Cyber Resilience and Interoperability as Institutional Preconditions for Digital Transformation of Document Workflow in Ukraine's Defence Governance

UDC 351:614.2 DOI: https://doi.org/10.15421/152556

Sikalo Maksym
Ph.D., Doctoral Student, https://orcid.org/0000-0001-5949-5712, sikalomv@i.ua
V. N. Karazin Kharkiv National University (Kharkiv, Ukraine)

Abstract.
The article examines the digital transformation of document management in Ukraine's defense sector as a component of broader public governance reform during war. The relevance of the study is obusловлена the growing dependence of military command and administrative processes on digital systems, which must operate reliably in a high-risk cyber environment and ensure coordinated interaction between institutional actors. In this context, cyber resilience and interoperability are considered not as auxiliary technical features but as fundamental managerial conditions that determine the effectiveness, accountability, and scalability of digital document circulation within the Ministry of Defense of Ukraine and the Armed Forces of Ukraine.

The purpose of the article is to identify the managerial conditions under which electronic document management evolves from a set of fragmented IT solutions into an element of a controlled and sustainable institutional reform.

The results demonstrate that the maturity of digital document management should be assessed through three interrelated dimensions: cyber resilience, interoperability, and process efficiency. Particular attention is given to data quality, metadata standardization, unified registries and identifiers, access control mechanisms, continuity of services, and secure cross-domain exchange between classified and non-classified environments. The article proposes a managerial maturity framework that links technological solutions with institutional responsibility and measurable performance indicators.

The conclusions emphasize that the transition to a cyber-resilient and interoperable digital document system is a prerequisite for effective defense governance during wartime and a foundation for post-war modernization. Sustainable transformation requires institutionalized ownership of processes and data, unified standards, and a shift from isolated IT projects to a coherent policy of managed digital change.

Keywords: cyber resilience, interoperability, electronic document management, defence governance, digital transformation, data governance, military information systems, public administration reform

Кіберстійкість та інтероперабельність як управлінські умови цифрової трансформації документообігу у системі оборонного управління України

Сікало Максим
Харківський національний університет імені В. Н. Каразіна (Харків, Україна)

Анотація.
У статті досліджено цифрову трансформацію документообігу в оборонному секторі України як складову ширшої реформи публічного управління в умовах воєнного стану. Актуальність дослідження зумовлена зростаючою залежністю систем військового управління та адміністративних процесів від цифрових рішень, які мають функціонувати стабільно в умовах підвищених кіберризиків та забезпечувати узгоджену взаємодію між численними інституційними суб'єктами. У цьому контексті кіберстійкість та інтероперабельність розглядаються не як допоміжні технічні характеристики, а як базові управлінські умови, що визначають ефективність, підзвітність і масштабованість електронного документообігу в Міністерстві оборони України та Збройних Силах України.

Метою статті є визначення управлінських умов, за яких електронний документообіг переходить від фрагментарних IT-рішень до елементу керованої та стійкої інституційної реформи.

Отримані результати засвідчують, що зрілість цифрового діловодства доцільно оцінювати за трьома взаємопов'язаними вимірами: кіберстійкістю, інтероперабельністю та процесною ефективністю. Особливу увагу приділено якості даних, стандартизації метаданих, уніфікованим довідникам та ідентифікаторам, механізмам контролю доступу, забезпеченню безперервності сервісів і безпечному міждоменному обміну між класифікованими та некласифікованими середовищами. Запропоновано рамку управлінської зрілості, що поєднує технологічні рішення з інституційною відповідальністю та вимірюваними показниками результативності.

У висновках наголошено, що перехід до кіберстійкої та інтероперабельної системи електронного документообігу є передумовою підвищення ефективності оборонного управління під час війни та основою післявоєнної модернізації. Стійка трансформація потребує інституційного закріплення відповідальності за процеси й дані, уніфікації інформаційних стандартів та переходу від ізольованих IT-проєктів до цілісної політики керованих цифрових змін.

Ключові слова: кіберстійкість, інтероперабельність, електронний документообіг, оборонне управління, цифрова трансформація, управління даними, військові інформаційні системи, реформа публічного управління

Стаття надійшла / Article arrived: 18.02.26 // Схвалено до друку / Accepted: 19.03.26 // Підписано до друку / Approved for printing: 20.03.26

Вступ.

На сучасну військову діяльність все більше впливає не тільки кількість особового складу та ресурсів, а й здатність військових реагувати швидко, адаптивно та синхронно. У світлі всеосяжної агресії, спрямованої на Україну, стало очевидним, що ефективність оборонного сектору багато в чому безпосередньо залежить від ступеня інтеграції держави та Збройних Сил у цифрову сферу. Цифрова трансформація в публічному секторі інтерпретується як перехід від оцифрування окремих функцій до платформено-даних моделей управління.

Цифрова трансформація оборонного управління в Україні відбувається в контексті гібридної транзитивної цифрової державності, яка поєднує технократичні, демократичні та елементи контролю, формуючи складну конфігурацію впливів на управлінські процеси та цифрові інструменти (Сікало, 2025).

В цій конструкції ключовими стають інтероперабельність, управління даними та спроможність організацій до змін. У межах підходів цифрового урядування нової епохи цифрове військове діловодство слід розглядати не стільки як автоматизацію паперових процедур, скільки як перебудову системи управління (її стандартів, процесів, ролей, контролю та відповідальності) (Dunleavy et al., 2006; Breaking Defense, 2025).

