простору [1]. Водночас складність реалізації проекту полягає в гетерогенності наявних ЕКС, різноманітності стандартів і високих вимогах до захисту інформації з обмеженим доступом.

Метою цього розділу є аналіз ключових аспектів розробки проекту ЄСЕМД, включаючи вимоги до системи, її архітектуру, механізми захисту інформації, виклики інтеграції та шляхи їх вирішення. Розділ структуровано для послідовного висвітлення технічних, організаційних і нормативних аспектів, що забезпечують створення ефективної системи документообігу.

Традиційні паперові та частково автоматизовані системи документообігу в оборонній сфері України мають низку недоліків: високу трудомісткість, ризик втрати даних, низьку швидкість обробки та обмежену сумісність між відомствами. Наприклад, обмін документами між військовими частинами та центральними органами часто потребує фізичного транспортування, що знижує

оперативність і підвищує вразливість до витоку інформації. За оцінками експертів, до 30% часу управлінських процесів у Збройних Силах України витрачається на ручну обробку документів [**Error! Reference source not found.**].

Автоматизовані системи, що використовуються в окремих відомствах, часто базуються на різних платформах і не забезпечують повноцінної інтеграції. Наприклад, системи управління логістикою можуть не синхронізуватися з системами кадрового обліку, що ускладнює комплексне планування. Ця проблема особливо гостра в умовах воєнного стану, коли швидкість і точність обміну інформацією є критичними.

ЄСЕМД покликана усунути ці недоліки шляхом:

- Уніфікації процесів – створення єдиних стандартів оформлення, обробки та зберігання документів.
- Оперативності – автоматизація передачі документів між відомствами в реальному часі.
- Безпеки – впровадження комплексних систем захисту інформації (КСЗІ) для даних із грифами “таємно” та “цілком таємно”.
- Сумісності – інтеграція ІТС різного призначення (військові, адміністративні) та складності (локальні, регіональні, національні).
- Економії ресурсів – скорочення витрат на паперові носії, логістику та адміністративний персонал.

Згідно з європейським досвідом, впровадження подібних систем (наприклад, e-Government у Естонії) підвищує ефективність управління на 20–40% [171]. Для України це особливо важливо в контексті євроінтеграції та модернізації оборонного сектору.

Вимоги до єдиної системи електронного документообігу:

Функціональні вимоги

ЄСЕМД має забезпечувати такі основні функції:

- **Реєстрація та обробка** документів. Автоматичне створення, класифікація, маршрутизація та архівування документів.

– Міжвідомчий обмін. Безпечна передача документів між ІТС різних відомств із підтримкою електронного цифрового підпису (ЕЦП).

– Контроль виконання. Моніторинг статусу документів і завдань у реальному часі.

– Інтеграція з іншими системами. Синхронізація з логістичними, фінансовими та кадровими ІТС.

– Доступність. Забезпечення роботи в умовах обмеженого зв'язку (офлайн-режим із подальшою синхронізацією).

– Нефункціональні вимоги

– Безпека. Відповідність стандартам захисту інформації, включаючи криптографічний захист і автентифікацію користувачів.

– Масштабованість. Можливість розширення системи для нових відомств і типів документів.

– Надійність. Гарантована доступність системи на рівні 99,9% (згідно з міжнародними стандартами для критичних ІТС).

– Інтероперабельність. Сумісність із міжнародними стандартами, такими як European Interoperability Framework (EIF) [182].

– Ергономічність. Зручний інтерфейс для користувачів із різним рівнем підготовки.

Нормативні вимоги

Система має відповідати таким нормативним документам України:

– Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [47].

– Закон України "Про електронні довірчі послуги" [**Error! Reference source not found.**].

– Правила забезпечення захисту інформації в ЕКС, затверджені постановою КМУ № 373 [**Error! Reference source not found.**].

– Державні стандарти серії ДСТУ ISO/IEC 27001 щодо управління інформаційною безпекою [**Error! Reference source not found.**].

Архітектура ЄСЕМД базується на модульному підході, що дозволяє інтегрувати ІТС різного призначення та складності. Основні компоненти:

- **Центральний сервер** – координує обмін даними, забезпечує зберігання та обробку документів.
- Локальні модулі – встановлюються в окремих відомствах для автономної роботи та синхронізації з центральним сервером.
- Шлюзи безпеки – забезпечують шифрування даних під час передачі між ІТС.
- Інтерфейси користувача – веб- і десктоп-додатки для доступу до системи.
- API для інтеграції – дозволяють підключати зовнішні системи (наприклад, логістичні чи фінансові).
- Для реалізації технологічного стеку системи пропонується:
- Бази даних – PostgreSQL для зберігання документів і метаданих із підтримкою шифрування.
- Мови програмування – Java або Python для серверної логіки, JavaScript (React) для фронтенду.
- Протоколи безпеки – TLS 1.3 для захищеної передачі даних, OAuth 2.0 для автентифікації.
- Криптографія – алгоритми ДСТУ 4145-2002 для ЕЦП і шифрування [**Error! Reference source not found.**].
- Хмарні технології – використання гібридної хмари для масштабування та резервування.

Інтеграція ЕКС різного рівня складності

ЕКС у сфері оборони різняться за масштабом (локальні, регіональні, національні) і призначенням (військові, адміністративні, логістичні). Для їх інтеграції пропонується:

- **Уніфіковані протоколи.** Використання стандартів SOAP або REST для обміну даними.

– Адаптери. Програмні модулі для конвертації форматів даних між системами.

– Система “Трембіта”. Українська платформа інтероперабельності, яка забезпечує обмін даними між державними ЕКС [123].

Захист інформації в ЄСЕМД:

Основні загрози

Система оброблятиме дані з обмеженим доступом, тому ключовими загрозами є:

– Несанкціонований доступ до даних.

– Витік інформації через кібератаки (DDoS, фішинг, зловмисне ПЗ).

– Порушення цілісності документів.

– Втрата даних через технічні збої.

Комплексна система захисту інформації (КСЗІ)

Для протидії загрозам необхідно впровадити КСЗІ, яка включає:

– Криптографічний захист. Шифрування документів за стандартом ДСТУ 4145-2002, використання ЕЦП для автентифікації [**Error! Reference source not found.**].

– Контроль доступу. Рольова модель (RBAC) із двофакторною автентифікацією.

– Моніторинг і аудит. Виявлення аномалій у реальному часі, журналювання дій користувачів.

– Резервне копіювання. Розподілені резервні копії з періодичною перевіркою цілісності.

– Фізична безпека. Розташування серверів у захищених дата-центрах.

– Відповідність стандартам

КСЗІ має відповідати:

– ДСТУ ISO/IEC 27001:2015 (управління інформаційною безпекою) [**Error! Reference source not found.**].

– Постанові КМУ № 373 щодо захисту інформації в ІТС [7].

– Вимогам НАТО до кібербезпеки, якщо система використовуватиметься в міжнародних операціях [**Error! Reference source not found.**].

Виклики розробки та шляхи їх вирішення:

Технічні виклики

– **Гетерогенність ЕКС.** Різні відомства використовують застарілі або власні системи.

Рішення: Розробка адаптерів і використання відкритих API для інтеграції.

– **Обмежена пропускна здатність.** Військові ЕКС можуть працювати в умовах слабкого зв'язку.

Рішення: Впровадження офлайн-режиму з кешуванням і синхронізацією.

– **Масштабування.** Зростання кількості користувачів і документів. **Рішення**: Використання хмарних технологій і розподілених баз даних.

Організаційні виклики

– **Координація між відомствами.** Різні пріоритети та бюрократичні процедури.

Рішення: Створення міжвідомчої робочої групи під егідою Міноборони.

– **Навчання персоналу.** Низький рівень цифрової грамотності в окремих підрозділах.

Рішення: Проведення тренінгів і розробка інтуїтивного інтерфейсу.

– **Фінансування.** Висока вартість розробки та впровадження.

Рішення: Залучення міжнародної технічної допомоги, наприклад, через програму Ukraine Facility [233].

Безпекові виклики

– **Кібератаки.** Зростання загроз в умовах інформаційної війни. **Рішення**: Впровадження систем раннього виявлення та регулярні пентести.

– **Витік даних.** Помилки користувачів або інсайдерські загрози. **Рішення**: Обов'язкове навчання з кібергігієни та моніторинг дій.

Нормативно-правова база

Розробка ЄСЕМД регулюється такими документами:

- Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” № 80/94-ВР [47].
- Закон України “Про електронні довірчі послуги” № 2155-VIII [**Error! Reference source not found.**].
- Постанова КМУ від 29.03.2006 № 373 “Про затвердження Правил забезпечення захисту інформації” [**Error! Reference source not found.**].
- Указ Президента України від 27.09.1999 № 1229 “Про Положення про технічний захист інформації” [118].
- ДСТУ ISO/IEC 27001:2015 “Інформаційна безпека” [**Error! Reference source not found.**].
- Стратегія кібербезпеки України (2021–2025) [105].

Міжнародні стандарти, такі як EIF і NATO STANAG, також враховуються для забезпечення сумісності з партнерами [182, **Error! Reference source not found.**].

Перспективи впровадження

Етапи реалізації

- **Аналіз і проектування (6–12 місяців).** Визначення вимог, розробка ТЗ, створення прототипу.
- **Розробка та тестування (12–18 місяців).** Кодування модулів, інтеграція з ІТС, пілотне тестування.
- **Впровадження (6–12 місяців).** Розгортання системи, навчання користувачів, перехід на повну експлуатацію.
- **Підтримка та модернізація.** Постійне оновлення безпеки та функціоналу.

Очікувані результати

- Скорочення часу обробки документів на 50–70%.
- Підвищення безпеки даних завдяки КСЗІ.
- Зниження витрат на адміністративні процеси на 20–30%.
- Забезпечення сумісності з міжнародними партнерами (НАТО, ЄС).

Підсумовуючи, необхідно зазначити, що досвід Естонії (система X-Road) та Фінляндії (e-Government) показує, що уніфіковані системи документообігу підвищують ефективність державного управління [171]. Для України ці приклади можуть бути адаптовані з урахуванням оборонної специфіки.

Отже, розробка єдиної системи електронного міжвідомчого документообігу для сфери оборони є стратегічно важливим завданням, яке сприятиме підвищенню ефективності управління, безпеки даних і оперативності прийняття рішень [155]. Ключовими аспектами проекту є:

- Уніфікація процесів документообігу в гетерогенних ІТС.
- Впровадження комплексної системи захисту інформації, що відповідає національним і міжнародним стандартам.
- Забезпечення інтероперабельності через стандартизовані протоколи та платформи, такі як «Трембіта».
- Подолання технічних і організаційних викликів шляхом координації, навчання та фінансування.

Подальші дослідження мають зосередитися на розробці детальних технічних специфікацій, пілотному тестуванні та адаптації міжнародного досвіду. Впровадження ЄСЕМД стане важливим кроком у цифровій трансформації оборонного сектору України, сприяючи її інтеграції до європейського безпекового простору.

3.3. Принципові напрями розгортання захищеного документообігу на платформах штучного інтелекту

Сучасні тенденції цифрової трансформації документообігу в організаціях різних типів зумовлюють необхідність пошуку інноваційних рішень, які б забезпечували одночасно високу ефективність обробки документів та надійний захист конфіденційної інформації. Використання технологій штучного інтелекту, зокрема великих мовних моделей (LLM), відкриває принципово нові

можливості для автоматизації процесів документообігу, проте водночас створює додаткові виклики в контексті інформаційної безпеки [191].

Ключовою проблемою при розгортанні документообігу на базі штучного інтелекту залишається пошук оптимального балансу між функціональністю, продуктивністю та безпекою системи. Традиційні хмарні рішення на основі ШІ забезпечують високу обчислювальну потужність, але призводять до потенційних ризиків витоку конфіденційних даних через необхідність їх передачі на сторонні сервери [157]. Локальні ж рішення, хоча й мінімізують ризики компрометації даних, часто стикаються з обмеженнями в обчислювальних ресурсах та функціональних можливостях.

У цьому контексті інтеграція інструментів локального розгортання LLM, таких як Ollama та DeepSeek-R1, в контейнеризовану інфраструктуру на базі Docker Desktop представляється перспективним напрямом для створення захищених систем документообігу. Такий підхід потенційно дозволяє поєднати переваги хмарних та локальних рішень, забезпечуючи ефективну обробку, аналіз та зберігання документів з дотриманням високих стандартів інформаційної безпеки [220].

Проблематика застосування технологій штучного інтелекту в системах документообігу привертає значну увагу наукової спільноти. Аналіз публікацій останніх років демонструє зростання інтересу до використання великих мовних моделей для оптимізації процесів обробки документів.

Дослідження [230] визначають ключові тенденції в галузі інтелектуальної обробки документів (IDP) та підкреслюють трансформаційний потенціал технологій ШІ для автоматизації робочих процесів, прискорення процедур затвердження та вдосконалення механізмів виявлення шахрайства. Показано, що впровадження IDP у фінансовому секторі дозволяє скоротити час обробки документів на 70% та підвищити ефективність виявлення шахрайських схем на 50%.

Колектив авторів DeepSeek AI [202] представив комплексне дослідження моделі DeepSeek-R1, яка демонструє значний потенціал у сферах творчого

мислення, генерації програмного коду, вирішення математичних задач та автоматизованого рефакторингу програм. Особливу увагу дослідники приділяють функціональності самостійного обмірковування (self-reflection), реалізованої за допомогою технології навчання з підкріпленням, що дозволяє моделі ефективно опрацьовувати складні документи.

Zhang з співавторами [236] провели порівняльний аналіз різних великих мовних моделей для вирішення комплексних завдань, включаючи обробку документів. Їх дослідження підтверджує, що DeepSeek-R1, хоча й потребує більшої кількості обчислювальних ресурсів порівняно з аналогами, забезпечує високу точність навіть для найскладніших задач, що робить її перспективною для застосування в системах документообігу з підвищеними вимогами до якості обробки.

Derczynski, та Galinkin [159] акцентують увагу на проблематиці безпеки великих мовних моделей і представляють фреймворк Garak для тестування вразливостей LLM. Дослідники виявили, що деякі моделі, включаючи DeepSeek-R1, потенційно можуть генерувати небезпечні відповіді за певних умов, що підкреслює необхідність впровадження комплексних стратегій мінімізації ризиків та проведення регулярного тестування безпеки. Вони також розробили методологію автоматизованого виявлення вразливостей в LLM з використанням утиліти Garak. Їхнє дослідження демонструє ефективність даного підходу для своєчасної ідентифікації та нейтралізації потенційних загроз, пов’язаних з використанням великих мовних моделей у критичних системах, включаючи документообіг.

Sahana Upadhya [226] досліджує особливості використання Docker для розгортання додатків штучного інтелекту та машинного навчання. Автори аналізують аспекти продуктивності та безпеки контейнеризованих рішень, надаючи рекомендації щодо оптимальної конфігурації для різних типів AI/ML додатків.

Деякі компанії вже пропонують комплекс найкращих практик забезпечення безпеки Docker-контейнерів, включаючи методи верифікації

образів, перевірки можливостей та вибору надійних сховищ. Їхні дослідження особливо актуальні в контексті розгортання захищених систем документообігу на базі контейнеризованої інфраструктури.

H. R. Penubadi та співавтори [203] представили всеохоплюючу методологічну основу для безпечного управління документами в регульованих галузях. Автори детально аналізують взаємозв'язок між технологічними рішеннями, організаційними процесами та нормативними вимогами, що є критично важливим для впровадження систем захищеного документообігу в секторах з підвищеними вимогами до конфіденційності даних.

Незважаючи на значний обсяг досліджень у галузі застосування технологій ШІ в документообігу, питання ефективної інтеграції локальних LLM з контейнеризованою інфраструктурою залишається недостатньо вивченим [143]. Зокрема, існує потреба в комплексному аналізі переваг, ризиків та перспектив такої інтеграції, а також у розробці практичних рекомендацій щодо розгортання захищених систем документообігу на базі штучного інтелекту.

Аналіз наукової літератури свідчить про наявність кількох суттєвих прогалин у дослідженнях захищеного документообігу на платформах штучного інтелекту:

1. Недостатньо досліджена ефективність інтеграції локальних LLM, зокрема Ollama та DeepSeek-R1, з контейнеризованою інфраструктурою на базі Docker Desktop для забезпечення захищеного документообігу.

2. Відсутній комплексний аналіз безпекових ризиків, пов'язаних з використанням великих мовних моделей у системах документообігу, та методологій їх мінімізації.

3. Не розроблено чітких рекомендацій щодо архітектурної організації багаторівневих систем захищеного документообігу на базі ШІ, що враховували б специфіку локально розгорнутих LLM.

4. Недостатньо вивчено питання оптимального балансу між функціональністю, продуктивністю та безпекою в системах документообігу на базі локальних LLM.

5. Відсутні емпіричні дослідження ефективності застосування DeepSeek-R1 для специфічних задач документообігу в порівнянні з іншими моделями.

Метою даного підрозділу є комплексний аналіз принципових напрямів розгортання захищеного документообігу на платформах штучного інтелекту з використанням локальних LLM та контейнеризованої інфраструктури, а також розробка практичних рекомендацій щодо впровадження таких систем.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Дослідити технологічні особливості та функціональні можливості інструментів Ollama та DeepSeek-R1 в контексті їх застосування в системах документообігу.

2. Проаналізувати переваги, обмеження та ризики контейнеризації додатків ШІ на базі Docker Desktop для забезпечення захищеного документообігу.

3. Розробити концептуальну модель багаторівневої архітектури системи захищеного документообігу на базі локальних LLM та контейнеризованої інфраструктури.

4. Ідентифікувати ключові безпекові ризики, пов’язані з використанням великих мовних моделей у системах документообігу, та запропонувати методологію їх мінімізації.

5. Сформулювати практичні рекомендації щодо розгортання та налаштування систем захищеного документообігу на базі Ollama, DeepSeek-R1 та Docker Desktop.

6. Визначити перспективні напрями подальших досліджень у галузі застосування технологій ШІ для захищеного документообігу.

Вирішення цих завдань дозволить сформувати комплексне розуміння проблематики розгортання захищеного документообігу на платформах штучного інтелекту та запропонувати ефективні підходи до впровадження таких систем у практичну діяльність організацій різного типу.

З моменту появи генеративних моделей штучного інтелекту, зокрема ChatGPT, постало питання щодо забезпечення конфіденційності користувацьких даних при використанні таких технологій у документообігу. Хмарні сервіси генеративного ШІ викликають обґрунтовані занепокоєння щодо безпеки даних, оскільки інформація передається на сторонні сервери для обробки. Альтернативним підходом стало розгортання великих мовних моделей (LLM) локально, що суттєво підвищує рівень захисту даних при збереженні функціональних можливостей ШІ для роботи з документами.

Одним із перспективних інструментів для локального використання LLM є Ollama – програмне забезпечення з відкритим вихідним кодом, що дозволяє запускати великі мовні моделі безпосередньо на персональному комп'ютері користувача [222]. Основними перевагами Ollama є:

1. Приватність даних – вся обробка інформації відбувається локально, без передачі на зовнішні сервери, що забезпечує високий рівень конфіденційності.
2. Різноманітність підтримуваних моделей – платформа сумісна з широким спектром LLM, включаючи Llama 2, Mistral, Gemma та інші [158].
3. Простота використання – процес встановлення та налаштування є інтуїтивно зрозумілим і не потребує спеціальних знань.
4. Гнучкість конфігурації – наявність інструменту Modfile дозволяє тонко налаштовувати параметри моделі відповідно до специфічних завдань документообігу [220].
5. Можливість автономної роботи – після завантаження моделі її використання не потребує підключення до мережі Інтернет.

На сучасному етапі розвитку технологій існує кілька альтернативних інструментів для роботи з локальними LLM. Серед них: LM Studio [208], llamafile [215], Jan [207], NextChat [218], Faraday.dev [189], Backyard AI [144] та GPT4All [200]. Кожен з цих інструментів має свої особливості щодо підтримуваних моделей, зручності користувацького інтерфейсу, сумісності з різними платформами та ліцензійні умови.

Нами було зроблено порівняння характеристик та особливостей існуючого програмного забезпечення для роботи з локальними LLM, зокрема таких інструментів, як Ollama, LM Studio, llamafile, Jan, NextChat, Faraday.dev, Backyard AI та GPT4All. Результати цього порівняння представлені у таблиці 5 нижче.

Таблиця 5. Порівняння характеристик та особливостей різних програм для роботи з локальними LLM

Хар-ка	**Ollama**	**LM Studio**	**llamafile**	**Jan**	**NextChat**	**Faraday.dev**	**Backyard AI**	**GPT4All**
Підтримка моделей	Власні моделі та інтеграція з популярними LLM (LLaMA)	LLaMA, GPT-J, GPT-NeoX, Mistral та інші	LLaMA, Mistral та інші через єдиний файл	LLaMA, GPT-J, Mistral та інші	LLaMA, Mistral, GPT-J та інші	LLaMA, GPT-J, Mistral та інші	LLaMA, GPT-J, Mistral та інші	LLaMA, GPT-J, Mistral та інші
Зручність використання	Простий інтерфейс, орієнтований на розробників	ГрІнт (GUI)	Використовує єдиний файл для запуску моделей	ГрІнт (GUI)	ГрІнт (GUI), орієнтований на чат-додатки	ГрІнт (GUI)	ГрІнт (GUI)	ГрІнт (GUI)
Платформи	macOS, Linux (Windows у розробці)	Windows, macOS	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux
Ліцензія	Open Source	Власницька ліцензія	Open Source	Open Source	Open Source	Open Source	Open Source	Open Source
Інтеграція з API	Так (REST API)	Ні	Ні	Так (REST API)	Так (REST API)	Ні	Ні	Ні
Особливості	Легка інтеграція з інструментами розробки, підтримка Docker	Зручний інт. для вибору та налаштування моделей	Моделі у вигляді єдиного файлу для простоти використання	Підтримка лок-го чату, інтеграція з API	Орієнтований на чат-додатки, підтримка REST API	Зручний інт. для нетехн. корист.	Зручний інт. для нетехн. корист.	Легка інстал., підтримка лок-го використ.

Мова програмування	Go	C++	C++	JavaScript/TypeScript	JavaScript/TypeScript	JavaScript/TypeScript	JavaScript/TypeScript	Python

*Джерело: розробка автора

Проведений порівняльний аналіз характеристик та особливостей існуючого програмного забезпечення для роботи з локальними LLM вказує на наявність кількох інструментів, які можуть бути впроваджені в державне управління, а саме:

1. Ollama виділяється своєю простотою інтеграції з інструментами розробки та підтримкою Docker, що робить її зручною для розробників і може бути корисною для інтеграції в системи державного управління, де важливою складовою є локальна обробка даних і конфіденційність.

2. LM Studio та Faraday.dev пропонують зручні графічні інтерфейси, що підходять для нетехнічних користувачів, що може бути корисним для держслужбовців, які не мають глибоких технічних знань, але потребують ефективних інструментів для управління документообігом.

3. Llamafile пропонує унікальну можливість упаковки моделей у єдиний файл для простоти використання, що може бути корисним для швидкої інтеграції в різні державні платформи.

4. Jan та NextChat орієнтовані на створення чат-додатків з підтримкою API, що дозволяє інтегрувати ці інструменти в чат-боти та інші платформи для автоматизації взаємодії з громадянами, що може сприяти підвищенню прозорості та оперативності в управлінських процесах.

5. GPT4All є популярним вибором для локального використання моделей через свою простоту та відкриту ліцензію, що робить його доступним інструментом для використання в публічному секторі.

Особливість використання Ollama у публічному управлінні полягає в його здатності інтегрувати різноманітні інструменти, такі як biorecap та rollama, які

забезпечують ефективну роботу з текстовими та графічними даними через API. Це дозволяє автоматизувати процеси документообігу, а також анотування даних, що, в свою чергу, сприяє підвищенню рівня управлінської прозорості. Завдяки можливості зберігати конфіденційність даних і налаштовувати моделі для специфічних завдань, Ollama може стати потужним інструментом для оптимізації та вдосконалення управлінських процесів у державному секторі.

Ollama вирізняється серед аналогів можливістю інтеграції з різними інструментами аналізу даних, зокрема з R-пакетом rollama, що дозволяє використовувати API Ollama для анотування текстових або графічних даних, а також для вбудовування документів у власні інформаційні системи [201].

Яскравим прикладом технічної реалізації сучасних інструментів є модель DeepSeek-R1, обрана для локального використання на платформі Ollama. Ця модель виявляється особливо ефективною для вирішення складних завдань, де критично важлива висока точність, навіть за рахунок більших обчислювальних ресурсів. Впровадження DeepSeek-R1 у державні інституції може значно покращити ефективність аналізу даних, підвищити точність ухвалення рішень, а також сприяти зниженню адміністративних бар'єрів. Це, у свою чергу, дозволить підвищити ефективність і оперативність функціонування публічного управління, сприяючи більш прозорому та ефективному процесу прийняття рішень.

Таким чином, впровадження локальних LLM у документообіг забезпечує підвищений рівень захисту даних порівняно з хмарними сервісами ШІ. Інструменти на кшталт Ollama надають можливість організаціям використовувати передові технології обробки природної мови без компромісів щодо конфіденційності інформації. Водночас необхідно враховувати апаратні вимоги та особливості функціонування таких моделей для забезпечення оптимальної продуктивності системи документообігу.

Важливим елементом для забезпечення ефективного функціонування цих інструментів є використання Docker Desktop, який дозволяє швидко розгортати додатки та їх компоненти в стандартизованому середовищі. У контексті державного управління, Docker може бути використаний для безпечного

розгортання додатків і модулів ШІ, забезпечуючи масштабованість і безпеку, що є критичними для обробки великих обсягів даних і збереження конфіденційності інформації.

Загалом, впровадження інтелектуальної обробки документів (IDP) на основі ШІ, зокрема через Docker та Ollama, може змінити підходи до автоматизації документообігу в державному управлінні. Використання таких систем може значно зменшити час обробки документів, підвищити точність у виявленні шахрайства, а також забезпечити більшу прозорість і підзвітність в управлінських процесах. Як показує досвід банківського сектору, автоматизація документів на основі ШІ може знизити витрати, прискорити процеси та покращити моніторинг відповідності [52].

Підсумовуючи, можна констатувати, що інтеграція інструментів ШІ, таких як Ollama, DeepSeek-R1, і Docker, у публічний сектор має великий потенціал для оптимізації управлінських процесів і покращення ефективності функціонування державних інституцій.

В цілому захищений документообіг з використанням Ollama, DeepSeek-R1 та Docker Desktop передбачає створення системи, де конфіденційність, цілісність і доступність документів забезпечуються на кожному етапі їх обробки. Нижче наведено структурну схему такої системи, оформлену у вигляді ієрархічної конструкції (Рис. 1.). Ця схема дозволяє візуалізувати всі ключові компоненти системи та їх взаємодію.

Представлена схема описує систему захищеного документообігу, яка використовує Ollama, DeepSeek-R1 та Docker Desktop для забезпечення безпеки та ефективності. Вона складається з чотирьох основних рівнів, кожен з яких виконує певні функції для забезпечення цілісності та конфіденційності даних.

Інфраструктурний рівень (Docker Desktop). Цей рівень формує технологічну базу всієї системи. Docker Desktop служить основою для ізоляції середовищ, де обробляються та зберігаються документи. Завдяки використанню контейнеризації, можна створювати окремі, захищені простори для кожного процесу документообігу. Це дає можливість ефективно керувати ресурсами,

зменшити ризик витоків даних та забезпечити високу надійність роботи всієї системи.

– Віртуалізація через Docker – дозволяє запускати кожен сервіс як окремий контейнер, що гарантує незалежність, легкість у розгортанні й безпеку.

– Ізоляція – забезпечує чітке розмежування ресурсів і доступів між модулями.

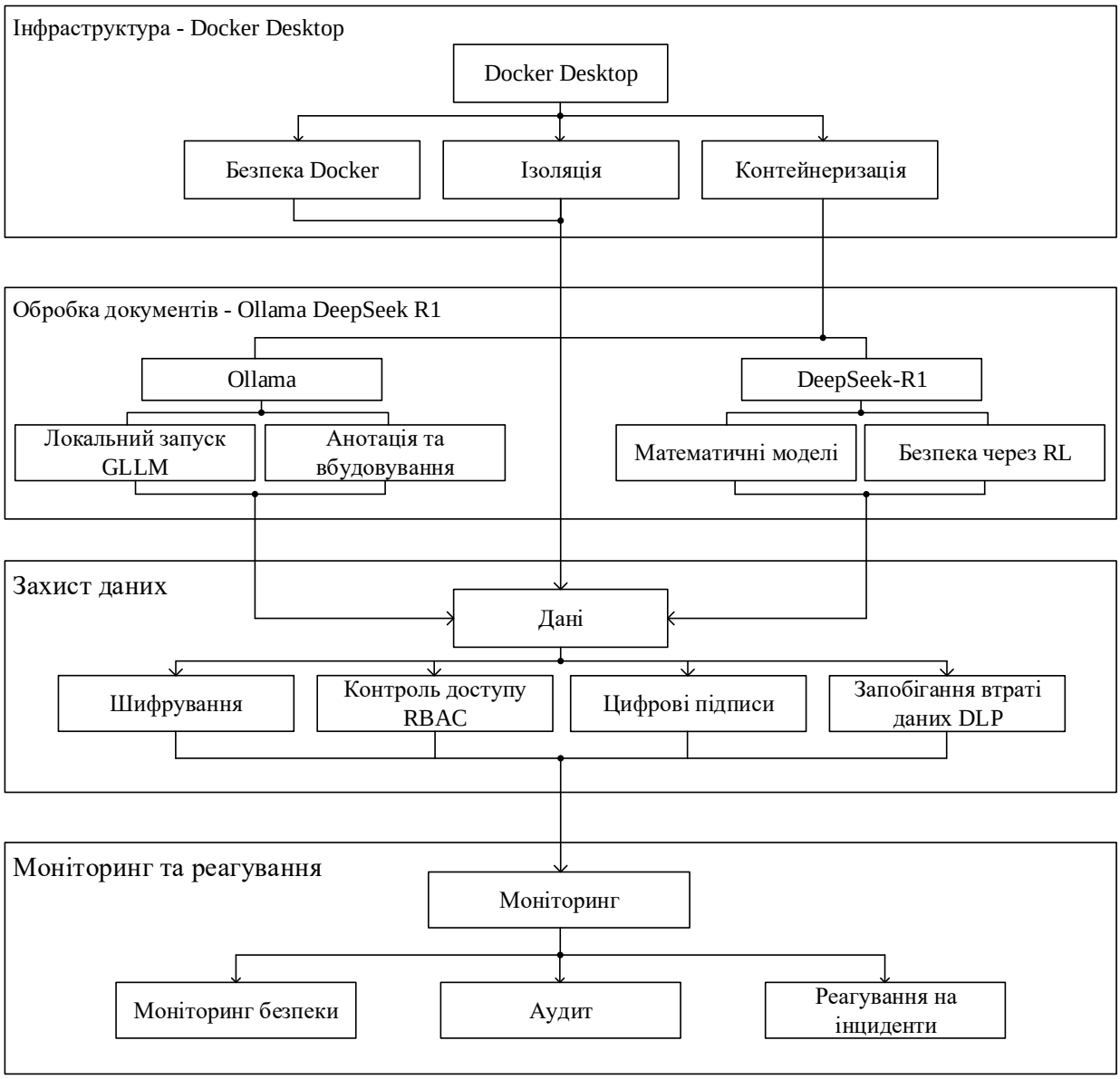


Рисунок 7. – Методологія документообігу в контексті механізмів державного управління

*Джерело: розробка автора.

– Контейнеризація – прискорює процес впровадження нових сервісів та мінімізує конфлікти в системі.

– Інституційна стійкість. Забезпечує безперебійну роботу критичних державних сервісів завдяки гнучкості та надійності інфраструктури [25].

– Міжвідомча інтеграція. Через мікросервісну архітектуру державні відомства можуть ефективно інтегруватися, зберігаючи контроль над власними сервісами.

– Гнучке розгортання е-сервісів. У рамках державних програм цифровізації, контейнеризація дозволяє оперативно масштабувати сервіси.

Рівень обробки документів (Ollama & DeepSeek-R1). Цей рівень відповідає за інтелектуальну обробку документів, аналіз, анотації, резюмування, машинне навчання документів за допомогою моделей штучного інтелекту. Ollama відповідає за безпеку на початковому етапі обробки даних, зокрема за захист документів від несанкціонованого доступу та втручання. Вона використовує передові алгоритми шифрування для забезпечення конфіденційності та аутентифікації користувачів. Цей рівень є критично важливим для публічних органів, оскільки дозволяє контролювати доступ до документів на етапі їх створення або редагування. DeepSeek-R1 виступає інструментом для аналізу та перевірки змісту документів на наявність потенційних загроз або вразливих місць. Вона здатна виявляти несанкціоновані зміни, аналізуючи структуру і зміст документів. Це важливо для публічного управління, адже дозволяє оперативно виявляти можливі маніпуляції з документами та забезпечує їх достовірність на всіх етапах обігу.

– Локальний запуск GLLM – дає змогу обробляти документи без зовнішнього з’єднання (критично для чутливої державної інформації).

– Анотація та обговорення – автоматичне створення тез, рекомендацій, політик.

– Математичні моделі – використовуються для прогнозування наслідків рішень, обґрунтувань регуляторних актів.

- Вставка через RL (Reinforcement Learning) – навчання на практиках реального врядування (поліпшення релевантності висновків).
- Підтримка процесу прийняття рішень. LLM можуть готувати довідки, пояснювальні записки, аналіз впливу регуляцій (RIA).
- Уніфікація державних документів. ШІ-моделі стандартизують термінологію, структуру документів, що сприяє правовій визначеності.
- Аналітична підтримка. Прогнозування ефективності політик, оцінка ризиків, текстовий аналіз суспільної думки тощо.