У цьому контексті критичне значення набуває вивчення історичного досвіду, сучасного стану та перспектив розвитку електронного документообігу у Збройних Силах України. Аналіз цього виміру дозволяє не тільки оцінити ефективність поточних реформ, але й допомагає визначити основні проблеми, з якими має зіткнутися державне управління в оборонній сфері. Разом з тим, доцільно розглянути міжнародний досвід цифрової трансформації військових організацій, який може стати основою для подальших напрямків дій оборонного сектору України, який прагне до створення повністю реалізованої цифрової армії. У цьому зв'язку принципового значення набувають кіберстійкість, захист інформації та інтероперабельність, оскільки саме вони визначають здатність електронного документообігу забезпечувати безперервність управління, збереження чутливих даних і узгоджену взаємодію між інформаційними **системами в умовах війни.**

Актуальність тематики. Цифровізація, перехід до електронного документообігу має низку переваг. Це суттєво скорочує час проходження документів, підвищує дисципліну виконання, забезпечує трасованість рішень і підзвітність посадових осіб, знижує корупційні ризики та створює передумови для датоцентричного управління. Одночасно існують проблеми, пов'язані з нормативно-правовою сумісністю, кібербезпекою, захистом персональних даних, організаційною готовністю підрозділів, зміною управлінської культури, інтеграцією з національними реєстрами та досягненням інтероперабельності із стандартами партнерів. Отже, наукова експертиза цифрової трансформації процесів документації у Збройних Силах є доречною як для вдосконалення державної політики, так і для підвищення ефективності управління обороною у сценаріях воєнного часу. Кіберстійкість, захист інформації та інтероперабельність у цьому контексті постають не допоміжними технічними вимогами, а базовими управлінськими умовами ефективного функціонування цифрового документообігу, від яких залежить керованість, підзвітність і можливість подальшого масштабування цифрових рішень у ЗСУ. Вони є ключовими аспектами цифрового діловодства. Саме якість даних, наявність і стандартизація метаданих, уніфіковані довідники, стійкі ідентифікатори та формалізовані правила обміну визначають можливість переходу від фіксації «електронного документа» до управління на основі даних. У секторі оборони зазначені підходи мають реалізовуватися в єдності з вимогами кіберстійкості, зокрема контролем доступу, повнотою журналювання, забезпеченням безперервності сервісів і налагодженим реагуванням на інциденти, оскільки рівень довіри до електронного документообігу безпосередньо обумовлюється доступністю та захищеністю відповідних систем (Breaking Defense, 2025; Foreign Policy Research Institute, 2024).

Мета статті полягає у визначенні управлінських умов, за яких електронний документообіг у Міністерстві оборони України та Збройних Силах України перестає бути набором окремих сервісів і стає елементом керованої реформи. Йдеться про поєднання трьох вимірів: процесної трансформації та скорочення надлишкових процедур; управління даними й метаданими як основи підзвітності та контролю виконання; закладання кіберстійкості й інтероперабельності як обов'язкових обмежень і критеріїв масштабування. Додаткове завдання – запропонувати рамку оцінювання зрілості цифрового діловодства, придатну

для управлінської пріоритизації рішень та порівняння підрозділів за єдиними показниками.

Методологія дослідження. Дане дослідження виконано в межах підходів публічного управління та адміністративної реформи, де цифрову трансформацію військового діловодства розглянуто як зміну управлінських правил і практик, а не просто як модернізацію ІТ-засобів. Вихідною рамкою є системний і структурно-функціональний аналіз, що дає змогу трактувати документообіг як управлінську підсистему, яка визначає порядок ухвалення рішень, формує підзвітність і розподіл відповідальності через регламенти, ролі, дані, контроль і відповідну інфраструктуру.

Емпірична база сформована на основі аналізу відкритих джерел: нормативно-правових актів, стратегічних документів, офіційних повідомлень і публічних матеріалів щодо цифрових сервісів у ЗСУ та МОУ. Для виявлення ключових проблем та обмежень використано проблемно-цільовий підхід і елементи інституційного аналізу. Аналіз вітчизняних на міжнародних практик здійснено за критеріями регуляторної визначеності, інтероперабельності, кіберстійкості та зрілості процесів і даних. Узагальнення проведено через аналітичний синтез, висновки структуруються навколо управлінських пріоритетів і рамки зрілості, яка охоплює процесні, інформаційні та безпекові параметри.

Аналіз попередніх досліджень і публікацій. У наукових публікаціях останніх років, присвячених цифровій трансформації сектору безпеки і оборони, електронний документообіг дедалі рідше розглядається як ізольований технічний інструмент. У ряді сучасних досліджень спостерігається тенденція до розширеного тлумачення ефективності електронного документообігу - її дедалі частіше пов'язують не лише з технічними характеристиками, а передусім з організаційною готовністю. Зокрема, звертається увага на проблеми кіберстійкості, захисту даних та інтероперабельності, які у військовому секторі стають визначальними чинниками (Interfax-Ukraine, n.d.; DOU, n.d.). В той же час фокус виходить за рамки лише технічних засобів захисту, охоплюючи здатність організаційних структур підтримувати керованість, контроль доступу та відновлення функцій.

Окрема група досліджень присвячена інтероперабельності. У них аналізується, як міжнародний досвід - зокрема, стандарти союзників - впливає на здатність національних систем ефективно обмінюватися даними (CERT-UA, 2025; Foreign Policy Research Institute, 2024; Frantzman, 2021). Автори зазначають: інтероперабельність не можна зводити до технічної сумісності, адже мова йде і про організаційні узгодження, і про подолання міжвідомчої роз'єднаності (MediaSapiens, 2024, 2025).

У низці публікацій простежується прагнення до більш комплексного бачення цифрової трансформації, в межах якого документообіг поєднується з процесами управління персоналом, логістикою та управлінням даними (Boyd, 2017). Така парадигма дозволяє розглядати цифрові рішення як складову загальної системи управління, а не як допоміжний сервіс.

Узагальнення проаналізованих джерел дає підстави виокремити дві стійкі тематичні лінії: по-перше, визнання безпеки та кіберстійкості обов'язковими умовами функціонування цифрового документообігу у військових структурах (NATO, 2024; United Nations in Ukraine, n.d.); по-друге, орієнтацію на міжнародний досвід як методологічну основу для забезпечення інтероперабельності та розвитку управління на основі даних (Boyd, 2017; Mitnick, 2020; Frantzman, 2021; NATO, 2024; Foreign Policy Research Institute, 2024).

Водночас у наявних дослідженнях залишаються невирішеними низка управлінських питань. Зокрема, недостатньо розробленими є підходи до оцінювання зрілості цифрового документообігу, механізми управління змінами у військових організаціях, а також інструменти подолання нерівномірної інтероперабельності між інформаційними системами. У межах цієї статті зазначені прогалини уточнено шляхом поєднання оцінки зрілості документообігу з вимогами кіберстійкості та інтероперабельності, що дозволяє розглядати цифрову трансформацію документообігу як елемент системних змін у публічному управлінні оборонною сферою.

Результати дослідження.

Сучасний світ диктує свої умови – паперовий документообіг стрімко поступається електронному, який окрім смислового навантаження має бути належним чином оформлений та завірений. Україна не є виключенням. На сьогодні надійність та юридична сила електронних документів переважно гарантуються за допомогою використання електронного підпису. У 2017 році прийнятий Закон України «Про електронну ідентифікацію та електронні довірчі послуги» (Верховна Рада України, 2017), який включив європейські стандарти

(Регламент eIDAS) та запровадив концепцію кваліфікованого електронного підпису (КЕП) замість попереднього електронного підпису. Цей прогрес сприяв суттєвому підвищенню безпеки та надійності цифрових документів у державному секторі.

За цих умов подальший розвиток електронного документообігу в оборонному секторі потребує переходу від фрагментарних нормативних рішень до узгодженого стратегічного бачення цифрової трансформації. Саме стратегічний рівень дозволяє пов'язати правове регулювання, організаційні зміни та технологічні інструменти в єдину логіку розвитку. В рамках розвитку нормативно-правового забезпечення цифрової трансформації в армії очікується, що спеціальна Стратегія цифрової трансформації оборонного сектору, що спрямована на систематичне встановлення пріоритетів для оцифровки військових операцій у найближчі роки, отримає офіційне схвалення, а її проект буде сформульований у співпраці з Міністерством цифрової трансформації та міжнародними консультантами.

Стратегія спрямована на підвищення операційної ефективності, прозорості та стійкості шляхом всебічної цифровізації процесів, що охоплює ланцюги від поставок та системи закупівель (такі як DOT-Chain) до розвідувальних операцій та кіберзахисту, сприяючи інтеграції інноваційних технологій (включаючи штучний інтелект та GovTech) та сприяючи партнерству з навчальними закладами та бізнес-сектором для забезпечення технологічної переваги.

Критичні аспекти впровадження цифрового документообігу в ЗСУ. Попри очевидне розуміння важливості переходу до електронного документообігу в оборонному секторі, практична реалізація змін у Збройних Силах України супроводжується системними ризиками.

Найсуттєвіші обмеження цифровізації в оборонному секторі пов'язані з кіберстійкістю, яку слід розмежовувати з кібербезпекою у вузькому значенні. Кібербезпека орієнтована на запобігання інцидентам та зниження ймовірності несанкціонованого доступу. Кіберстійкість характеризує здатність системи зберігати працездатність критичних функцій під час атак, деградації мереж і часткових відмов. Вона також охоплює спроможність до відновлення у визначені строки після порушень.

Для високонавантажених цифрових сервісів, які концентрують чутливі дані та обслуговують значну кількість користувачів, типовими є загрози порушення доступності (відмови в обслуговуванні, DoS/DDoS), компрометації облікових записів, інсайдерських витоків і ризики ланцюга постачання програмного забезпечення.

Станом на 2012–2026 роки офіційної статистики кіберінцидентів, прямо пов'язаних із системами електронного документообігу ЗСУ, у відкритому доступі не виявлено. Натомість Міністерство оборони приділяє підвищену увагу захисту цифрового документообігу і впроваджує відповідні заходи кібербезпеки.

Так, застосунок «Армія+» розгорнуто на захищеній хмарній інфраструктурі, має атестат КСЗІ (комплексної системи захисту інформації) і підключений до системи моніторингу та реагування на кіберінциденти (Незалежний антикорупційний комітет з питань оборони, 2026).

У жовтні 2024 року в Міноборони було створено окремий Центр реагування на кіберінциденти. Головні завдання Центру – це реагування на кібератаки, усунення їх наслідків, кіберзахист інформаційно-комунікаційних систем МОУ, впровадження систем управління інцидентами та обмін інформацією про кіберзагрози (Gwara Media, 2025).

На загальнодержавному рівні Національний центр реагування CERT-UA фіксує тисячі кіберінцидентів щорічно (для прикладу, 3018 кіберінцидентів за перше півріччя 2025 р. по всіх секторах (CERT-UA, 2025), але окремої публічної вибірки по ЗСУ чи системах документообігу не надано. Натомість Міністерство оборони приділяє постійну увагу кіберзахисту цифрових ресурсів, відомство впроваджує найсучасніші вимоги кібербезпеки, якими керуються країни НАТО, у свої інформаційні системи (Interfax-Ukraine, 2025). Зокрема, Міноборони впровадило багатофакторну аутентифікацію для доступу до внутрішніх систем, сертифіковане шифрування каналів зв'язку, а також активно адаптує стандарти STANAG до обробки військових даних у системах «Дельта» та «Резерв+».

Війна оголила вразливість цифрових сервісів до перебоїв інфраструктури: удари по енергосистемі та зв'язку спричинили масові відключення інтернету, особливо в зоні бойових дій (Wikipedia contributors, n.d.). Попри це, сервіси на кшталт «Дії» зберігали працездатність, хоча окрему інформацію довелося тимчасово приховати з міркувань безпеки (Слово і Діло, 2024; Коментарі Україна, n.d.). У сфері військових операцій потенційні небезпеки значно посилюються через критичний характер

метаданих. Оперативне значення охоплює не тільки суть документів, але й частоту їх подання, характер комунікацій, визначені маршрути та тимчасові атрибути, пов'язані з їх транзитом.