Рівень захисту даних. На цьому рівні реалізуються механізми захисту даних, забезпечується їх конфіденційність, цілісність та доступність. Застосовуються провідні механізми інформаційної безпеки.

- Шифрування – передача та зберігання інформації відбуваються в зашифрованому вигляді.
- RBAC (Role-Based Access Control) – дозволяє гнучко налаштовувати права доступу до інформації, зокрема між різними органами влади.
- Цифрові підписи – підтвердження автентичності документів, важливо в міжвідомчій комунікації та електронному документообігу.
- DLP (Data Loss Prevention) – захист від витоку критичної інформації зсередини чи зовні.
- Законодавча відповідність. Відповідає вимогам ЗУ “Про захист інформації”, КСЗІ, GDPR.
- Інформаційна безпека органів влади. Захист службових і персональних даних, державних інформаційних ресурсів та інформації з обмеженим доступом.
- Прозорість і контроль доступу. RBAC дозволяє забезпечити відповідальність осіб за свої дії з документами (audit trail).

Рівень моніторингу та реагування. Цей рівень відповідає за постійний контроль моніторинг системи та реагування на інциденти безпеки в реальному часі. 24/7 здійснюється перевірка відповідності системи політикам безпеки та виявлення порушень.

– Моніторинг безпеки – збір і аналіз журналів подій, виявлення підозрілої активності.

– Аудит – фіксація дій користувачів (важливо для службових розслідувань, перевірок НАЗК, СБ України).

– Реагування на інциденти – включає в себе автоматизовані сповіщення, блокування доступу, зберігання слідів.

– Підвищення підзвітності. Аудит дозволяє відслідковувати дії службовців і перевіряти їхню доброчесність.

– Кібергігієна державного апарату. Активне реагування на інциденти (частина кіберзахисту держави) [24].

– Інституційна прозорість. Моніторинг демонструє відповідність стандартам IT-управління, знижує ризики корупції.

Запропонована архітектура системи передбачає багаторівневу інтеграцію інструментів інфраструктури, штучного інтелекту, захисту даних та моніторингу в рамках єдиної екосистеми.

Аналізуючи загальні принципи взаємодії між рівнями запропонованої архітектури, доцільно підкреслити, що кожен з них виконує чітко визначені функціональні завдання, водночас перебуваючи у стані постійної взаємодії з іншими компонентами системи.

Така структурна організація забезпечує формування цілісного, узгодженого інформаційного та захисного потоку, що охоплює весь життєвий цикл документа – від його завантаження до безпечного зберігання або передачі визначеному суб’єкту. Це, у свою чергу, створює умови для реалізації комплексної цифрової трансформації процесів документопотоку з урахуванням актуальних ризиків, нормативних вимог у сфері інформаційної безпеки, а також впровадження механізмів інтелектуальної обробки даних.

Представлена система руху документів у межах публічного управління відповідно до адміністративно-правових регламентів, функціональних повноважень суб’єктів владних повноважень та організаційної структури органів державної влади. У запропонованій архітектурній схемі обробки документів

реалізовано комплексний підхід до забезпечення уніфікованого, прозорого та контрольованого електронного документообігу, з урахуванням нормативних вимог, ризик-орієнтованого управління та інформаційної безпеки.

Умовно документопотік охоплює такі функціональні стадії:

1. Ініціація документа – створення первинного документа внаслідок управлінського запиту, подання звернення або формування службової інформації. На цьому етапі система автоматично забезпечує первинну ідентифікацію користувача, валідацію структури документа, призначення метаданих та застосування криптографічних механізмів початкового рівня (електронний підпис, хешування тощо).

2. Маршрутизація та передача на розгляд – документ передається відповідним структурним елементам органу публічної влади згідно з внутрішніми маршрутами, що визначаються функціональною компетенцією. Здійснюється контроль доступу, реєстрація усіх транзакцій у системі журналювання та забезпечується цілісність інформації під час передачі.

3. Інформації та ухвалення рішень – на основі наявних даних проводиться їх аналітичне опрацювання, за потреби, доповнення чи узгодження, після чого формується проект управлінського рішення. У цьому процесі застосовуються засоби інтелектуальної обробки даних, автоматизованого аналізу та підтримки прийняття рішень, що сприяють підвищенню обґрунтованості та об’єктивності результатів.

4. Фіналізація документа та його подальше призначення – остаточно верифікований документ або зберігається у захищеній електронній архівній системі, або передається адресату через сертифіковані захищені канали. Передача супроводжується повторною криптографічною обробкою з дотриманням вимог щодо конфіденційності, автентичності та доступності даних.

5. Аудит та контроль процесів – усі дії в рамках життєвого циклу документа підлягають обліку, що дозволяє здійснювати системний моніторинг, аудит відповідності, а також формування аналітичної звітності для потреб

внутрішнього та зовнішнього контролю, у тому числі з боку органів державного фінансового чи адміністративного нагляду.

Таким чином, запропонована схема руху документів забезпечує не лише автоматизовану обробку інформації, але й створює основу для цифрової трансформації управлінських процесів, підвищення прозорості державного управління, зміцнення інформаційної безпеки та підвищення загальної ефективності публічного адміністрування.

У межах проведеного дослідження було здійснено комплексний аналіз можливостей використання інтелектуальних технологій у сфері організації електронного документообігу в системах державного управління. Обґрунтовано концептуальні положення щодо впровадження захищених архітектурних рішень, які поєднують можливості штучного інтелекту з сучасними вимогами інформаційної безпеки, нормативно-правової відповідності та міжвідомчої інтероперабельності.

Встановлено, що ефективне розгортання систем електронного документообігу з використанням ШІ дозволяє:

- забезпечити високий рівень автоматизації процесів створення, класифікації, маршрутизації та зберігання документів;
- істотно зменшити навантаження на людські ресурси в системах публічного адміністрування;
- підвищити достовірність прийнятих рішень через аналітичну обробку великих масивів управлінських даних;
- реалізувати гнучкі, адаптивні моделі безпеки з урахуванням змінного ризикового профілю.

Окрім того, запропонована архітектурна модель демонструє перспективність побудови багаторівневої системи обробки документів, що включає модулі машинного навчання, криптографічного захисту, цифрової автентифікації та журналювання дій користувачів. Такий підхід формує основу для нової генерації систем публічного управління – прозорих, безпечних і здатних до самонавчання.

З огляду на актуальність цифрової трансформації державного управління, подальші наукові розвідки можуть бути зосереджені на таких напрямах:

Розробка моделей довірчих взаємодій у системах державного електронного документообігу з використанням цифрових ідентичностей та смарт-контрактів.

Оптимізація алгоритмів інтелектуального аналізу документів для підвищення релевантності класифікації, виявлення аномалій та прогнозування управлінських сценаріїв.

Поглиблене вивчення етичних і правових аспектів застосування ШІ в автоматизованих управлінських процесах, зокрема у сфері персональних даних та прийняття рішень.

Інтеграція із національними інформаційними системами через єдині шлюзи обміну даними, що дозволить масштабувати рішення в межах єдиного цифрового простору держави.

Моделювання стійкості систем електронного документообігу до гібридних загроз, включно з інформаційними атаками, втручанням у ланцюжки прийняття рішень та маніпуляціями даними.

Таким чином, перспективи подальших досліджень відкривають широкі можливості для формування інтелектуальних, безпечних та гнучких систем публічного управління нового покоління, здатних ефективно функціонувати в умовах складного інформаційного середовища.

3.4. Обґрунтування напрямів удосконалення системи електронного міжвідомчого документообігу сфери оборони

Електронний міжвідомчий документообіг у сфері оборони України є ключовим елементом цифрової трансформації, що забезпечує оперативний обмін інформацією між органами військового управління, такими як Міністерство оборони, Генеральний штаб Збройних Сил України та іншими відомствами. Єдина система електронного міжвідомчого документообігу покликана підвищити ефективність управління, забезпечити безпеку даних і

підтримувати сумісність ЕКС різного призначення (військові, адміністративні, логістичні) та рівня складності (локальні, регіональні, національні). Проте сучасні виклики, зокрема зростання кіберзагроз, гетерогенність ЕКС і потреба в інтеграції з міжнародними стандартами, вимагають удосконалення системи.

Актуальність удосконалення ЄСЕМД зумовлена необхідністю адаптації до нових технологій, підвищення стійкості до кібератак і забезпечення оперативності в умовах воєнного стану. За даними Національного інституту стратегічних досліджень, модернізація ЕКС у сфері оборони може скоротити час обробки інформації на 30–50% [**Error! Reference source not found.**]. Удосконалення системи також сприятиме інтеграції України до європейського безпекового простору, зокрема через відповідність стандартам НАТО та ЄС [**Error! Reference source not found.**].

Метою цього розділу є обґрунтування напрямів удосконалення ЄСЕМД, включаючи технічні, безпекові та організаційні аспекти. Розділ аналізує сучасний стан системи, визначає ключові недоліки, пропонує шляхи їх усунення та оцінює перспективи впровадження змін.

Наявні системи електронного документообігу в оборонній сфері України частково автоматизують процеси створення, обробки та передачі документів. Наприклад, окремі відомства використовують системи на базі платформ “Діловод” або власних розробок, що підтримують електронний цифровий підпис (ЕЦП) і базові функції маршрутизації. Проте ці системи мають обмежену інтеграцію між собою, що ускладнює міжвідомчий обмін.

Основні досягнення включають:

- Впровадження ЕЦП для юридично значущих документів [44].
- Автоматизацію окремих процесів у центральних органах (наприклад, кадровий облік у Міноборони).
- Використання захищених каналів зв’язку для передачі даних із грифом “таємно”.
- Аналіз сучасного стану ЄСЕМД виявив такі проблеми:

– Фрагментація систем. Різні відомства використовують несумісні платформи, що призводить до дублювання даних і затримок у передачі.

– Обмежена масштабованість. Наявні системи не розраховані на значне зростання кількості користувачів чи документів.

– Недостатній рівень безпеки. Застарілі криптографічні алгоритми та слабкий захист від сучасних кібератак (наприклад, APT-груп) [29].

– Низька інтероперабельність. Відсутність єдиних стандартів обміну даними між ІТС різного призначення.

– Організаційні бар'єри. Недостатня координація між відомствами та низький рівень цифрової грамотності персоналу.

За оцінками експертів, до 40% документів у сфері оборони все ще обробляються вручну через технічні або процедурні обмеження [2]. Ці недоліки знижують оперативність і підвищують ризик інформаційних інцидентів.

Для усунення фрагментації та підвищення масштабовальності пропонується перехід до модульної архітектури ЄСЕМД, яка включає:

– Централізований хаб. Координує обмін даними між відомствами, забезпечує єдине сховище метаданих.

– Локальні вузли. Автономні модулі для роботи в окремих підрозділах із підтримкою офлайн-режиму.

– API-шлюзи. Забезпечують інтеграцію з зовнішніми ІТС (логістичними, фінансовими).

Модульний підхід дозволяє поступово оновлювати систему, не зупиняючи її роботу. Наприклад, досвід Естонії з платформою X-Road показує, що модульна архітектура підвищує гнучкість і знижує витрати на інтеграцію [235].

Для підвищення ефективності ЄСЕМД необхідно:

– Хмарні рішення. Використання гібридних хмар (приватних для чутливих даних, публічних для некритичних) для масштабування та резервування.

– Блокчейн. Застосування для забезпечення незмінності документів і аудиту операцій [146].

– Штучний інтелект. Автоматизація класифікації документів, аналізу ризиків і прогнозування навантаження.

– Big Data. Обробка великих обсягів даних для моніторингу та оптимізації процесів.

Інтероперабельність ІТС різного призначення та складності є ключовим викликом. Пропонується:

– Уніфіковані протоколи. Використання REST API та стандартів XML/JSON для обміну даними.

– Платформа «Трембіта». Розширення її функціоналу для оборонних ІТС [**Error! Reference source not found.**].

– Адаптація до стандартів ЄС. Впровадження European Interoperability Framework (EIF) для сумісності з партнерами [**Error! Reference source not found.**].

Це дозволить інтегрувати локальні системи (наприклад, у військових частинах) із національними (Міноборони, Держспецзв'язку).

Наявні КСЗІ не повною мірою відповідають сучасним загрозам, таким як цільові кібератаки чи інсайдерські витоки. Напрями удосконалення:

– Оновлення криптографії. Перехід на постквантові алгоритми для захисту від майбутніх загроз [225].

– Двофакторна автентифікація. Впровадження біометричних методів (відбитки пальців, розпізнавання облич) для критичних операцій.

– Моніторинг у реальному часі. Використання SIEM-систем (Security Information and Event Management) для виявлення аномалій.

– Зростання кібератак, зокрема в умовах війни, вимагає:

– Системи раннього виявлення. Впровадження IDS/IPS (Intrusion Detection/Prevention Systems).

– Регулярні пентести. Імітація атак для перевірки стійкості системи.

– Резервне копіювання. Розподілені копії даних із шифруванням для відновлення після атак [33].

– КСЗІ має бути оновлена для відповідності:

– ДСТУ ISO/IEC 27001:2015 (управління інформаційною безпекою) [34].

– Вимогам НАТО до кібербезпеки (STANAG 4677) для міжнародної співпраці [217].

– Стратегії кібербезпеки України (2021–2025) [105].

Низька цифрова грамотність є бар'єром для ефективного використання ЄСЕМД. Пропонується:

– Тренінги з кібергігієни. Навчання правил безпечної роботи з даними.

– Спеціалізовані курси. Для адміністраторів і операторів системи.

– Симуляції. Практичні заняття з реагування на кібератаки.

За даними досліджень, регулярне навчання знижує ризик інсайдерських інцидентів на 70% [154].

Відсутність єдиних стандартів ускладнює міжвідомчу взаємодію. Напрями:

– Уніфіковані шаблони документів. Для всіх відомств.

– Протоколи маршрутизації. Автоматизація передачі завдань.

– Єдина номенклатура. Класифікація документів за типами та рівнями доступу.

– Для синхронізації зусиль необхідно:

– Міжвідомча робоча група. Під керівництвом Міноборони та Держспецзв'язку.

– Регулярні консультації. Для узгодження вимог і графіків.

– Пілотні проекти. Тестування оновлень у окремих підрозділах.

– Удосконалення ЄСЕМД вимагає оновлення регуляторних документів:

- ***Законодавчі зміни:***

– Доповнення Закону України "Про захист інформації в ІТС" вимогами до постквантової криптографії [48].

– Розширення Закону "Про електронні довірчі послуги" для підтримки нових методів автентифікації [44].

- ***Нормативні акти:***

- Оновлення постанови КМУ № 373 для врахування хмарних технологій [**Error! Reference source not found.**].
- Розробка нових ДСТУ для блокчейн і ШІ в документообігу.

- ***Міжнародні стандарти:***

- Адаптація EIF для інтероперабельності [**Error! Reference source not found.**].
- Врахування вимог НАТО до безпеки даних [217].

Пропонується розробити окремий нормативний акт, який регулюватиме ЄСЕМД у сфері оборони, враховуючи її критичність.

- Аналіз (3–6 місяців): Оцінка поточного стану, визначення пріоритетів удосконалення.
- Проектування (6–12 місяців): Розробка нових модулів, оновлення КСЗІ.
- Тестування (6–9 місяців): Пілотні проекти в окремих відомствах.
- Повне впровадження (12–18 місяців): Розгортання оновленої системи, навчання користувачів.
- Моніторинг і підтримка: Постійне оновлення функціоналу та безпеки.

Очікувані результати

- Скорочення часу обробки документів на 60–80%.
- Зниження ймовірності кіберінцидентів на 50% завдяки новим КСЗІ.
- Підвищення інтероперабельності ІТС на 70% за рахунок стандартів.
- Економія ресурсів на 25–40% через автоматизацію.

Міжнародний досвід

- Естонія (X-Road): Модульна система для безпечного обміну даними [235].
- Фінляндія (e-Government): Інтеграція державних ІТС із високим рівнем безпеки [**Error! Reference source not found.**].
- США (DoD ECM): Система документообігу для оборонного сектору з акцентом на кібербезпеку [164].

Ці приклади можуть бути адаптовані до умов України з урахуванням оборонної специфіки.

Таким чином, удосконалення системи електронного міжвідомчого документообігу сфери оборони є стратегічно важливим завданням, яке сприятиме підвищенню ефективності, безпеки та оперативності управління. Основні напрями включають:

- Технічну модернізацію: модульна архітектура, хмарні технології, ШІ та блокчейн.
- Посилення безпеки: оновлення КСЗІ, постквантова криптографія, моніторинг загроз.
- Організаційні покращення: навчання, стандартизація, координація.
- Оновлення нормативної бази для підтримки нових технологій і стандартів.

Реалізація цих напрямів дозволить усунути фрагментацію ІТС, підвищити стійкість до кібератак і забезпечити сумісність із міжнародними партнерами. Подальші дослідження мають зосередитися на пілотному тестуванні нових технологій і розробці детальних планів впровадження.