В період 2022–2026 років Збройні Сили України форсовано впроваджували низку цифрових сервісів – від електронного обліку особового складу до мобільних застосунків для військових. Наведені приклади свідчать, що стрімкий запуск таких систем часто супроводжувався технічними збоями, перевантаженнями та помилками. Застосунки «Резерв+» та «Армія+» стали корисними інструментами для військовозобов'язаних і військовослужбовців, але їхній розвиток не був гладким: початкові релізи довелося екстрено доопрацьовувати. Типові причини проблем – надмірне навантаження на суміжні сервіси (BankID, державні реєстри) при різкому напливі користувачів, неповна підготовка даних (неактуальні реєстри, неінтегровані підрозділи) та людський фактор при тестуванні (помилкові дії команди розробки) (ТСН, n.d.; ITC.ua, n.d.).

Важливо, що реакція органів управління ЗСУ та Міноборони була оперативною і прозорою. Про збої негайно повідомлялося, користувачі отримували рекомендації про дії для мінімізації втрат часу (зберігати PDF-документи, почекати, оновити дані через альтернативний сервіс тощо) (Страшкулич, 2024; ТСН, n.d.). Одночасно IT--фахівці займаються виправленнями в режимі реального часу, як правило, відновлюючи функціональність протягом декількох годин. Таким чином, хоча швидке розгортання цифрових рішень у війську іноді призводило до збоїв, ці виклики послужили каталізатором системного вдосконалення. Як результат, сервісами розширювали функціонал, посилили стійкість (наприклад, шифрування даних та інтеграцію з іншими системами) (Верховна Рада України, 2017) та включили отримані уроки в наступні етапи цифровізації Збройних Сил.

З огляду на значущість кіберстійкості для цифрових сервісів, варто окремо зупинитися на типових інцидентах, що мали місце під час впровадження застосунків «Резерв+» та «Армія+», оскільки саме вони ілюструють найбільш поширені вразливості на практиці (наведено в табл.1).

Табл.1.

Основні кіберінциденти, пов'язані з електронним документообігом в ЗСУ

Дата	Суть інциденту	Орієнтовний термін вирішення проблеми
Жовтень 2024	помилка в відображенні відстрочок	день-в-день
Листопад 2024	перевантаження системи BankID	2 години
Листопад 2024	помилковий статус «в розшуку»	день-в-день
Грудень 2024	технічні проблеми при запуску	2 години
Лютий 2025	перевантаження системи BankID	4 години
Лютий 2025	втрата доступу до системи «Трембіта»	3 години
Вересень 2025	збій в обміні даними з реєстром	3 години

** створено за результатами власного дослідження та аналізу відкритих джерел*

Можна прослідкувати тенденцію зміни суті кіберінцидентів – від одиночних випадків до системних проблем з обміном між реєстрами та цифровими системами. Пріоритетом в сфері кіберзахисту на поточному етапі є налагодження швидкого стійкого обміну між реєстрами шляхом запровадження дублюючих каналів синхронізації, резервування точок обміну даними, уніфікації протоколів взаємодії на рівні метаданих і структур даних. Це дозволяє мінімізувати ризики втрати доступу до критичної інформації внаслідок точкових відмов або перевантаження суміжних систем, забезпечуючи безперервність обслуговування користувачів навіть за умов пікових навантажень або інцидентів у базових сервісах. Доцільним є впровадження асинхронної моделі обміну з реєстрами із буферизацією даних, що дозволить зберігати запити під час збою і передавати їх після відновлення зв'язку. Важливим є питання стандартизації інтерфейсів API між ключовими реєстрами та сервісами Міноборони, що має забезпечити їх моніторинг у реальному часі з автоматичним сповіщенням про збої.

За таких обставин вкрай важливим є запровадження механізмів реєстрації, принципів найменших привілеїв, багатофакторної аутентифікації, сегментації шляхів та регулярний аудит в якості основних інструментів в рамках нормативної бази та практики управління.

Крім того, кіберстійкість вимагає встановлення процедур безперервності. Вони охоплюють стратегії відновлення, визначені місця резервного копіювання, тестування сценаріїв аварійного перемикання та формулювання цілей відновлення для життєво важливих функцій робочого процесу, зокрема цільового часу відновлення та цільової точки відновлення даних.

Основною передумовою цифрової трансформації є сумісність, яка в практичному плані часто обмежується технічним зв'язком систем. У оборонному секторі це тягне за собою узгодженість даних, процесів та інтерпретації вмісту, що виходить за рамки простої сумісності форматів. Встановлення уніфікованих каталогів та ідентифікаторів, протоколів класифікації, профілів метаданих, протоколів обміну та заходів контролю якості даних під час передачі має першорядне значення. За відсутності цих компонентів інтеграція посилює ризики неточностей та надмірностей. Це призводить до генерації недостовірної управлінської інформації, особливо коли операційна ефективність є основною проблемою.

Додаткова проблема полягає у взаємодії між класифікованими та некласифікованими доменами. У таких умовах інтероперабельність слід забезпечувати через коректне розмежування доступів і застосування безпечних механізмів міждоменного обміну, а не через послаблення режимних вимог. Узгодження зі стандартами партнерів варто розглядати як довгострокову політику стандартизації даних і процесів. Така політика підвищує сумісність, підтримує масштабованість і посилює керованість екосистеми оборонних цифрових сервісів.

Додатково зберігається дисбаланс між заходами захисту та забезпеченням безперервності роботи цифрових сервісів у кризових режимах. Подальший розвиток доцільно орієнтувати на перехід від точкових рішень до керованої політики змін. Така політика має включати визначення власників процесів і даних, уніфікацію правил роботи з даними та запровадження вимірюваних параметрів результативності.