ВИСНОВКИ

На виконання поставленої мети у представленому дослідженні здійснено комплексну розробку теоретико-методологічних засад та сформульовано практичні рекомендації, спрямовані на створення та вдосконалення захищеної системи електронної взаємодії і міжвідомчого документообігу в органах державної влади України. Такий підхід забезпечує наукову обґрунтованість запропонованих рішень і враховує актуальні виклики цифрової трансформації державного управління.

У дослідженні враховано контекст цифрової трансформації, виклики повоєнного відновлення та стратегічні орієнтири європейської інтеграції. Проведено аналіз міжнародного досвіду, охоплено нормативно-правові, організаційні й технологічні аспекти функціонування відповідних систем у провідних країнах. Обґрунтовано інтеграцію сучасних інноваційних технологій, зокрема штучного інтелекту, блокчейну, локальних великих мовних моделей та інструментів контейнеризації, як ключових чинників підвищення ефективності, кібербезпеки, інформаційної безпеки та забезпечення інтероперабельності цифрових рішень у сфері публічного управління та електронного урядування, з акцентом на захист об'єктів критичної інфраструктури.

На основі проведеного дослідження, яке охоплює аналіз міжнародного досвіду, нормативно-правової бази, технологічних рішень і розробку практичних рекомендацій, сформульовано висновки, що структуровані за ключовими напрямами:

1. Порівняльний аналіз і адаптація міжнародного досвіду

Моделі електронної взаємодії. Розроблена методологічна структура порівняльного аналізу за вісьмома критеріями (технологічна архітектура, безпека, інтероперабельність, масштабованість, правове забезпечення, організаційна координація, інноваційність, економічна ефективність) дозволила ідентифікувати резерви для вдосконалення української системи електронної взаємодії (СЕВ). Досвід країн ЄС (Естонія – X-Road, Нідерланди – Digikoppeling, Німеччина – IT-Grundschutz, Фінляндія – KEJO) та інших країн (Ізраїль, Данія,

Австралія, Південна Корея) показує, що децентралізовані архітектури, стандартизовані API, цифрові ідентичності та багаторівневий захист є ключовими для ефективних СЕВ.

Адаптація до українських реалій. Запропонована модель «Цифрового стрибка» інтегрує елементи естонської децентралізації, ізраїльського захисту критичної інфраструктури, данської цифрової інклюзії, австралійської міжрівневої координації та південнокорейських інновацій. Модель адаптовано до повоєнного контексту України, враховуючи обмежені ресурси, воєнні виклики та потреби європейської інтеграції.

Синергетичний ефект. Встановлено, що міжвідомча інтеграція через СЕВ забезпечує синергетичний ефект у п'яти аспектах: підвищення ефективності управління, прозорості, зручності для громадян, стимулювання інновацій та конкурентоспроможності держави. Порівняльна таблиця ефектів демонструє нелінійні результати, що перевищують суму окремих покращень, особливо в умовах повоєнної відбудови.

2. Нормативно-правове забезпечення

Фрагментарність законодавства. Аналіз чинної нормативно-правової бази України виявив фрагментарність, недостатню адаптацію до інноваційних технологій (ШІ, блокчейн) і прогалини в регулюванні безпеки даних у секторі оборони. Відсутність спеціальних стандартів для ШІ та блокчейну створює ризики для ефективності та безпеки.

Міжнародний досвід. У країнах НАТО та ЄС (Німеччина, Франція, Нідерланди) нормативна база поєднує загальні закони про електронний документообіг із галузевими стандартами безпеки. Це забезпечує сумісність, гнучкість і баланс між інноваціями та захистом даних.

Пропозиції вдосконалення. Запропоновано комплекс заходів, а саме: розробка спеціального закону про електронний документообіг у секторі оборони, внесення змін до чинних актів, створення галузевих стандартів для ШІ та блокчейну, впровадження регуляторних «пісочниць» для тестування технологій.

Рекомендується гармонізація з європейськими стандартами (NIS 2 Directive, GDPR) і НАТО для забезпечення інтероперабельності.

3. Технологічні рішення

Концептуальна модель СЕВ. Розроблено комплексну модель електронної взаємодії, яка синтезує шість підходів (технологічний, соціально-організаційний, функціональний, процесний, правовий, системний). Модель враховує повоєнні виклики, акцентуючи на безпеці, адаптивності та інтероперабельності через сервісно-орієнтовану архітектуру (SOA), подібну до EIRA.

Інтеграція ШІ та блокчейну. Впровадження ШІ (зокрема локальних LLM, таких як Ollama, DeepSeek-R1) і блокчейну підвищує автоматизацію, достовірність і безпеку документообігу. Технології NLP дозволяють структурувати дані, класифікувати документи та реагувати на запити, а блокчейн забезпечує цілісність і верифікацію. Контейнеризація (Docker Desktop) оптимізує розгортання систем, але потребує контрольованих середовищ для донавчання моделей.

Безпекові виклики. Ідентифіковано ризики ШІ (упередження, непередбачуваність) і блокчейну (юридичний статус документів, інтеграція з існуючими системами). Запропоновано багаторівневу систему захисту: криптографія, багатофакторна автентифікація, моніторинг загроз, фізична сегментація мереж (за фінським досвідом).

Архітектура ЄСЕМД. Теоретичні моделі для електронного міжвідомчого документообігу (ЄСЕМД) у секторі оборони базуються на модульному принципі, федеративній інтеграції та «глибокій обороні». Запропоновано уніфікацію процесів, використання платформи «Трембіта» та впровадження хмарних технологій для масштабованості.

4. Практичні рекомендації

Коротко- та середньострокові заходи. Запропоновано рекомендації з горизонтом 1–5 років:

- ***Технічна модернізація.*** Впровадження модульної архітектури, ШІ, блокчейну, постквантової криптографії.

- ***Безпека.*** Оновлення комплексних систем захисту інформації (КСЗІ), створення національного каталогу загроз (за німецьким досвідом), впровадження API для інтеграції (за нідерландським досвідом).
- ***Організація.*** Координація між відомствами, стандартизація, навчання персоналу.
- ***Нормативна база.*** Розробка стандартів для ШІ (критерії валідації, автономність, відповідальність) і блокчейну (юридичний статус, верифікація транзакцій).

Пілотне впровадження. Рекомендується пілотне розгортання платформи, подібної до X-Road, для координації між Міноборони, РНБО та іншими відомствами, з використанням децентралізованої архітектури та блокчейну.

Європейська інтеграція. Адаптація стандартів NIS 2 Directive, розвиток цифрової ідентичності (аналог DigiD) і стратегії цифровізації (за прикладом Digital Agenda 2020) сприятиме гармонізації з ЄС і НАТО.

Оцінка ефективності. Запропоновано оцінювати СЕВ і ЄСЕМД за функціональними, технічними, економічними, організаційними та безпековими показниками, з акцентом на вплив на управлінські процеси та інформаційну безпеку.

5. Перспективи подальших досліджень

Інноваційні технології. Подальші дослідження мають зосередитися на потенціалі ШІ, блокчейну, квантових обчислень і обробки великих даних для посилення стійкості цифрової інфраструктури. Особлива увага – розробка спеціалізованих моделей ШІ для юридичних документів і гібридних систем із перевіркою людиною (Human-in-the-loop).

Соціально-економічні аспекти. Вивчення впливу цифрових трансформацій на внутрішньо переміщених осіб і маргіналізовані групи для забезпечення інклюзивності.

Глобальний внесок. Унікальний український досвід цифрової стійкості в умовах війни може стати основою для міжнародних стандартів захисту критичної інформаційної інфраструктури.

Таким чином успішне впровадження захищених систем електронної взаємодії та міжвідомчого документообігу в Україні вимагає комплексного підходу, що поєднує технологічні інновації, нормативно-правові реформи та організаційні зміни. Адаптація європейського досвіду, зокрема моделей Естонії, Німеччини, Фінляндії та Нідерландів, дозволить Україні подолати фрагментацію цифрової інфраструктури, підвищити стійкість до кіберзагроз і забезпечити інтероперабельність із європейськими системами. Запропонована модель «Цифрового стрибка» є стратегічним інструментом для повоєнної відбудови, зміцнення національної стійкості та цифрової трансформації державного управління, зокрема в секторі безпеки й оборони.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Алішов Н.І. (2011). Теорія, технології й засоби системної взаємодії ресурсів в інтелектуальних системах і мережах комп'ютерів: автореф. дис. ... докт. техн. наук: 05.13.13. Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України, 34 с. URL: http://www.nas.gov.ua/UA/Sites/GlushkovInstitute/Documents/Avtoreferaty/2011/Alishov.pdf.

2. Аналіз ефективності інформаційних систем у Збройних Силах України. Військово-технічний журнал, 2023, 29 (2), 45–50.

3. Андрощук Г.О. (2021). Цифрова трансформація в країнах ЄС на 2021 рік. У: Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання: матеріали Всеукр. наук.-практ. конф., м. Київ, 2 груд. 2021 р. / наук. керівник О.А. Баранов; упоряд.: В.М. Фурашев, С.О. Дорогих. Київ-Одеса: Фенікс, с. 41–50. (Інформація і право, (1(44)), 78). URL: https://ippi.org.ua/sites/default/files/socialna_i_cifrova_transformaciya_2021.pdf.

4. Державна служба спеціального зв'язку та захисту інформації України. Атестат відповідності комплексної системи захисту інформації ядра СЕВ ОВВ версії 2.0 : офіц. документ № 20965 від 20 груд. 2019 р. [Електронний ресурс]. – Режим доступу: https://se.diia.gov.ua/sev-ovv.

5. Бакалінська О.О. (2022). Економічні аспекти впровадження електронного документообігу. *Економіка та держава*, (3), 8–14. URL: http://www.economy.in.ua/pdf/3_2022/3.pdf.

6. Бакалінська О.О. (2023). Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*, (2), 73–78. URL: http://pgp-journal.kiev.ua/archive/2023/2/15.pdf.

7. Баранов О., Швець М., Брижко В. Електронне урядування в Україні: правові аспекти. Інформація і право. 2019. №2. С. 39-51. URL: http://ippi.org.ua/sites/default/files/2_2019.pdf.

8. Баранов О.А. (2020). Електронне урядування в Україні: пріоритети та проблеми впровадження. *Інформація і право*, (3(34)), 9–16. URL: http://ippi.org.ua/sites/default/files/3_34_2020_2.pdf.

9. Баранов О.А. (2021). Соціальна та цифрова трансформації: джерело правових проблем. *Інформація і право*, **(**3(38)), 59–73. URL: http://ippi.org.ua/sites/default/files/3_38_2021_6.pdf.

10. Баранов О.А. (2022). *Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія*. Київ: НДЦПІ НАПрН України, 628 с. URL: http://www.ndcpi.gov.ua/index.php/uk/ publikatsiji/monografiji.

11. Баранов О.А. Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом. Інформація і право. 2018. № 4. С. 46-70. URL: http://nbuv.gov.ua/UJRN/Infpr_2018_4_7.

12. Баранович М.В. (2024). Організація роботи з електронними зверненнями громадян в Україні. [Електронний ресурс]. URL: https://evnuir.vnu.edu.ua/handle/123456789/24428 (Дата звернення: 18.03.2025).

13. Беланюк М.В. (2021). Електронний документообіг у секторі безпеки і оборони: правові аспекти. *Інформаційна безпека людини, суспільства, держави*, (1(29)), 42–50. URL: http://infbez.knu.ua/index.php/main/article/view/489.

14. Білик О. (2023). Сучасні підходи до впровадження електронного документообігу у систему державного управління. Науковий вісник Вінницької академії безперервної освіти. Серія «Екологія. Публічне управління та адміністрування». DOI: https://doi.org/10.32782/2786-5681-2023-4.06 [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/5ded60938581d8e36f5754b77c69dab0ac684182 (Дата звернення: 18.03.2025).

15. Богданович В.Ю. (2021). *Методологія формування та забезпечення інформаційної безпеки України: теоретичні засади: монографія*. Київ: НАДУ, 374 с. URL: http://academy.gov.ua/?lang=ukr&tip=dop&tipid=monogr.

16. Богданович В.Ю. (2021). *Системи підтримки прийняття рішень в оборонній сфері: теорія та практика: монографія*. Київ: НУОУ, 412 с. URL: https://nuou.org.ua/library.

17. Богданович В.Ю. (2022). Розвиток систем прийняття рішень на основі технологій штучного інтелекту. *Сучасні інформаційні технології у сфері безпеки та оборони*, (3(45)), 5–12. URL: http://sit.nuou.org.ua/index.php/sit/article/view/212.

18. Богданович В.Ю. (2022). *Теоретико-методологічні основи забезпечення національної безпеки України в умовах позаблоковості: монографія*. Київ: НУОУ, 416 с. URL: https://nuou.org.ua/library.

19. Болдуєв М.В., Болдуєва О.В., Лищенко О.Г. Потенціал і проблеми запровадження електронного документообігу в Україні. Ефективна економіка. 2024. №4. DOI: https://doi.org/10.32702/2307-2105.2024.4.9.

20. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. В.Б. Толубка. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/l_1234_56789012.pdf.

21. Величко О.Ф., Гриб Д.А., Демідов Б.О., Коростельов О.П., Кучеренко Ю.Ф., Луханін М.І., Чепков І.Б., Хмелевська О.О. Методологічні й системотехнічні аспекти інформаційного забезпечення управління системами військового призначення та діяльністю в оборонній сфері: монографія / за ред. Б.О. Демідова, О.П. Коростельова. К.: Видавничий дім «Стилос», 2021. Т. 1. 624 с.

22. Гасанов. З.М. (2024). Використання штучного інтелекту та автоматизації в державних послугах: можливості та ризики. Law. State. Technology, 23 Dec. 2024. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/d9a037364ca72b7f535c506cec9d832d286dccd7 (Дата звернення: 18.03.2025).

23. Гелецька І. О., Шовдра М. М. (2024). Визначення поняття «штучного інтелекту» та його місце у системі цивільного законодавства України. In Galician

Studies Law Sciences. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/898f6121bfd286d51ab8d937ba6c000b6513c11c (Дата звернення: 18.03.2025).

24. Глибовець А.М. (2017). Автоматизований пошук іменованих сутностей у нерозмічених текстах українською мовою. Штучний інтелект, № 2, с. 45-51 (Дата звернення: 18.03.2025).

25. Гненик М.О. (2024). Діджиталізація та штучний інтелект у адміністративному менеджменті громад і територій. [Електронний ресурс]. URL: https://essuir.sumdu.edu.ua/handle/123456789/97932 (Дата звернення: 18.03.2025).

26. Горбулін В.П. (2023). *Стратегічне планування: вирішення проблем національної безпеки: монографія*. Київ: НІСД, 240 с. URL: https://niss.gov.ua/publikacii/monografiyi.

27. Горбулін В.П. (2023). Цифрова трансформація оборонно-промислового комплексу України: виклики та перспективи. *Стратегічні пріоритети*, (3(64)), 5–14. URL: https://niss.gov.ua/sites/default/files/2023-09/Strategic-Priorities-64-2023.pdf.

28. Грицяк Н., Литвинова Л. Електронне урядування: нормативно-правове забезпечення та особливості впровадження в Україні. Публічне врядування в Україні: стан, виклики та перспективи розвитку. 2020. №3. С. 121-134.

29. Крайнов, В. О., Маланчук, М. Ф. і Грозовський, Р. І. (2020) «Методика оцінки ефективності комплексної системи захисту інформації автоматизованих інформаційних систем органів військового управління», Сучасні інформаційні технології у сфері безпеки та оборони. Київ, Україна, 37(1), с. 103–106. doi: 10.33099/2311-7249/2020-37-1-103-106.

30. Zakhyst informaciji v avtomatyzovanykh systemakh upravlinnja : navchaljnyj posibnyk / Uklad. I. A. Piljkevych, N. M. Lobanchykova, K. V. Molodecjka. – Zhytomyr : Vyd-vo ZhDU im. I. Franka, 2015. – 226 s.

31. Дашко І., Михайліченко Л. (2024). Особливості використання штучного інтелекту в діяльності підприємств. Сталий розвиток економіки.

[Електронний ресурс]. URL: https://www.semanticscholar.org/paper/16f903385e242c5fe377a77cb9b70e57d974a767 (Дата звернення: 18.03.2025).

32. Досин Д.Г., Литвин В.В., Нікольський Ю.В., Пасічник В.В. Інтелектуальні системи, базовані на онтологіях: Монографія. – Л.: Видавничий дім „Цивілізація”, 2009. – 414 с. – Тираж – 300 прим. – ISBN 978-966-7719-17-3, URL: https://www.ipm.lviv.ua/files/monograph_fmi_1951-2021.pdf.

33. ДСТУ 4145-2002 Криптографічний захист інформації. Алгоритм цифрового підпису. URL: http://dstu.gov.ua

34. Чунарьова, А. В., & Чунарьов, А. В. (2012). Аналіз нормативно-правового забезпечення захисту інформації сучасних ІКСМ. Ukrainian Information Security Research Journal, 14(2), Article 2185. https://doi.org/10.18372/2410-7840.14.2185.

35. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. – [Електронний ресурс]. – Режим доступу: http://dstu.gov.ua.

36. ISO/IEC 27001:2015. Information technology – Security techniques – Information security management systems – Requirements. – [Electronic resource]. – Access mode: https://www.iso.org/standard/27001.html.

37. Дубов Д.В. (2022). *Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України: монографія*. Київ: НІСД, 392 с. URL: https://niss.gov.ua/publikacii/monografiyi.

38. Дубов Д.В. (2022). *Кібербезпека: світові тенденції та виклики для України: аналітична доповідь*. Київ: НІСД, 96 с. URL: https://niss.gov.ua/sites/default/files/2022-06/cybersecurity-2022.pdf.

39. Дубов Д.В. (2022). Стратегічні комунікації: проблеми концептуалізації та практичної реалізації. *Стратегічні пріоритети*, (1(42)), 9–17. URL: https://niss.gov.ua/sites/default/files/2022-03/Strategic-Priorities-42-2022.pdf.

40. Дубов Д.В. (2022). Штучний інтелект у системах підтримки прийняття рішень: перспективи застосування в оборонній сфері. *Стратегічні пріоритети*, (2(43)), 87–95. URL: https://niss.gov.ua/sites/default/files/2022-06/Strategic-Priorities-43-2022.pdf.

41. Дубов Д.В. (2023). *Інформаційні технології в системі національної безпеки: монографія*. Київ: НІСД, 376 с. URL: https://niss.gov.ua/publikacii/monografiyi.

42. Дубов Д.В. (2023). Оцінка ризиків інформаційної безпеки: методологія та практика. *Стратегічні пріоритети*, (1(62)), 98–106. URL: https://niss.gov.ua/sites/default/files/2023-03/Strategic-Priorities-62-2023.pdf.

43. Дьяченко М. І., Роскладка А. А. (2024). Впровадження штучного інтелекту в процес менеджменту інцидентів. Information Technology and Society. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/4fb5b62c6d98674d9d9f2e18afe3206560e6d40d (Дата звернення: 18.03.2025).

44. Закон України «Про електронний цифровий підпис» від 22.05.2003 № 852-IV. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/852-153.

45. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19.3.

46. Постанова Кабінету Міністрів України від 1 серпня 2023 р. № 798 “Про затвердження Порядку використання електронних довірчих послуг в органах державної влади, органах місцевого самоврядування, підприємствах, установах та організаціях державної форми власності”. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/798-2023-п.

47. Закон України “Про електронні документи та електронний документообіг” від 22.05.2003 № 851-IV. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/851-153.

48. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/80/94-вр.

49. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/373-2006-п.

50. Ільєнко А., Ільєнко С., Яковенко О., Галич Є., Павленко В. Перспективи інтеграції штучного інтелекту в системи кібербезпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2024. №1(25). С. 318-329. DOI: https://doi.org/10.28925/2663-4023.2024.25.318329.

51. Інтелектуальні системи прийняття рішень та проблеми обчислювального інтелекту: зб. наук. пр. міжнар. наук. конф. ISDMCI'2013. Херсон: ХНТУ, 2013, 579 с. URL: http://www.kntu.net.ua/index.php?id=isdmci.

52. Інформаційно-керуючі системи: моделювання та оптимізація / ред. А. Шишацький. – Харків: ПК «ЦЕНТР ТЕХНОЛОГІЙ», 2024. – ISBN: 978-617-8360-04-7. – DOI: 10.15587/978-617-8360-04-7.

53. Нестеренко В.О. Порядок здійснення діловодства та документування управлінської інформації в електронній формі в Міністерстві оборони України та Генеральному штабі Збройних Сил України. Публічне управління XXI століття: портал можливостей: зб. тез XX Міжнар. наук. конгресу. – Вид-во ХарРІ НАДУ "Магістр", 2020. – С. 467-470.

54. Клименко І., Линьов К. Технології електронного урядування: Навч. посіб. К.: Центр навчальної літератури, 2018. 225 с.

55. Ковальова В.І., Литовченко О.Ю. (2024). Стандарти, впровадження та перспективи цифровізації документообігу в Україні. [Електронний ресурс]. URL: http://journals-lute.lviv.ua/index.php/visnyk-econom/article/view/1760 (Дата звернення: 18.03.2025).

56. Ковальова, В. І., Михайленко, Д. Г., Куц, Н. В. (2025). Особливості реалізації процесу автоматизації діловодства на підприємствах України.

Проблеми сучасних трансформацій. Серія: економіка та управління, (17). DOI: https://doi.org/10.54929/2786-5738-2025-17-04-10 (Дата звернення: 18.03.2025).

57. Ковач О.В., Ковач Д.Л. Досвід країн ЄС щодо використання технології блокчейн (технології розподіленого реєстру) у публічному управлінні: порівняльно-правовий аналіз. Фінансова архітектоніка та сценарії конкурентних моделей розвитку: тези доповідей Міжнар. наук.-практ. конф., 17 листопада 2023 р. Харків: Держ. біотехнологічний ун-т, 2023. С. 135-136.

58. Кокорєва, О. В. (2024). Використання штучного інтелекту в адміністративному менеджменті: переваги та ризики. Economic Synergy, (4), 46–56. DOI: https://doi.org/10.53920/ES-2024-4-3 (Дата звернення: 18.03.2025).

59. Колощук, М. С., Дячук, О. Ю., Окунькова, О. О., & Пірог, О. В. (2024). Інструменти штучного інтелекту для автоматизації тестування на проникнення. Технічна інженерія, (2(94), 121–128. DOI: https://doi.org/10.26642/ten-2024-2(94)-121-128 (Дата звернення: 18.03.2025).

60. Концепція розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 13.12.2010 № 2250-р. URL: https://zakon.rada.gov.ua/laws/show/2250-2010-%D1%80#Text.

61. Корж І.Ф. (2023). *Адміністративно-правове регулювання відносин у сфері державної безпеки України: монографія*. Київ: НДЦПІ НАПрН України, 556 с. URL: http://www.ndcpi.gov.ua/index.php/uk/publikatsiji/monografiji.

62. Коростін, О. О. (2024). Ефективність розпізнавання тексту в автоматизації міжнародних морських перевезень за допомогою штучного інтелекту. Таврійський науковий вісник. Серія: Технічні науки, (3), 29–38. DOI: https://doi.org/10.32782/tnv-tech.2024.3.4 (Дата звернення: 18.03.2025).

63. Кравченко О.В., Шаповал О.Б. Блокчейн технології: стан та перспективи розвитку в Україні. Вісник Хмельницького національного університету. Серія «Економічні науки». 2021. №6, Т. 2. С. 267-272. URL: http://economy.khmnu.edu.ua/index.php/economy/article/view/123456.

64. Круглов, Віталій Вікторович, Терещенко, Діна Акрамівна. Інновації в системі державного управління: Вісник Національного технічного

університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства / № 2 (2023). DOI: https://doi.org/10.20998/2227-6890.2023.2.13 (Дата звернення: 18.03.2025).

65. Крутов В.В. (2022). *Протидія інформаційним загрозам та кібертероризму: монографія*. Київ: Наукова думка, 326 с**.** URL: http://www.ndumka.kiev.ua/product/protidiya-informatsiynim-zagrozam-ta-kiberterorizmu/.

66. Кудь А., Кучерявенко М., Смичок Є. Цифрові активи та їх правове регулювання у світі розвитку технології блокчейн. Харків: Право, 2022. 216 с.

67. Куйбіда В.С., Петроє О.М., Федулова Л.І., Андрощук Г.О. (2019). Цифрові компетенції як умова формування якості людського капіталу: аналіт. записка. Київ: НАДУ, 28 с. URL**:** http://academy.gov.ua/pages/dop/198/files/90a7d5c8-d10a-4f8f-8987-4d1077fdc8f6.pdf.

68. Кураташвілі А.А. (2022). Електронне урядування та проблеми захисту інформації. *Публічне управління та митне адміністрування*, (1(32)), 86–92. URL: http://www.pma.dsu.dp.ua/index.php/pma/article/view/448.

69. Лєнков С.В. (2021). *Комплексний захист інформації в комп'ютерних системах та мережах: навчальний посібник*. Київ: НПУ імені М.П. Драгоманова, 534 с. URL: http://www.npu.edu.ua/ua/library.

70. Лєнков С.В. (2021). *Методи та засоби захисту інформації: У 2-х томах. Т. 1: Несанкціонований доступ до інформації*. Київ: НПУ імені М.П. Драгоманова, 462 с. URL: http://www.npu.edu.ua/ua/library.

71. Лєнков С.В. (2023). Збалансована система показників для оцінки інформаційних систем оборонного призначення. *Сучасні інформаційні технології у сфері безпеки та оборони*, (1(46)), 13–20. URL: http://sit.nuou.org.ua/index.php/sit/article/view/234.

72. Ліпкан В.А. (2022). *Національна безпека України: навчальний посібник*. Київ: КНТ, 576 с. URL: https://knt.com.ua/product/natsionalna-bezpeka-ukrayini-navchalniy-posibnik/.

73. Лопушинський І.П. (2021). *Електронне урядування та електронна демократія: навчальний посібник*. Київ: НАДУ, 144 с. URL: http://academy.gov.ua/?lang=ukr&tip=dop&tipid=monogr.

74. Луценко В.Р., Пікуля Т.О. (2024). Правове забезпечення цифрової трансформації в Україні. *Науковий вісник Ужгородського національного університету. Серія Право*, (81, ч. 1, т. 1), 61–67. URL: http://www.visnyk-pravo.uzhnu.edu.ua/article/view/123456.

75. Матвієнко О., Цивін М. (2008). Основи організації електронного документообігу. Київ: Центр навчальної літератури, 112 с. URL: http://www.dut.edu.ua/uploads/l_1583_62194647.pdf.

76. Матвієнко О.В., Цивін М.Н. (2021). *Документознавство та інформаційна діяльність: навчальний посібник*. Київ: Центр навчальної літератури, 352 с. URL: https://cnl.com.ua/book/1677-dokumentoziavstvo-ta-informaciyna-diyalnist.html.

77. Мельник Р.С. (2021). *Адміністративне право України (у схемах та коментарях): навчальний посібник*. Київ: Юрінком Інтер, 344 с. URL: https://yurincom.com/ua/book/Administratyvne-pravo-Ukrayiny-u-skhemah-ta-komentaryah/.

78. Мельник Р.С. (2021). *Сервісно-орієнтований підхід у державному управлінні: теорія та практика: монографія*. Київ: Видавничий дім "Гельветика", 346 с. URL: https://helvetica.com.ua/product/servisno-oriyentovanyy-pidhid-u-derzhavnomu-upravlinni-teoriya-ta-praktyka/.

79. Мельник Р.С. (2022). Методика оцінки ефективності інформаційних систем у державному управлінні. *Ефективність державного управління*, (2(71)), 56–67. URL: http://www.lvivacademy.com/vidannya_edu/visnyk_71/71_05.pdf.

80. Миколаєць, В. А. (2023). Стан правової регламентації застосування технологій штучного інтелекту. Ірпінський юридичний часопис, (1(8), 42–51. DOI: 10.33244/2617-4154-1(8)-2022-42-51 (Дата звернення: 18.03.2025).

81. Наказ Міністерства юстиції України від 1 листопада 2012 року № 1600/5 “Про затвердження Порядку роботи з електронними документами через

систему електронної взаємодії”. URL: https://zakon.rada.gov.ua/laws/show/z1867-12.

82. Оксютенко, К. В. (2024). Правові засади розвитку електронного урядування в Україні в умовах європейської інтеграції. Київський часопис права, (3), 163–170. DOI: https://doi.org/10.32782/klj/2024.3.24 (Дата звернення: 18.03.2025).

83. Особиста кібербезпека: паролі та месенджери. URL: https://mod.gov.ua/osobista-kiberbezpeka-paroli-ta-mesendzheri (дата звернення: 15.03.2025).

84. Осьмак, А., Карпенко, Ю., & Семененко, І. (2023). Використання інструментів штучного інтелекту в мережевому управлінні: переваги, ризики та розвиток. Аспекти публічного управління, 11(3), 38–42. DOI: https://doi.org/10.15421/152333 (Дата звернення: 18.03.2025).

85. Пархоменко-Куцевіл, О. (2024). Обґрунтування використання технологій штучного інтелекту у системі управління персоналом публічної служби України. Публічне управління: концепції, парадигма, розвиток, удосконалення, (8), 98–106. DOI: https://doi.org/10.31470/2786-6246-2024-8-98-106 (Дата звернення: 18.03.2025).

86. Петров В.В. (2021). *Адаптивне управління інформаційними системами: теорія та практика: навчальний посібник*. Київ: КНЕУ, 298 с. URL: https://kneu.edu.ua/ua/library.

87. Петров В.В. (2022). *Національна безпека України: інформаційна складова: монографія*. Київ: Кондор, 408 с. URL: https://kondor.com.ua/product/natsionalna-bezpeka-ukrayini-informatsiyna-skladova/.

88. Петров В.В. (2023). *Інформаційні системи і технології в кібербезпеці: навчальний посібник*. Київ: КНЕУ, 272 с. URL: https://kneu.edu.ua/ua/library.

89. Плахов, В. Ю., Доценко, Н. В. (2024). Автоматизація управління проектними показниками через використання AI та Predictive Analytics.

Таврійський науковий вісник. Серія: Технічні науки, (5), 65–78. DOI: https://doi.org/10.32782/tnv-tech.2024.5.7. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/100f259e94b3b5317bd094fbb7d1af4a2839d2ee (Дата звернення: 18.03.2025).

90. Попов О.П. (2023). Дискурсне поле цифрової взаємодії органів публічної влади в умовах розвитку електронного урядування. *Державне управління: удосконалення та розвиток*, (11). URL: http://www.dy.nayka.com.ua/?op=1&z=123456.

91. Постанова Кабінету Міністрів України від 17 січня 2018 року № 55 "Деякі питання документообігу в органах виконавчої влади". URL: https://zakon.rada.gov.ua/laws/show/55-2018-п.

92. Постанова Кабінету Міністрів України від 18 липня 2012 року № 670 "Деякі питання електронної взаємодії органів виконавчої влади". URL: https://zakon.rada.gov.ua/laws/show/670-2012-п.

93. Почепцов Г.Г. (2022). *Сучасні інформаційні війни*. Київ: Видавничий дім "Києво-Могилянська академія", 504 с. URL: https://www.ukma.edu.ua/index.php/virobnitstvo/vidavnichii-dim/pocheptsov-g-g-suchasni-informatsiini-viini.

94. Державне агентство з питань технічного регулювання та споживчої політики України. (2019). ДСТУ ISO/IEC 27001:2019. Інформаційні технології – Методи управління інформаційною безпекою – Системи управління інформаційною безпекою – Вимоги [Стандарт]. Київ. https://standart.gov.ua/uk/standarts/dstu-iso-iec-27001-2019.

95. Постанова Кабінету Міністрів України "Питання забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах" від 08.02.2021 № 92. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/go/92-2021-п.

96. Примиська, С. О., Кримська, А. О., Супрун, О. М. (2024). Стратегії забезпечення безпеки даних у системах штучного інтелекту. Таврійський

науковий вісник. Серія: Технічні науки, (2), 88–99. DOI: https://doi.org/10.32782/tnv-tech.2024.2.8 (Дата звернення: 18.03.2025).

97. Про внесення змін до деяких законів України щодо функціонування Національної системи конфіденційного зв'язку та Національної електронної комунікаційної мережі: Проєкт Закону від 20.11.2023 № 10273. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/43261.

98. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12 (дата звернення: 15.03.2025).

99. НД ТЗІ 2.5-010-03. Керівництво з розроблення засобів технічного та криптографічного захисту інформації. – [Електронний ресурс]. – Режим доступу: офіційний сайт Державної служби спеціального зв'язку та захисту інформації України – https://dsszzi.gov.ua (дата звернення: 15.03.2025).

100. Закон України "Про електронну ідентифікацію" від 07.06.2018 № 2156-VIII. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2156-19 (дата звернення: 15.03.2025).

101. НД ТЗІ 2.5-004-99 Вимоги щодо захисту інформації в автоматизованих системах. Загальні положення. – [Електронний ресурс]. – Режим доступу: https://dsszzi.gov.ua (дата звернення: 15.03.2025).

102. Про затвердження Порядку організації електронного документообігу в системі Міністерства оборони України: Наказ Міністерства оборони України від 20.07.2020 № 256. URL: https://www.mil.gov.ua/content/mou_orders/mou_2020/nm_256.pdf (дата звернення: 15.03.2025).

103. General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. – [Electronic resource]. – Mode of access: https://eur-lex.europa.eu/eli/reg/2016/679/oj (date of access: 15.03.2025).

104. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. – [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 15.03.2025).

105. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021 (дата звернення: 15.03.2025).

106. Радутний О.Е. Criminal Liability of the Artificial Intelligence. Problems of Legality. 2017. No. 138. P. 132-141. DOI: 10.21564/2414-990x.138.105661.

107. Роман В.І. (2022). Міжнародний досвід розвитку систем електронного урядування. *Ефективність державного управління*, (1(70)), 30–45. URL: http://www.lvivacademy.com/vidannya_edu/visnyk_70/70_03.pdf.