Першорядне значення мають формалізація власників процесів та продуктів, введення єдиного джерела правдивості документів та статусів, встановлення стандартів управління даними, створення кіберстійкої архітектури безперервності та впровадження взаємодії як принципу організації всієї цифрової екосистеми оборонного сектору. Саме в такій логіці СЕДО, «Армія+» і інститут цифрових офіцерів, що запроваджується, можуть перетворитися з простого набору інструментів у всеосяжний механізм реформи управління, здатний зменшити транзакційні витрати, підвищити підзвітність та забезпечити стійкість управління обороною в контексті війни та післявоєнної реконструкції.

Тенденції і перспективи розвитку цифрового документообігу у військовій сфері.

Однією з задач військового керівництва України є поширення електронного документообігу на всі рівні управління у Збройних Силах України – від центрального апарату до тактичної ланки. Однак цей підхід є життєздатним лише за умови, що інтероперабельність і кіберстійкість закладаються як базові принципи архітектури управління. Якщо їх розглядати як додаткові вимоги після впровадження, управлінський ефект буде обмеженим та мінімальним. У підсумку цифрова трансформація має перетворюватися з набору окремих рішень на стійку управлінську спроможність діяти швидко, узгоджено та підзвітно в умовах високих ризиків і обмежень зв’язку.

Підвищення кібербезпеки та стійкості системи має вирішальне значення. Перехід до електронного документообігу відбувається на тлі триваючої кібер- та повномасштабної війни з боку росії. Тому значна увага - як зараз, так і в майбутньому - спрямована на безпеку цифрових систем. Експерти застерігають, що поспішне оцифрування потоку військових документів у воєнний час створює ризики порушення персональних даних для військовослужбовців та викриття інформації безпеки військ, оскільки російські хакери, безсумнівно, спробують проникнути в цифрові сервіси Збройних Сил (Суспільне Новини, n.d.). Усвідомлюючи цю надзвичайну загрозу, Україна запроваджує багаторівневий механізм захисту: робочі процеси військових електронних документів працюють у захищених мережах, які використовують сертифіковані корінні криптографічні рішення; основні дані реєстру, такі як Єдиний реєстр військових зобов'язань, підлягають дублюванню та резервуванню для зменшення ризиків кібервторгнення. Застосування технології блокчейн для захисту особливо чутливих транзакцій (тим самим запобігаючи несанкціонованому втручанню або саботажу в цифрові замовлення) є перспективним шляхом (U.S. Department of Defense, 2019). DOT-Chain Defence є прикладом цифрової платформи МОУ, побудованої з елементами цифрового реєстру й логістики, які можуть бути потенційно

реалізовані з використанням розподілених технологій (Незалежний антикорупційний комітет з питань оборони, 2026). Проактивне залучення України до ініціатив НАТО з кіберзахисту сприятиме прийняттю оптимальних практик безпеки. Зрештою, еволюція робочих процесів цифрових документів узгоджується з розвитком кіберпідрозділів у Збройних Силах, з прагненням створити спеціальні сили кіберзахисту, завданням яких є захист як військової ІТ-інфраструктури, так і ширшої цифрової структури країни.

Міжвідомча та міжнародна інтеграція є ключовою сферою уваги. Мета виходить за рамки простої внутрішньої автоматизації Міністерства оборони, охоплюючи консолідацію інформаційних мереж серед усіх військових гілок та союзних держав. Наразі ініційована електронна співпраця між Міністерством оборони, МВС, Міністерством у справах ветеранів та іншими відповідними суб'єктами для обміну даними військовослужбовців (відповідно до ініціативи Єдиного реєстру захисників). У найближчому майбутньому планується розробка єдиної цифрової платформи для сектору безпеки та оборони, яка охоплює Збройні Сили, Державну прикордонну охорону, Національну гвардію, Службу безпеки України (СБУ) та інші організації. Ця ініціатива дозволить автоматизувати процес передачі документації під час перепризначення військовослужбовців, синхронізувати записи про жертви та травми та покращити логістичну координацію. Метою є задача спростити координацію спільних дій, прискорити обмін розвідувальною інформацією та забезпечити технічну сумісність із Digital Backbone Альянсу (NATO, 2024).

Для перевірки реалістичності таких очікувань варто зіставляти українські підходи з практиками цифровізації у збройних силах держав, які мають підтверджені результати в цій сфері (насамперед окремі країни НАТО, США, Ізраїль, Естонія). Висновки, отримані з міжнародного досвіду, вказують на те, що, незважаючи на різницю в масштабах та контекстуальних умовах, всі зразкові випадки оцифрування у військовому управлінні мають спільні характеристики, а саме: наявність політичної волі та стратегічного спрямування з боку вищих органів влади, інвестиції в основну інфраструктуру, розвиток персоналу, трансформація когнітивних рамок і забезпечення кібербезпеки та сумісності. Україна, розпочавши свій шлях під час війни, ефективно інтегрує досвід НАТО, США, Ізраїлю та Естонії, прагнучи прискорити досягнення сучасних стандартів. Українські військові вже використовують низку цифрових рішень (такі як «Армія+» та «Дельта»), які недоступні деяким її союзникам. Це свідчить про значний прогрес, але також підкреслює необхідність постійного навчання на провідних прикладах та адаптації їх методології до наших обставин (Boyd, 2017; Frantzman, 2021; Foreign Policy Research Institute, 2024; Mitnick, 2020; NATO, 2024).

У прагненні до всебічної оцифровки робочих процесів військових документів різні виклики та бар'єри вимагають зосередження уваги державного управління. Визначено потенційні стратегії вирішення цих проблем:

- стійкість до трансформації та людський вимір;
- взаємодія з міжнародними партнерами;
- кібербезпека та захист конфіденційності.