108. Руснак І.С. (2023). *Військова безпека України: теорія, методологія, практика: монографія*. Київ: НУОУ, 488 с. URL: https://nuou.org.ua/library.

109. Сизов А.І. (2023). Критичні фактори успіху впровадження інформаційних систем у секторі безпеки і оборони. *Стратегічні пріоритети*, (2(63)), 108–116. URL: https://niss.gov.ua/sites/default/files/2023-06/Strategic-Priorities-63-2023.pdf.

110. Сніцаренко П.М. (2022). *Інформаційно-аналітичне забезпечення органів державного управління: теоретико-методологічні засади: монографія*. Київ: НАДУ, 386 с. URL: http://academy.gov.ua/?lang=ukr&tip=dop&tipid=monogr.

111. Сорока, Л. В., Луценко-Миськів, Л. І., & Куркова, К. М. (2024). Правове регулювання платформізації суспільних відносин на прикладі соціально-трудової сфери. Київський часопис права, (1), 85–91. DOI: https://doi.org/10.32782/klj/2024.1.11 (Дата звернення: 18.03.2025).

112. European Defence Agency. Cyber Defence Programme. –Електронний ресурс. – Режим доступу: офіційний сайт Європейської оборонної агенції – https://www.eda.europa.eu/what-we-do/capability-development/cyber.

113. Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards the

establishment of a framework for a European Digital Identity. – [Electronic resource]. – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1183 (date of access: 15.03.2025).

114. Толубко В.Б. (2021). Інформаційне забезпечення оперативного управління військами. *Наука і техніка Повітряних Сил Збройних Сил України*, (3(44)), 12–18. URL: http://ntps.vntu.edu.ua/index.php/ntps/article/view/432.

115. Толубко В.Б. (2022). Розвиток інформаційних технологій в оборонній сфері. *Наука і техніка Повітряних Сил Збройних Сил України*, (1(46)), **7–12.** URL: http://ntps.vntu.edu.ua/index.php/ntps/article/view/456.

116. Трофименко, О. Г., Соколов, А. В., Чикунов, П. О., Ахмаметьєва, Г. В., Манаков, С. Ю. (2024). AI in the Military Cyber Domain. Technologies and Engineering, (4), 85–92. DOI: https://doi.org/10.30857/2786-5371.2024.4.8. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/ffe7e81af3f86c8cd0dfab729acc0064e5b26dde (Дата звернення: 18.03.2025).

117. Турчинов О.В. (2022). Трансформація системи стратегічного планування у секторі безпеки і оборони. *Стратегічні пріоритети*, (1(62)), 5–14. URL: https://niss.gov.ua/sites/default/files/2022-03/Strategic-Priorities-62-2022.pdf.

118. Указ Президента України від 27.09.1999 № 1229 “Про Положення про технічний захист інформації”. URL: https://zakon.rada.gov.ua/laws/show/1229/99.

119. Хорошко В.О. (2021). *Методи та засоби захисту інформації: навчальний посібник*. Київ: ДУІКТ, 478 с. URL: http://www.duikt.edu.ua/library.

120. Хорошко В.О. (2023). Перспективні технології захисту інформації в системах оборонного призначення. *Захист інформації*, 25(2), 73–81. URL: http://journal.itz.org.ua/index.php/zi/article/view/345.

121. Хорошко В.О. (2023). *Технічний захист інформації на об’єктах інформаційної діяльності: навчальний посібник*. Київ: ДУІКТ, 372 с. URL: http://www.duikt.edu.ua/library.

122. Цира, О. В. (2024). Цифрова трансформація органів державного управління: роль ІКТ в оптимізації управлінських процесів. Economic Synergy, (4), 171–181. DOI: https://doi.org/10.53920/ES-2024-4-12 (Дата звернення: 18.03.2025).

123. Цифрова трансформація економіки України в умовах війни. Жовтень 2024 року. Національний інститут стратегічних досліджень. URL: https://niss.gov.ua/news/komentari-ekspertiv/tsyfrova-transformatsiya-ekonomiky-ukrayiny-v-umovakh-viyny-zhovten-2024.

124. Олійченко, І., Дітковська, М., & Клочко, А. (2024). Digital Transformation of Public Authorities in Wartime: The Case of Ukraine. Journal of Information Policy, 14, 686–746. https://doi.org/10.5325/jinfopoli.14.2024.0020.

125. Цифрові трансформації в Україні: чи відповідають вітчизняні інституційні умови зовнішнім викликам та європейському порядку денному? (2021). URL: http://eap-csf.org.ua/wp-content/uploads/2021/04/Research_DT_PF_WG2_ua-1.pdf.

126. Чередник, Л. А., Юницька, В. В. (2024). Використання штучного інтелекту в документообігу та інформаційній діяльності. [Електронний ресурс]. URL: https://reposit.nupp.edu.ua/bitstream/PoltNTU/17541/1/%D0%AE%D0%9D%D0%B8%D1%86%D0%AC%D0%9A%D0%90%20151-155.pdf (Дата звернення: 18.03.2025).

127. Чистоклетов Л., Обрембальський С. Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. Академічні візії. 2024. Вип. 29. URL: https://www.academy-vision.org/index.php/av/article/view/1141.

128. Швед, В., Щур, І. (2024). Використання штучного інтелекту в управлінні діяльністю підприємства. Подільський науковий вісник. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/10d1b99a523f52465ad55fc4218b5851470521bb (Дата звернення: 18.03.2025).

129. Шевченко В.Л. (2021). *Проектування комп'ютеризованих систем управління: теорія та практика: монографія*. Київ: НУОУ, 284 с. URL: https://nuou.org.ua/library.

130. Шевченко В.Л. (2021). Управління змінами в інформаційних системах оборонного призначення. *Збірник наукових праць ВІТІ,* (3), 73–82. URL: http://viti.nuos.mil.gov.ua/index.php/viti/article/view/123.

131. Шевченко В.Л. (2022). Онтологічний підхід до побудови інформаційних систем. *Збірник наукових праць ВІТІ*, (2), 62–70. URL: http://viti.nuos.mil.gov.ua/index.php/viti/article/view/156.

132. Шевченко В.Л. (2022). Технологія blockchain у системах електронного документообігу. *Збірник наукових праць ВІТІ*, (4), 81–89.URL: http://viti.nuos.mil.gov.ua/index.php/viti/article/view/167.

133. Шевченко В.Л. (2023). Комплексна оцінка ефективності інформаційних систем. *Збірник наукових праць ВІТІ*, (1), 45–53.URL: http://viti.nuos.mil.gov.ua/index.php/viti/article/view/189.

134. Яковлєв, С.Ю. (2023). Інструменти електронного урядування в Україні: стан та перспективи розвитку. Bulletin of the National University of Civil Protection of Ukraine. Series: Public Administration. DOI: 10.52363/2414-5866-2023-2-23. [Електронний ресурс]. URL: https://www.semanticscholar.org/paper/5ff86c21b43f6cb5f04aa44791af34ab8259ece6 (Дата звернення: 18.03.2025).

135. Яровой, Т. С. (2023). Можливості та ризики використання штучного інтелекту в публічному управлінні. Economic Synergy, (2), 36–47. DOI: https://doi.org/10.53920/ES-2023-2-3 (Дата звернення: 18.03.2025).

136. Actively exploit new opportunities. Siemens. (2025). URL: https://new.siemens.com/global/en/markets/municipalities-dsos/business-models.html.

137. Agence Nationale de la Sécurité des Systèmes d'Information. (2017). Guide d'hygiène informatique. Paris: ANSSI. URL:

https://www.ssi.gouv.fr/uploads/2017/01/anssi-cgpmi-guide_hygiene_informatique-2017.pdf.

138. Нестеренко В. О. Напрями організації взаємодії складових сектору безпеки і оборони держави в системі електронного міжвідомчого документообігу. Публічне у правління XXI століття: погляд у майбутнє: зб. тез XXI Міжнар. наук. конгресу. – Вид-во ХарРІ НАДУ "Магістр", 2021. – С.494-497.

139. Agence Nationale de la Sécurité des Systèmes d'Information. (2018). Référentiel Général de Sécurité, version 2.0. Paris: ANSSI. URL: https://www.ssi.gouv.fr/uploads/2018/02/referentiel_general_de_securite_v2.0.pdf.

140. Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Référentiel général de sécurité (RGS), version 2.0 – arrêté du Premier ministre du 13 juin 2014. – [Ressource électronique]. – Mode d'accès : https://www.ssi.gouv.fr/uploads/2018/02/referentiel_general_de_securite_v2.0.pdf.

141. Agence Nationale de la Sécurité des Systèmes d'Information. (2019). Qualification des produits de sécurité. Paris: ANSSI. URL: https://www.ssi.gouv.fr/administration/qualifications/qualification-des-produits-de-securite/.

142. Agence Nationale de la Sécurité des Systèmes d'Information. (2020). Prestataires de services de confiance qualifiés. Paris: ANSSI. URL: https://www.ssi.gouv.fr/administration/prestataires/prestataires-de-services-de-confiance-qualifies/.

143. Assessing the Effects and Risks jf Large Language Models in Ai-Mediated Communication Maurice Jakesch, Ph.D. Cornell University 2022. https://www.jakesch-lab.org/assets/pdf/thesis_jakesch_cornell_phd.pdf.

144. Backyard AI. (2024). Self-hosted AI assistant platform. https://backyard.ai/.

145. Bhelotkar, M. (2008). E-Governance in India: Way to Success. *Semantic Scholar* URL: https://www.semanticscholar.org/paper/E-Governance-in-India%3A-Way-to-Success-Bhelotkar/4b5b74599ca2c3e69989b9a63d633cf64d614736.

146. Blockchain for Secure Document Management. Journal of Cybersecurity, 2024, 10(3), 215–230.

147. Bundesamt für Sicherheit in der Informationstechnik. (2016). IT-Grundschutz Catalogues. Bonn: BSI. URL: https://www.bsi.bund.de/EN/Topics/IT-Grundschutz/IT-Grundschutz-Catalogues/it-grundschutz-catalogues_node.html.

148. Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Kompendium – Edition 2022. Bonn: BSI, 2022. – [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2022.pdf (дата звернення: 15.03.2025).

149. Bundesamt für Sicherheit in der Informationstechnik. (2018). Secure Information Sharing Architecture. Bonn: BSI. URL: https://www.bsi.bund.de/EN/Topics/Cyber-Security/Recommendations/Secure-Information-Sharing/secure-information-sharing_node.html.

150. Bundesamt für Sicherheit in der Informationstechnik (BSI). Technische Richtlinie TR-03181 Technical Guideline for Cryptographic Service Provider 2 (CSP-2). Bonn: BSI. – [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/EN/Themen/Standards/TR-03181 (дата звернення: 15.03.2025).

151. Bundesamt für Sicherheit in der Informationstechnik. (2020). IT-Grundschutz Methodology. Bonn: BSI. URL: https://www.bsi.bund.de/EN/Topics/IT-Grundschutz/it-grundschutz_node.html.

152. Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 200-2: IT-Grundschutz-Methodik. Version 1.0 (May 2008). Bonn: BSI, 2008. – [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.pdf (дата звернення: 15.03.2025).

153. Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz Compendium – Edition 2021. Bonn: BSI, 2021. – [Електронний ресурс]. – Режим доступу:

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf (дата звернення: 15.03.2025).

154. Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI Standard 200-2: IT-Grundschutz Methodology, Version 1.0. Bonn: BSI, 2020. – [Електронний ресурс]. – Режим доступу: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/BSI-Standard_200-2.pdf (дата звернення: 15.03.2025).

155. Нестеренко В.О., Нагорний О.А. Теоретичні засади Державної політики щодо створення, впровадження та функціонування захищеної системи електронного міжвідомчого документообігу сфери оборони Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: тези доповідей XXIX міжнародної науково-практичної конференції MicroCAD-2021, 18-20 травня 2021р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ «ХПІ».с. 145.

156. Cybersecurity Training Impact. SANS Institute, 2023. URL: https://www.sans.org.

157. DAS, B. C., Amini, M. H., & Wu, Y. (2025). Security and privacy challenges of large language models: A survey. ACM Computing Surveys, 57(6), 1-39.

158. DAS, Badhan Chandra; AMINI, M. Hadi; WU, Yanzhao. Security and privacy challenges of large language models: A survey. ACM Computing Surveys, 2025, 57.6: 1-39. Ollama Models Library. (2024). Available models. https://ollama.com/library.

159. Derczynski, L., Galinkin, E., Martin, J., Majumdar, S., & Inie, N. (2024). garak: A framework for security probing large language models. arXiv preprint arXiv:2406.11036. Kolchenko, V., Khoma, V., Sabodashko, D., & Perepelytsia, P. (2024). Exploring large language models' security threats with automated tools. Social Development and Security, 14(6), 81-96. https://doi.org/10.33445/sds.2024.14.6.9.

160. Digital Economy and Society Index 2022: overall progress but digital skills, SMEs and 5G networks lag behind. (2022). European Commission. URL:

https://digital-strategy.ec.europa.eu/en/news/digital-economy-and-society-index-2022-overall-progress-digital-skills-smes-and-5g-networks-lag.

161. European Commission. Digital Economy and Society Index (DESI) 2023 Report. URL: https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2023 (дата звернення: 15.03.2025).

162. Нестеренко В.О., Перспективи та виклики впровадження захищеного ШІ-орієнтованого СЕДО в Збройних Силах України XXV Міжнародного наукового конгресу Публічне управління XXI століття: основні виклики післявоєнної відбудови.

163. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on Measures for a High Common Level of Cybersecurity Across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022L2555.

164. Нестеренко В. О. Огляд створення та впровадження захищеної системи електронного документообігу Збройних Сил України // Електронне наукове видання "Публічне адміністрування та національна безпека". – 2020. – *№1*. https://doi.org/10.25313/2617-572X-2020-1-5580.

165. DoD Enterprise Content Management. U.S. Department of Defense, 2024. URL: https://www.defense.gov.

166. Dutch Government. (2020). API Strategy: The Application Programming Interface for the Dutch government. The Hague: Ministry of the Interior and Kingdom Relations. URL: https://www.government.nl/documents/publications/2020/03/01/api-strategy-for-the-dutch-government.

167. Dutch Ministry of Defence. (2018). Defence Cyber Strategy. The Hague: Ministry of Defence. URL: https://www.defensie.nl/downloads/publicaties/2018/11/12/defence-cyber-strategy-2018.pdf.

168. Dutch Ministry of the Interior and Kingdom Relations. (2020). NL DIGIbeter – Digital Government Agenda. The Hague: Ministry of the Interior and Kingdom Relations. URL:

https://www.government.nl/documents/publications/2020/07/01/nl-digibeter-digital-government-agenda.

169. Netherlands Government. NL DIGIbeter – Digital Government Agenda 2020. The Hague: Ministry of the Interior and Kingdom Relations, 2020. URL: https://www.government.nl/documents/publications/2020/07/01/nl-digibeter-digital-government-agenda (дата звернення: 15.03.2025).

170. Estonian Information System Authority. (2020). X-Road: The Backbone of e-Estonia. Tallinn: RIA. URL: https://x-road.global/x-road.

171. Estonian Information System Authority. (2020). Estonian Information Security Strategy 2019–2023. Tallinn: RIA. URL: https://www.ria.ee/en/information-security-strategy.html (дата звернення: 15.03.2025).

172. Орлов, О., Живило, Є., & Нестеренко, В. (2025). Нормативно-правові аспекти електронного документообігу в системі державного управління сектору оборони держави. *Аспекти публічного управління, 13* (1), 106-113. https://doi.org/10.15421/152512.

173. Estonian Information System Authority. (2021). X-Road Security Server User Guide. Tallinn: RIA. URL: https://x-road.global/documentation.

174. Estonian Information System Authority. (2020). X-Road Security and Trust Model. Tallinn: RIA. URL: https://x-road.global/assets/files/X-Road-Security-and-Trust-Model.pdf (дата звернення: 15.03.2025).

175. Estonian Ministry of Defence. (2019). Cyber Security Strategy 2019-2022. Tallinn: Ministry of Defence. URL: https://www.kaitseministeerium.ee/sites/default/files/content-files/2019-06/Cyber_Security_Strategy_2019-2022_ENG.pdf.

176. Kaska, K., & Kaska, K. (2020). Cybersecurity in Estonia: Lessons Learned and Future Challenges. Journal of Cyber Policy, 5(1), 1–18. DOI: 10.1080/23738871.2020.1723856.

177. European Commission. (2016). eGovernment Action Plan 2016-2020. Brussels: European Commission. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179.

178. European Commission. (2017). New European Interoperability Framework. Brussels: European Commission. URL: https://ec.europa.eu/isa2/sites/default/files/eif_brochure_2017.pdf.

179. European Commission. (2021). European Interoperability Framework – Implementation Strategy. Brussels: European Commission. URL: https://ec.europa.eu/isa2/sites/default/files/eif_implementation_strategy_2021.pdf.

180. European Commission. (2019). European Interoperability Reference Architecture (EIRA). Brussels: European Commission. URL: https://joinup.ec.europa.eu/collection/eira/about.

181. European Parliament & Council. (2022, 30 листопада). Directive (EU) 2022/2107 – Interoperable Europe Act. Official Journal of the European Union, L 283, 1–22. https://eur-lex.europa.eu/eli/reg/2022/2107/oj.

182. European Interoperability Framework (EIF). European Commission. URL: https://ec.europa.eu/isa2/eif_en.

183. Meyer, I., & Kunzmann, C. (2017). European Interoperability Framework: A practical implementation approach for public administrations. Government Information Quarterly, 34(4), 512–521. https://doi.org/10.1016/j.giq.2017.07.002.

184. European Parliament and Council. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng.

185. Mellquist, A., & Schmidt, C. (2018). Implementing the NIS Directive: Challenges and opportunities for EU member states. Journal of Cyber Policy, 3(2), 203–223. https://doi.org/10.1080/23738871.2018.1496783.

186. European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

187. Kuner, C. (2017). The General Data Protection Regulation: A commentary. International Data Privacy Law, 7(1), 1–3. https://doi.org/10.1093/idpl/ipw025.

188. European Parliament and Council. (2019). Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification. Official Journal of the European Union. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj.

189. Smith, J., & Müller, A. (2020). Enhancing Cybersecurity in the EU: An Analysis of the Cybersecurity Act and ENISA's New Role. Journal of Information Security and Applications, 53, 102512. https://doi.org/10.1016/j.jisa.2020.102512.

190. Faraday.dev. (2024). Local AI Development Environment. https://faraday-dev.en.softonic.com/web-apps.

191. Feretzakis G, Papaspyridis K, Gkoulalas-Divanis A, Verykios VS. Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review. *Information*. 2024; 15(11):697. https://doi.org/10.3390/info15110697.

192. Finland e-Government Strategy. Ministry of Finance, 2023. – [Електронний ресурс]. – Режим доступу: https://vm.fi/en/e-government (дата звернення: 24.06.2025).

193. Finnish Government. (2016). Digital security: Guidance of services and security Helsinki: Ministry of Finance. URL: https://vm.fi/en/information-security-and-cybersecurity.

194. Finnish Government. (2017). Security Strategy for Society. Helsinki: The Security Committee. URL: https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf.

195. Virtanen P., Stenvall J. Smart government: A new adjective to government // Information Polity. – 2019. – Vol. 24, № 1. – P. 3–14. – DOI: https://doi.org/10.3233/IP-180083.

196. Finnish Government. (2020). Information Security and Cybersecurity in Defence Administration. Helsinki: Ministry of Defence. URL:

https://www.defmin.fi/files/4749/Information_Security_and_Cybersecurity_in_Defence_Administration_2020.pdf.

197. Finnish Ministry of the Interior. (2019). KEJO – A common field command system for all security authorities. Helsinki: Ministry of the Interior. URL: https://intermin.fi/en/projects/kejo.

198. Simola, J., & Rajamäki, J. (2022). Common Cyber Situational Awareness: An Important Part of Modern Public Protection and Disaster Relief. WSEAS Transactions on Communications, 21, 48–62. https://doi.org/10.37394/23204.2022.21.9.

199. Gelashvili, T., Pappel, I. (2021). Challenges of Transition to Paperless Management: Readiness of Incorporating AI in Decision-making Processes. 2021 Eighth International Conference on eDemocracy & eGovernment (ICEDEG), Quito, Ecuador, pp. 41–46. DOI: 10.1109/ICEDEG52154.2021.9530905 (Дата звернення: 18.03.2025).

200. GPT4All. (2024). Run open-source large language models locally. https://gpt4all.io.

201. Gruber, Johannes B. and Maximilian Weber. “rollama: An R package for using generative large language models through Ollama.” ArXiv abs/2404.07654 (2024): n. pag. https://doi.org/10.21105/joss.05321.

202. Guo, D., Zhu, Q., Yang, D., Xie, Z., Dong, K., Zhang, W., ... & Liang, W. (2024). DeepSeek-Coder: When the Large Language Model Meets Programming--The Rise of Code Intelligence. arXiv preprint arXiv:2401.14196.. https://arxiv.org/abs/2401.14196.

203. H. R. Penubadi, “Sustainable electronic document security: A comprehensive framework integrating encryption, digital signature and watermarking algorithms”, Heritage and Sustainable Development, vol. 5, no. 2, pp. 391–404, Dec. 2023. DOI: https://doi.org/10.37868/hsd.v5i2.359.

204. High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. European Commission. 2019. URL: https://digital-

strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (дата звернення: 15.03.2025).

205. Орлов, О., & Нестеренко, В. (2025). Використання штучного інтелекту в документообігу: перспективи та виклики.

206. ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. Schaumburg, IL: ISACA. , обмежений доступURL: https://www.isaca.org/resources/cobit.

207. Jan AI. (2024). Run open-source LLMs locally. https://jan.ai.

208. LM Studio. (2024). Run local large language models. https://lmstudio.ai.

209. Logius. (2020). DigiD: Digital Identity in the Netherlands. The Hague: Ministry of the Interior and Kingdom Relations. URL: https://www.logius.nl/en/services/digid.

210. Stokkink, Q., Ishmaev, G., Epema, D., & Pouwelse, J. (2020). A truly self-sovereign identity system. arXiv. https://doi.org/10.48550/arXiv.2007.00415.

211. Logius. (2021). Digikoppeling Standards and Specifications. The Hague: Ministry of the Interior and Kingdom Relations. URL: https://www.logius.nl/en/services/digikoppeling.

212. Hering, P. (2025, травень 15). Digikoppeling – overzicht actuele documentatie & compliance [Стандартний технічний документ]. Logius. https://gitdocumentatie.logius.nl/publicatie/dk/actueel/1.12.1/.

213. Ministry of Economic Affairs and Communications of Estonia. (2018). Digital Agenda 2020 for Estonia. Tallinn: Ministry of Economic Affairs and Communications. https://www.mkm.ee/en/objectives-activities/digital-society.

214. Ministry of Finance Finland Digital security: Guidance of services and security/ The Act on the Provision of Shared Government Information and Communications Technology Services enables the uniform production and use of such services.. URL: https://vm.fi/en/information-security-and-cybersecurity.

215. Mozilla. (2024). llamafile: Distribute and run LLMs with a single file. https://github.com/Mozilla-Ocho/llamafile.

216. MUC-6. [Електронний ресурс]. URL: http://www.cs.nyu.edu/cs/faculty/grishman/muc6.html (Дата звернення: 11.03.2025).

217. NATO. (2014, October 3). STANAG 4677: Dismounted Soldier Systems Standards and Protocols for Command, Control, Communications and Computers (C4) Interoperability (Ed. 1) [NATO standard]. Retrieved from NATO Standards Library (Active, 11 pp.).

218. NATO Land Capability Group Dismounted Soldier System. (2023, 1 грудня). AEP-76 Vol III Ed A Ver 3: Specifications defining the Joint Dismounted Soldier System Interoperability Network (JDSSIN) – Loaned Radio [Allied Engineering Publication]. NATO Standards Library. https://nso.nato.int/nso/nsdd/main/standards/ap-details/3438/EN.

219. NextChat. (2024). Local ChatGPT-like assistant. https://github.com/next-chat/next-chat.

220. Орлов, О., Живило, Є., & Нестеренко, В. (2025). Принципові напрями розгортання захищеного документообігу на платформах штучного інтелекту.

221. Ollama Documentation. (2024). Modelfile reference. https://github.com/ollama/ollama/blob/main/docs/modelfile.md.

222. Ollama. (2024). Run Llama 2, Mistral, Gemma and other large language models locally. https://ollama.com.

223. Onyshchenko S., Zhyvylo Y., Cherviak A., Bilko S. Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. Eastern-European Journal of Enterprise Technologies. 2023. Vol. 5. No. 13 (125). P. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175.

224. Pooja Bhagavat & Memorial Mahajana. (2008). Successful e-Governance Projects in Karnataka - A Case Study. *Semantic Scholar***.** URL: https://www.semanticscholar.org/paper/Successful-e-Governance-Projects-in-Karnataka-A-Bhagavat-Mahajana/5783a3a5210bce321b9382b0576ae4ff0373f9c5.

225. Post-Quantum Cryptography Standards. NIST, 2024. URL: https://csrc.nist.gov/projects/post-quantum-cryptography.

226. Sahana Upadhya et al., A State-of-Art Review of Docker Container Security Issues and Solutions American International Journal of Research in Science, Technology, Engineering & Mathematics, 17(1), December 2016-February 2017, pp. 33-36 https://www.researchgate.net/publication/315823494.

227. Spasiteleva S.O., Buriachok V.L. Перспективи розвитку додатків блокчейн в Україні. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». 2018. №1(1). С. 35-48. DOI: https://doi.org/10.28925/2663-4023.2018.1.3548.

228. Summary of the NATO Artificial Intelligence Strategy. 2021. URL: https://www.nato.int/cps/en/natohq/official_texts_187617.htm (дата звернення: 15.03.2025).

229. Taranych, A., Pelekhatskyi, D. (2024). Use of Artificial Intelligence in Strategic Management of Enterprises. Economy of Ukraine, 67(1(746), 54–65. DOI: https://doi.org/10.15407/economyukr.2024.01.054 (Дата звернення: 18.03.2025).

230. The “Big 8” Trends in Document Management in 2025. January 27, 2025 https://www.adlibsoftware.com/news/the-big-8-trends-in-document-management-in-2025.

231. Towards a European Strategy on Business-to-Government Data Sharing for the Public Interest: Final Report. Brussels: European Commission, 2024. URL: https://digital-strategy.ec.europa.eu/en/policies/business-government-data-sharing.

232. U.S. Department of Defense. DoD Adopts Ethical Principles for Artificial Intelligence. 2020. URL: https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/ (дата звернення: 15.03.2025).

233. Ukraine Facility. European Union. URL: https://www.ukrainefacility.me.gov.ua.

234. Vassil, K. (2016). Estonian e-Government Ecosystem: Foundation, Applications, Outcomes. Washington: World Development Report. URL: https://documents1.worldbank.org/curated/en/165711468179099592/pdf/106160-WP-PUBLIC-WDR16-BP-Estonian-eGov-Ecosystem-Vassil.pdf.

235. X-Road: Data Exchange Layer. e-Estonia. URL: https://e-estonia.com/solutions/interoperability/x-road/.

236. Zhang et al. Analyzing Temporal Complex Events with Large Language Models? ACL 2024. https://doi.org/10.18653/v1/2024.acl-long.87.

237. Zhyvylo , Y. (2024). National macrofinancial stability in the context of cyber threats. Pressing Problems of Public Administration, 2(65), 347-369. https://doi.org/10.26565/1684-8489-2024-2-18.

238. Орлов, О., Живило, Ю., та Нестеренко, В. (2025). Електронна взаємодія органів державної влади в контексті цифрової трансформації в повоєнній Україні: де шукати резерви вдосконалення?. Актуальні проблеми державного управління , 1 (66), 273-296. https://doi.org/10.26565/1684-8489-2025-1-13.

239. Zhyvylo, Ye O.; Orlov, O. V. The essence of cyber security of the national segment of the state's cyberspace in the context of crisis management. In: Collection of scientific materials of the 22nd International Scientific Congress "Public administration of the 21st century in the context of hybrid threats" April. 2022. p. 248-254.

ДОДАТКИ

ДОДАТОК А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. Нестеренко В. О. Огляд створення та впровадження захищеної системи електронного документообігу Збройних Сил України // Електронне наукове видання "Публічне адміністрування та національна безпека". — 2020. — №1. *https://doi.org/10.25313/2617-572X-2020-1-5580*.

2. Орлов, О., Живило, Є., & Нестеренко, В. (2025). Нормативно-правові аспекти електронного документообігу в системі державного управління сектору оборони держави. Аспекти публічного управління, 13 (1), 106-113. https://doi.org/10.15421/152512.

3. Орлов, О., & Нестеренко, В. (2025). Використання штучного інтелекту в документообігу: перспективи та виклики. State Formation. No. 1 (37)/2025. https://periodicals.karazin.ua/db/article/view/27245/24168.

4. Орлов, О., Живило, Є., & Нестеренко, В. (2025). Принципові напрями розгортання захищеного документообігу на платформах штучного інтелекту. Theory and Practice of Public Administration 1 (80)/2025. http://doi.org/10.26565/1727-6667-2025-1-02.

5. Орлов, О., Живило, Ю., та Нестеренко, В. (2025). Електронна взаємодія органів державної влади в контексті цифрової трансформації в повоєнній Україні: де шукати резерви вдосконалення?. Актуальні проблеми державного управління , 1 (66), 273-296. https://doi.org/10.26565/1684-8489-2025-1-13.

6. Нестеренко В.О., Аналіз досвіду європейської спільноти держав із запровадження захищеної системи електронної взаємодії в органах державної влади. Суспільство та національні інтереси № 8(16) 2025 с.719. https://doi.org/10.52058/3041-1572-2025-8(16)

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Нестеренко В.О. Порядок здійснення діловодства та документування управлінської інформації в електронній формі в Міністерстві оборони України та Генеральному штабі Збройних Сил України. Публічне управління XXI століття: портал можливостей: зб. тез XX Міжнар. наук. конгресу. – Вид-во ХарРІ НАДУ “Магістр”, 2020. – С. 467-470.

8. Нестеренко В. О. Напрями організації взаємодії складових сектору безпеки і оборони держави в системі електронного міжвідомчого документообігу. Публічне у правління XXI століття: погляд у майбутнє: зб. тез XXI Міжнар. наук. конгресу. – Вид-во ХарРІ НАДУ “Магістр”, 2021. – С.494-497.

9. Нестеренко В.О., Нагорний О.А. Теоретичні засади Державної політики щодо створення, впровадження та функціонування захищеної системи електронного міжвідомчого документообігу сфери оборони Інформаційні технології: наука, техніка, технологія, освіта, здоров’я: тези доповідей XXIX міжнародної науково-практичної конференції MicroCAD-2021, 18-20 травня 2021р.: у 5 ч. Ч. V. / за ред. проф. Сокола Є.І. – Харків: НТУ «ХПІ».с. 145.

10. Нестеренко В.О., Перспективи та виклики впровадження захищеного ШІ-орієнтованого СЕДО в Збройних Силах України. Публічне управління XXI століття: основні виклики післявоєнної відбудови : зб. наук. матер. XXV Міжнар. наук. конгресу [Електронний ресурс]. – Харків : ХНУ імені В. Н. Каразіна, 2025. (PDF 716 с.) с. 315 ISBN 978-966-285-798-6. URI https://ekhnuir.karazin.ua/handle/123456789/22470.

ДОДАТОК Б

ЗАТВЕРДЖУЮ
Начальник Головного управління підготовки Збройних Сил України – заступник начальника Генерального штабу Збройних Сил України

полковник Олексій ТАРАН

“15” 01 2020р.

АКТ

впровадження результатів

наукових досліджень пов’язаних з супроводженням захищеної системи електронного документообігу Міністерства оборони України та Збройних сил України

По навчальній план-програмі підвищення кваліфікації керівників та спеціалістів структурних підрозділів Міністерства оборони України, Генерального штабу Збройних Сил України, органів військового управління, військових частин та установ Збройних Сил України – виконаної в період з 05.11.2019 р. по 04.01.2020 р.

Напряму: Забезпечення та організація електронного документування управлінської інформації.

Категорія тих, хто навчається: військовослужбовці та працівники Збройних Сил України.

Комісія в складі:

голова комісії – заступник начальника Головного управління підготовки Збройних Сил України – полковник ШВЕЦЬ О. М.;

заступник голови комісії – начальник управління підготовки персоналу Головного управління підготовки Збройних Сил України – полковник ГУБЕНЬ М. В.;

члени комісії:

начальник відділу супроводження підготовки у навчальних центрах Головного управління підготовки Збройних Сил України – полковник РУМАК В.А.;

заступник начальника відділу супроводження підготовки у ВВНЗ та ВНП управління підготовки персоналу Головного управління підготовки Збройних Сил України – полковник БЕСТЮК А.І.,

начальник організаційно-планового відділу Головного управління підготовки Збройних Сил України – полковник МАРАНДЮК Г.П.,

встановила, що окремі результати проведених наукових досліджень особисто опрацьовані полковником НЕСТЕРЕНКО Віктором Олександровичем та реалізовані під час розробки навчальної план-програми, зокрема:

у модулі № 1 "Основи організації електронного документообігу" надавати теоретичні та практичні основи системного підходу до діловодства у Збройних Силах України як об'єкта впровадження системи електронного документообігу (далі – СЕДО).

у модулі № 2 "Автоматизована система контролю й організації діловодства (АСКОД)" викладати: основні положення організації документообігу в Центральному апараті Міністерства оборони України та Генерального штабу Збройних Сил України, в частинах і підрозділах Збройних Сил України, основні підходи до впровадження СЕДО; теорії та практики щодо основ організації електронного документування управлінської інформації. Порядок та способи дій щодо забезпечення функціонування СЕДО, надання початкових навичок щодо налаштувань роботи програмних засобів АСКОД та забезпечення діловодства в підрозділах та установах.