Стійкість до трансформації та людський вимір. Як і будь-яка суттєва ініціатива реформ, оцифрування стикається з системною інерцією, характерною для усталених практик. Старше покоління звикло користуватися фізичною документацією, при цьому дехто проявляє скептицизм до нових технологічних досягнень. Досвід військової цифрової трансформації Ізраїлю підтверджує, що головною перешкодою є необхідність трансформації управлінського мислення вищого командного складу на користь цифрових підходів (Mitnick, 2020).

Успішне подолання таких бар’єрів вимагає не лише змін у мисленні, а й впровадження системного інструментарію для управління цифровими змінами. Для підвищення керованості трансформації рамка зрілості може бути структурована у трьох блоках: кіберстійкість, інтероперабельність і процесна ефективність. Блок кіберстійкості має відображати здатність сервісів документообігу підтримувати функціональність під час інцидентів і відмов, а також відновлювати роботу у визначені терміни та з допустимим рівнем втрати даних. Оцінювання кіберстійкості повинна ґрунтуватися на доступності ключових функцій і цільових параметрах відновлення. Він також повинен охоплювати результати планових тестів відновлення та показників реагування на інциденти, включаючи час виявлення та час усунення. Окремо слід враховувати зрілість управління доступом, повноту журналювання та сегментацію контурів інтеграції. В умовах деградації зв’язку важливим індикатором є наявність режимів роботи з обмеженою мережею, зокрема офлайн-режиму або відкладеної синхронізації.

Показники інтероперабельності відображають здатність інформаційних систем і організаційних ланок обмінюватися документами та метаданими без спотворення змісту і без надлишкового введення даних. Змістовий компонент обміну включає, зокрема, класифікацію, статус документа, підставу, виконавця та інші атрибути процесу. Інтероперабельність розкривається за чотирма рівнями: технічним, синтаксичним, семантичним та організаційно-процесним. На технічному рівні ключовими є стабільні канали інтеграції та стандартизовані програмні інтерфейси або інтеграційна шина (шина обміну даними/повідомленнями) як інфраструктура взаємодії систем. На синтаксичному рівні визначальними є узгоджені формати документів і структур даних, наявність схем та правил валідації, а також керування версіями інтеграційних контрактів. На семантичному рівні критичними стають узгоджені довідники, класифікатори, профілі метаданих, унікальні ідентифікатори сутностей і правила зіставлення значень. На організаційно-процесному рівні інтероперабельність забезпечується регламентами взаємодії, угодами про рівень сервісу, матрицями відповідальності, правилами ескалації та визначенням власників даних і відповідальних за їх якість. В данному випадку доцільним буде використання методології оцінки, що ґрунтується на взаємодоповнюваних інструментах управління процесами та ризиками. З цією роллю справляється комплексна модель оцінювання, що поєднує аналіз ризиків, вимог користувачів, структуру процесів і безперервне вдосконалення на основі контрольованих метрик, що має стати сполучною ланкою між аналітикою та управлінням (Kovalenko et al., 2025).

З точки зору розуміння використання цифрових сервісів МОУ корисним є аналіз динаміки активних користувачів та обсягів звернень та операцій в застосунках «Резерв» та «Армія+».

Цифровий сервіс «Резерв+» офіційно запущено 18 травня 2024 року. Уже до 12 липня 2024 року в застосунку оновили свої дані 2,7 мільйона українців (близько 90–100 тис. осіб оновлювали дані щодня) (Незалежний антикорупційний комітет з питань оборони, 2026; MediaSapiens, 2025). Цей стрибок був пов'язаний із вимогою закону про мобілізацію щодо уточнення облікових даних протягом 60 днів.

Сервіс «Армія+» презентовано 8 серпня 2024 року. Менш ніж за тиждень після старту авторизувалися понад 50 тисяч військових. Це свідчить про значний початковий інтерес серед особового складу. За кілька днів було подано перші 250 електронних рапортів через застосунок (Бізнес Цензор, 2025; Черногоренко, 2024). Ключові функції застосунків «Резерв+» та «Армія+» та їхні характеристики наведено в табл.2.

Табл.2.

Основні функції та навантаження сервісів «Резерв+» та «Армія+»

Функція	Кількість звернень та операцій
уточнення особистих даних	2,7 млн оновлень, щоденний потік запитів більше 1 млн запитів на добу
оформлення відстрочки	понад 333 тисячі відстрочок від мобілізації станом на травень 2025
електронний військовий документ	понад 4 млн власників ЕВД станом на липень 2025 року
інтеграція з ВЛК	200 тис направлень станом на червень 2025 року
рекрутинг в ЗСУ	понад 100 тисяч заявок станом на середину 2025 року
подача стандартних рапортів	Більше 1,2 мільйона станом на грудень 2025 року
подача рапортів на переведення	Понад 55 тисяч рапортів станом на грудень 2025 року

** створено за результатами власного дослідження та аналізу відкритих джерел*

Узагальнена динаміка кількості користувачів «Резерв+» та «Армія+» за ключовими датами наведено на рис. 1.

Для аналізу рівня інтероперабельності варто розглянути кейси запуску застосунків, які були запущені МОУ. Так, в серпні 2024 року було презентовано застосунок «Армія+» для військовослужбовців ЗСУ, і вже в перший тиждень роботи виявилися проблеми з авторизацією деяких користувачів. Близько 60 тисяч військових успішно зареєструвалися за тиждень, проте багато хто не зміг створити обліковий запис – система не знаходила їхніх даних. Більшість проблем з авторизацією було вирішено: Міноборони запевнило, що поступово цифровізація охопить усі силові структури, і всі військові з часом отримають доступ до «Армія+» (Черногоренко, 2024).