Активними формами навчання під час засвоєння навчальної програми визначити практичні заняття з використанням автоматизованих робочих місць посадових осіб, що задіяні в документуванні управлінської інформації.

Інтенсифікацію навчання і розвиток творчих здібностей досягати шляхом створення на заняттях нестандартної обстановки й відтворення проблемних ситуацій, відпрацюванням ситуаційних задач.

Практичну підготовку посилити шляхом проведення практичних занять на автоматизованих робочих місцях керівників, діловодів, виконавців та архіваріусів захищеного СЕДО.

Комісія постановила:

вважати результати наукових досліджень пов'язаних з супроводженням захищеної СЕДО Міністерства оборони України та Збройних Сил України, виконаними полковником НЕСТЕРЕНКО Віктором Олександровичем, начальником загального відділу Головного управління підготовки Збройних Сил України особисто.

Пропозиції комісії:

використати результати наукових досліджень пов'язаних з супроводженням захищеної СЕДО Міністерства оборони України та Збройних сил України, під час здійснення підготовки на курсах підвищення кваліфікації керівників та спеціалістів структурних підрозділів Міністерства оборони України, Генерального штабу Збройних Сил України, органів військового

управління, військових частин та установ Збройних Сил України (військовослужбовці, державні службовці третьої-сьомої категорій та особи, призначені (зараховані до кадрового резерву для призначення) на відповідні посади).

“ 15 ” 01 2020 р.

Голова комісії:	полковник (військове звання)	(підпис)	О. М. ШВЕЦЬ (прізвище)
Заступник голови комісії:	полковник (військове звання)	(підпис)	М. В. ГУБЕНЬ (прізвище)
Члени комісії:	полковник (військове звання)	(підпис)	В.А. РУМАК (прізвище)
	полковник (військове звання)	(підпис)	А.І. БЕСТЮК (прізвище)
	полковник (військове звання)	(підпис)	Г.П.МАРАНДЮК (прізвище)

ДОДАТОК В

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ВІЙСЬКОВА ЧАСТИНА А0106
Код 22991103
«22» 01 2020 р.
№ 308/51/137
03168, м. Київ-168, п-кт Повітрофлотський, 9

ЗАТВЕРДЖУЮ
Начальник військ зв'язку Збройних Сил України – начальник Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України

генерал-лейтенант В.В. РАПКО

"22" 01 2020р.

АКТ
впровадження результатів дисертаційного дослідження під час розробки КСЗІ (комплексної системи захисту інформації) захищеної СЕДО (системи електронного документообігу) та розробки Порядку введення в експлуатацію модулів КСЗІ АРМ (автоматизованих робочих місць) захищеної СЕДО 33102567.62022.001.И2.2

Комісія в складі:

голова комісії – заступник начальника військ зв'язку – начальника Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України полковник ПЛУГОВИЙ Ю.А.;

заступник голови комісії – тимчасово виконуючий обов'язки начальника управління розвитку системи та засобів зв'язку Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України полковник КУДРЯШОВ Д.Л.;

члени комісії:

начальник управління організації зв'язку та інформаційних систем Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України полковник ПРОЦЕНКО О.М.;

начальник управління захисту інформації в інформаційно-телекомунікаційних системах Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України полковник ЛІСАКОНОВ В.В.;

начальник відділу розвитку комплексів і засобів зв'язку управління розвитку комплексів і засобів зв'язку управління розвитку системи та засобів

зв'язку Головного управління зв'язку та інформаційних систем Генерального штабу Збройних Сил України полковник ЛІПКО І.О.,

встановила, що наукові положення, досліджені та розроблені особисто полковником НЕСТЕРЕНКО Віктором Олександровичем, зокрема:

концептуальні положення, що визначають порядок створення та функціонування, введення в експлуатацію модулів КСЗІ АРМ захищеної СЕДО призначених для використання в структурних підрозділах органів військового управління Міністерства оборони України, Генерального штабу Збройних Сил України та інших структурних підрозділах Міністерства оборони України, у яких підключаються АРМ для роботи в захищеній СЕДО;

технологічна основа (побудова) КСЗІ захищеної СЕДО, яка створена за модульним принципом, має підключення до сховищ захищеної СЕДО у відповідності до умов розміщення та з'єднання. Організаційно-технічно обґрунтовано впровадження типових модулів (локальний, віддалений, мобільний) враховуючи тенденції розвитку систем електронного міжвідомчого документообігу сфери оборони.

Одержані результати відповідають:

1. Сучасному рівню наукових знань в галузі захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
2. Сучасним підходам до формування механізмів інформаційного забезпечення системи єдиного захищеного інформаційного середовища електронних документів складових сектору оборони держави.
3. Вимогам нормативно-правових актів з питань технічного захисту інформації в Україні, які визначають теоретичні засади державної політики щодо створення, впровадження та функціонування системи електронного міжвідомчого документообігу сфери оборони.

Комісія постановила:

вважати результати дисертаційного дослідження, виконаними полковником НЕСТЕРЕНКО Віктором Олександровичем, начальником загального відділу Головного управління підготовки Збройних Сил України особистими, а саме: створення та функціонування, введення в експлуатацію модулів КСЗІ АРМ захищеної СЕДО призначених для використання в структурних підрозділах органів військового управління МО України, ГШ ЗС України, порядку здійснення електронної взаємодії між органами державної влади за умов цифрової трансформації в Україні.

Пропозиції комісії:

використати результати дисертаційного дослідження, під час розробки проєкту єдиної системи електронного міжвідомчого документообігу сфери оборони у інформаційно-телекомунікаційних системах різного призначення та різного рівня складності.

“ 21 ” 01 2020 р.

Голова комісії:	полковник		Ю.А. ПЛУГОВИЙ
	(військове звання)	(підпис)	(прізвище)
Заступник голови комісії:	полковник		Д.Л. КУДРЯШОВ
	(військове звання)	(підпис)	(прізвище)
Члени комісії:	полковник		О.М. ПРОЦЕНКО
	(військове звання)	(підпис)	(прізвище)
	полковник		В.В. ЛІСАКОНОВ
	(військове звання)	(підпис)	(прізвище)
	полковник		І.О. ЛІПКО
	(військове звання)	(підпис)	(прізвище)

ДОДАТОК Г

ВИТЯГ З ПРОТОКОЛУ

засідання методичної ради Центру оперативних стандартів і методики підготовки Збройних Сил України

№1 "23" лютого 2020 року м. Житомир

У засіданні взяли участь:

голова методичної ради – начальник відділу узагальнення та аналізу підготовки – заступник начальника Центру оперативних стандартів і методики підготовки Збройних Сил України полковник Бойко О.П.

члени методичної ради:

заступник начальника відділу узагальнення та аналізу підготовки Центру оперативних стандартів і методики підготовки Збройних Сил України полковник Котляренко Я.М.;

тимчасово виконуючий обов'язки начальник відділу оперативних стандартів і методики підготовки Сухопутних військ полковник Грищук В.М.;

начальник відділу оперативних стандартів і методики підготовки Повітряних сил полковник Білецький Я.В.;

офіцер адміністративної групи підполковник Чернишов О.С.

секретар методичної ради:

головний спеціаліст відділу узагальнення та аналізу підготовки полковник Чернов О.В.

Всього: 6 офіцерів.

І. ПОРЯДОК ДЕННИЙ:

1. Про надання науково обґрунтованих рекомендацій та пропозицій в ініціативному порядку начальником загального відділу Головного управління підготовки Збройних сил України полковником Нестеренко В.О.

Доповідач: полковник Нестеренко Віктор Олександровичначальник загального відділу Головного управління підготовки Збройних сил України.

ІІ. СЛУХАЛИ:

Начальника загального відділу Головного управління підготовки Збройних сил України полковника Нестеренко Віктора Олександровича про надання науково обґрунтованих рекомендацій та пропозицій в ініціативному порядку, за рахунок всебічноговивчення та проведення наукових досліджень пов'язаних з супроводженням захищеної системи електронного документообігу Міністерства оборони України (далі – захищена СЕДО-М), процесу її створення та оцінки відповідності до встановленихвимог в Міністерстві Оборони України, який запропонував:

засвідчити, що окремі результати проведених наукових досліджень Нестеренка Віктора Олександровича пов'язаних з супроводженням захищеної СЕДО-М використано Центром оперативних стандартів і методики підготовки Збройних Сил України під час:

перевірки функціональних можливостей окремого розділу оновленого спеціального програмного забезпечення захищеної СЕДО-М за методикою перевірки, яка розроблялась Нестеренко Віктором Олександровичем за окремими складовими, а саме:

здійснення реєстрації, надання відповідного позначення проектам військових публікацій та в подальшому розміщення в захищеному СЕДО-М затверджених (або введених в дію) військових публікацій (доктринальних документів, навчально-методичних матеріалів) з усіх сфер військової діяльності Генерального штабу та Збройних Сил України;

наповнення відповідного розділу бази даних військовими публікаціями в новій редакції, відповідно вимог наказу Генерального штабу Збройних Сил України від 26.12.2018 №460 "Про затвердження Тимчасового порядку оформлення військових публікацій у Збройних Силах України";

проведення попередньої оцінки розширення функціональних можливостей захищеної СЕДО-М за умов збереження цілісності функціональних підсистем і даних;

вивчення питань щодо порядку використання захищеної СЕДО-М, рівня технічних рішень та технологій, які застосовувались при розробці (модернізації) та її експлуатації, відповідність сучасному стану та тенденціям розвитку існуючих систем, можливості її подальшої модернізації, ресурсного забезпечення справності таїї технічної придатності під час експлуатації, утилізації, відповідність нормативно-технічної документації встановленим вимогам тощо.

ІІІ. ВИРІШИЛИ:

1. Цим протоколом засвідчити, що окремі результати проведених наукових досліджень Нестеренка В.О. пов'язаних з супроводженням захищеної СЕДО-М,в частині що стосується розміщення затверджених (або введених в дію) військових публікацій з усіх сфер військової діяльності Генерального штабу та Збройних Сил України використано Центром оперативних стандартів і методики підготовки Збройних Сил України;

2. Визнати доцільність запропонованих ним рекомендацій та пропозицій щодо захищеної СЕДО-М;

3. Підтвердити, що функціональні можливості захищеної СЕДО-М розширились шляхом часткового удосконалення та доопрацювання модернізованих компонентів окремого розділу спеціального програмного забезпечення (далі – СПЗ) для:

СПЗ "Організація документообігу – військових публікацій (доктринальних документів, навчально-методичних матеріалів) ";

СПЗ “Адміністрування – здійснення реєстрації, надання відповідного позначення проектам військових публікацій”;

СПЗ “Контроль статусу військової публікації – проєкт, апрбація, діяючий, дія призупинена тощо”;

СПЗ “Архів та оперативне зберігання – військових публікацій”.

4. Продовжити супроводження та наповнення розділу “Військові публікації Збройних Сил України” захищеної СЕДО-М відповідними військовими публікаціями в новій редакції.

Голова методичної ради	полковник	Олег БОЙКО
Члени методичної ради	полковник	Ярослав КОТЛЯРЕНКО
	полковник	Ярослав БІЛЕЦЬКИЙ
	полковник	Валентин ГРИЩУК
	підполковник	Олександр ЧЕРНИШОВ
Секретар	полковник	Олег ЧЕРНОВ

ДОДАТОК Д

ЗАТВЕРДЖУЮ
Тимчасово виконуючий обов'язки начальника Воєнно-наукового управління Генерального штабу Збройних Сил України полковник

Микола СЕНЬ

"19" 05 2020р.

АКТ
впровадження результатів
виконаної дослідно-конструкторської роботи

По ДКР шифр "СЕДО-М" – виконаної в період з 21.09.2012 по 16.06.2015 Центральним науково-дослідним інститутом Збройних Сил України та Науковим центром зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут.

Комісія в складі:

голова комісії – начальник відділу планування наукової роботи Воєнно-наукового управління Генерального штабу Збройних Сил України полковник ЛЕВІЩЕНКО Є. В.;

заступник голови комісії – головний спеціаліст відділу наукових експертиз Воєнно-наукового управління Генерального штабу Збройних Сил України полковник ЛАГНО Є. О.;

члени комісії:

начальник відділу розробки методик випробувань та оцінювання Воєнно-наукового управління Генерального штабу Збройних Сил України полковник РАМШОВ Д. В.;

старший офіцер відділення підтримки та супроводження програм Воєнно-наукового управління Генерального штабу Збройних Сил України полковник ГРЕЧКО М. М.;

старший офіцер відділу наукових експертиз Воєнно-наукового управління Генерального штабу Збройних Сил України полковник ПОСТАШ Д. О.,

встановила, що наукові положення, досліджені та розроблені особисто полковником НЕСТЕРЕНКО Віктором Олександровичем, зокрема:

організація формування єдиного захищеного інформаційного середовища електронних документів за рахунок підтримки основних процесів обробки документів органів військового управління, установ, військових частин Збройних Сил України та інших складових сил оборони держави;

удосконалено спеціальне програмне забезпечення захищеної СЕДО за умови збереження цілісності програмного та інформаційного забезпечення функціональних підсистем захищеної СЕДО, шляхом розширення їх функціональних можливостей;

порядок обробки інформації з обмеженим доступом у захищеній системі електронного документообігу;

визначено склад та технічні характеристики захищеної системи електронного документообігу.

Одержані результати відповідають сучасним тенденціям розвитку систем електронного міжвідомчого документообігу, а також технічним вимогам щодо порядку взаємодії між складовими сил оборони та органами державної влади.

Комісія постановила:

вважати результати дисертаційного дослідження, виконаними полковником НЕСТЕРЕНКО Віктором Олександровичем, начальником загального відділу Головного управління доктрин та підготовки Генерального штабу Збройних Сил України особистими, а саме:

сформовано теоретичні засади державної політики щодо створення, впровадження та функціонування системи електронного міжвідомчого документообігу сфери оборони;

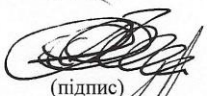
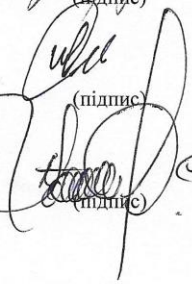
визначено порядок формування єдиного захищеного інформаційного середовища електронних документів в МО України, ГШ ЗС України та інших складових сектору оборони держави;

обґрунтовано напрями удосконалення системи електронного міжвідомчого документообігу сфери оборони в єдиному захищеному інформаційному середовищі електронних документів складових сектору оборони держави.

Пропозиції комісії:

використати результати дисертаційного дослідження, під час здійснення планування та проведення воєнно-наукових досліджень і робіт по обґрунтуванню, формуванню і реалізації оперативно-тактичних вимог (тактико-технічних), що пред'являються до перспективних систем електронного міжвідомчого документообігу сфери оборони у інформаційно-телекомунікаційних системах різного призначення та різного рівня складності, зразків озброєння та військової техніки, зразків, що модернізуються.

"18" 05 2020 р.

Голова комісії:	полковник (військове звання)	 (підпис)	Є. В. ЛЕВІЩЕНКО (прізвище)
Заступник голови комісії:	полковник (військове звання)	 (підпис)	Є. О. ЛАГНО (прізвище)
Члени комісії:	полковник (військове звання)	 (підпис)	Д. В. РАМШОВ (прізвище)
	полковник (військове звання)	 (підпис)	М. М. ГРЕЧКО (прізвище)
	полковник (військове звання)	 (підпис)	Д. О. ПОСТАШ (прізвище)

Онлайн сервіс створення та перевірки кваліфікованого та удосконаленого електронного підпису

ПРОТОКОЛ
створення та перевірки кваліфікованого та удосконаленого електронного підпису

Дата та час: 21:52:14 24.04.2026

Назва файлу з підписом: Діс_Нестеренко В.О__ОСТАТОЧ.pdf
Розмір файлу з підписом: 5.3 МБ

Перевірені файли:
Назва файлу без підпису: Діс_Нестеренко В.О__ОСТАТОЧ.pdf
Розмір файлу без підпису: 5.2 МБ

Результат перевірки підпису: Підпис створено та перевірено успішно. Цілісність даних підтверджено

Підписувач: НЕСТЕРЕНКО ВІКТОР ОЛЕКСАНДРОВИЧ
П.І.Б.: НЕСТЕРЕНКО ВІКТОР ОЛЕКСАНДРОВИЧ
Країна: Україна
РНОКПП: 2762519836
Організація (установа): ФІЗИЧНА ОСОБА
Час підпису (підтверджено кваліфікованою позначкою часу для підпису від Надавача): 21:52:12 24.04.2026
Сертифікат виданий: КНЕДП АЦСК АТ КБ "ПРИВАТБАНК"
Серійний номер: 5E984D526F82F38F0400000006DC540145A58107
Алгоритм підпису: ДСТУ 4145
Тип підпису: Удосконалений
Тип контейнера: Підписаний PDF-файл (PAdES)
Формат підпису: З повними даними для перевірки (PAdES-B-LT)
Сертифікат: Кваліфікований

Версія від: 2026.04.06 13:00