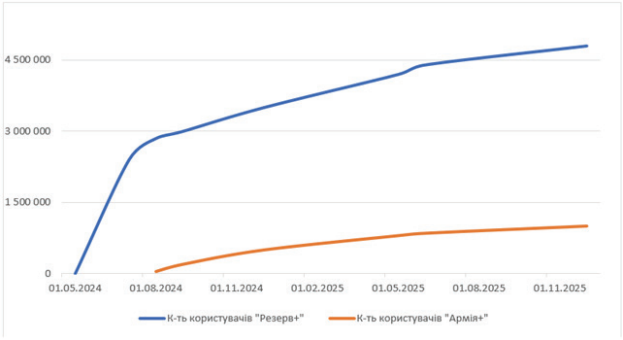

Рис. 1. Динаміка кількості активних користувачів застосунків «Резерв» та «Армія+»
** створено за результатами власного дослідження та аналізу відкритих джерел*

Для аналізу рівня інтероперабельності варто розглянути кейси запуску застосунків, які були запущені МОУ. Так, в серпні 2024 року було презентовано застосунок «Армія+» для військовослужбовців ЗСУ, і вже в перший тиждень роботи виявилися проблеми з авторизацією деяких користувачів. Близько 60 тисяч військових успішно зареєструвалися за тиждень, проте багато хто не зміг створити обліковий запис – система не знаходила їхніх даних. Більшість проблем з авторизацією було вирішено: Міноборони запевнило, що поступово цифровізація охопить усі силові структури, і всі військові з часом отримають доступ до «Армія+» (Черногоренко, 2024).

У грудні 2024 року після початкового етапу впровадження «Армія+» додав нові функції, зокрема можливість подати рапорт на переведення між військовими частинами онлайн. Проте одразу виявилися технічні проблеми: багато військових отримували відмову в додатку при спробі подати такий рапорт. В якості тимчасового вирішення було запропоновано гарячу лінію Єдиного центру рекрутингу ССО (Сікало, 2025).

Таким чином, досвід із «Армія+» також показав, що прискорений запуск цифрового інструменту без повного наповнення і перевірки даних призводить до збоїв і тимчасового зниження ефективності. На старті сервіс довелося обмежити лише частиною особового складу та покладатися на актуальність даних у реєстрах, які не встигли оновити належним чином. У випадку з новою функцією переведень, довелося терміново вносити зміни в бекенд-систему (довідники військових частин) і паралельно забезпечити альтернативний канал (телефон гарячої лінії) для підтримки військових (Черногоренко, 2024; Сікало, 2025).

Рівень інтероперабельності інформаційних систем у ЗСУ є критично важливим показником успішної цифровізації. За останні роки проводиться активна робота над об'єднанням розрізнених реєстрів і баз даних Міністерства оборони та Генерального штабу в єдиний інформаційний простір. Офіційного кількісного рейтингу рівня інтероперабельності не оприлюднено, але низка ініціатив демонструє значний прогрес у цій сфері.

Єдина система обліку особового складу «Імпульс», розгорнута у 2025 році, описується як фундамент для майбутньої цифрової екосистеми оборони. «Імпульс» забезпечує інтеграцію з іншими ключовими продуктами, як то «Армія+», із системою електронного документообігу, з Медичною інформаційною системою ЗСУ. Фактично це є створенням єдиного інформаційного середовища, де всі процеси взаємопов'язані і ґрунтуються на єдиному достовірному джерелі даних, що дозволяє прискорити роботу всіх служб (Interfax-Ukraine, 2025).

Єдиний державний реєстр призовників, військовозобов'язаних та резервістів «Оберіг» створено відповідно до закону 2017 року, а формально запущено у березні 2022 року. Він є спільним інструментом для військкоматів (ТЦК та СП), Генерального штабу і Міністерства оборони. За законом, Міністерство оборони є володільцем реєстру, а Генштаб ЗСУ – одним із розпорядників (нарівні зі СБУ та Службою зовнішньої розвідки). Тобто і МОУ, і ГШ мають прямий доступ до даних цього реєстру, що саме по собі забезпечує інтеграцію їхніх інформаційних потреб. Дані автоматично оновлюються шляхом обміну з багатьма національними реєстрами (РАЦС, Міграційна служба, Податкова, МОЗ, МОН тощо) через систему взаємодії «Трембіта». Модернізація «Оберігу» в 2023 році (за підтримки проєкту EU4DigitalUA) була спрямована на покращення інтероперабельності – налагоджено обмін даними з ключовими державними базами, що дозволило верифікувати близько 88% даних реєстру та додати 750 тис. записів. Таким чином, ступінь інтеграції між військовими реєстрами і зовнішніми базами значно підвищився: наприклад, виключено випадки подвійного вручення повісток або неактуальних даних про призовників (DOU, n.d.).

Важливо, що всі нові цифрові рішення впроваджуються у тісній координації між Міністерством оборони та Генштабом. Наприклад, при переході на електронний журнал обліку особового складу наказом №* було передбачено перехідний період до

1 вересня 2025 року, протягом якого Головне управління персоналу ГШ ЗСУ спільно з Директоратом цифрової трансформації МОУ збирають пропозиції від військових частин і аналізують виявлені проблеми з веденням нового електронного реєстру (Бізнес Цензор, 2025). Це свідчить про оцінювання та відстеження рівня інтеграції і взаємодії систем на практиці, з метою їх подальшого вдосконалення.

Окремо виділяється група показників процесної ефективності, яка характеризує швидкість та якість проходження документів і навантаження на персонал. До неї належать час повного циклу проходження документа від створення до завершення, час погодження та підпису (з урахуванням типових і граничних значень), частка ручних операцій і повторного введення даних, частота повернень на доопрацювання, пропускна здатність (кількість документів за період), а також простої та "черги" між етапами. Така трикомпонентна структура рамки зрілості дозволяє уникати методологічної помилки, коли зростання швидкості документообігу помилково ототожнюється зі зростанням кіберстійкості або сумісності систем: зрілість у цьому підході трактується як збалансований прогрес одночасно в кіберстійкості, інтероперабельності та процесній ефективності, що робить оцінювання більш доказовим і придатним для управлінських рішень та пріоритизації заходів.

Обидва цифрові сервіси МОУ – «Резерв+» для цивільних військовозобов'язаних і «Армія+» для військових – успішно набули багатомільйонної аудиторії за короткий час, суттєво спростивши взаємодію громадян і військовослужбовців з оборонним відомством. Статистика свідчить про мільйони проведених операцій: від оновлення даних і отримання відстрочок до подачі рапортів і електронних документів. Попри окремі технічні збої (здебільшого викликані кібератаками або високим навантаженням), команди Міноборони оперативно реагували і відновлювали роботу сервісів.

У Збройних Силах України швидкість документообігу традиційно визначалася часом проходження службових документів через всі необхідні інстанції. Офіційних публічних метричних показників саме швидкості обробки документів у відкритих джерелах не знайдено. Проте з 2012 по 2026 роки в ЗСУ відбувалася поступова цифровізація діловодства, яка мала на меті прискорити й спростити документообіг.

Так, при запуску мобільного застосунку «Армія+» за перші два місяці роботи (серпень–жовтень 2024) було подано понад 10 000 електронних рапортів саме через застосунок, кількість е-рапортів зростала щодня на 150–200 (Міністерство оборони України, 2025, n.d.). Наказом №* в 2024 році Міністерство оборони скоротило 12 паперових журналів обліку особового складу до одного електронного журналу (Бізнес Цензор, 2025). В 2025 році у ЗСУ розгорнуто першу централізовану цифрову систему персонального обліку «Імпульс», яка мала стати ядром цифрової екосистеми оборони, що система автоматизує створення документів (наказів, довідок, звітів) та формує узгоджену звітність, що усуває дублювання даних (Interfax-Ukraine, n.d.).

Взаємодія з міжнародними партнерами, зокрема через двосторонні домовленості щодо підтримки цифрових проєктів (Незалежний антикорупційний комітет з питань оборони, 2026), є важливим чинником прискорення цифрових змін. Окремого опрацювання потребує адаптація сервісів до умов бойових дій, розвиток мобільних клієнтських компонентів із підтримкою офлайн-функціонування та відкладеної синхронізації після відновлення зв'язку. Для мінімізації втрат інформації в разі нестабільного підключення слід передбачати захищені засоби локального зберігання з контрольованим доступом. Критичні дані мають резервуватися географічно віддалено, поза зонами активних бойових дій, із визначеними регламентами відновлення. За відкритими даними, така практика вже застосовується через віддалені центри обробки даних (АрміяInform, 2024).

Кібербезпека та захист конфіденційності є ключовими передумовами довіри до електронного документообігу. Електронні системи оборонного управління є привабливими цілями для противника, зокрема з мотивів отримання інформації або порушення роботи управлінських контурів (Суспільне Новини, n.d.). Паралельно зберігаються внутрішні ризики, пов'язані з несанкціонованим доступом і витоками. Тому потрібні чіткі правила доступу, журналювання дій і дисципліна виконання процедур на всіх рівнях. Курс дій зрозумілий: уряд повинен забезпечити сертифікацію та аудит безпеки всіх розгорнутих рішень. Наразі Міністерство оборони тісно співпрацює зі Службою безпеки України з цього питання. Наразі в Україні триває створення Єдиного державного реєстру військовослужбовців як інформаційно-комунікаційної системи, що передбачає міжвідомчу електронну інформаційну

взаємодію з іншими державними реєстрами та системами в рамках цифрового урядування й узгодження облікових даних відповідно до чинного законодавства (Бізнес Цензор, 2025; Департамент цифрової трансформації Харківської міської ради, n.d.). Обов'язково потрібно продовжити розробку фірмових криптографічних інструментів (витіснити російське програмне забезпечення, яке історично було вбудоване в системи). Регулярне навчання персоналу з кібербезпеки має вирішальне значення: воно включає недопущення відкриття або запуску вкладень і файлів із неперевірених джерел, а також утримання від використання персональних платформ для офіційного обміну інформацією (відомчими актами прямо заборонено використання незахищених програм обміну повідомленнями для передачі офіційної інформації) (Черногоренко, 2024). На урядовому рівні повинні бути сформульовані плани надзвичайних ситуацій у разі успішної кібератаки. Наприклад, розробка стратегії переходу на резервні системи та аналогові паперові процедури в критичні моменти (папір як резерв на крайній випадок). Фактично, йдеться про підвищення стійкості - система має витримати окремі збої чи атаки і швидко відновитися. Для цього в Міноборони створюється система кібероборони, підпорядковані структурі кіберсил фахівці моніторять мережі МОУ і ЗСУ, перешкоджають вторгненню та реагують на інциденти.

Висновки.

Цифрова трансформація військового документообігу в Україні вже не є допоміжною автоматизацією внутрішніх процедур. В умовах повномасштабної війни вона прямо впливає на керованість оборонного управління: скорочує цикл проходження управлінських рішень, підсилює дисципліну виконання, підвищує трасованість дій і робить підзвітність посадових осіб більш предметною. Водночас управлінський ефект знижується там, де цифровізація відтворює паперову логіку без перегляду маршрутизації та вимог: надлишкові погодження, дублювання операцій і паралельне ведення паперових та електронних контурів зберігають бюрократичне навантаження, а в окремих випадках навіть посилюють його через подвійний облік і розмитість правил. У ряді підрозділів зберігається практика дублювання – електронні документи роздруковуються для підпису або архівування, а маршрутизація залишається паперовою. Поширена й протилежна практика, коли документи роздруковуються, підписуються, відправляються засобами СЕДО, а потім ще раз роздруковуються та направляються за належністю. Це не лише ускладнює контроль виконання, а й розмиває відповідальність через паралельні контури погодження.

Ключовим обмеженням масштабування електронного діловодства в оборонному секторі є не тільки та не стільки темп розгортання сервісів, скільки здатність систем працювати у режимі підвищених ризиків і нестабільної інфраструктури. Для ЗСУ це означає, що кіберстійкість має бути задана як обов’язкова управлінська умова функціонування документообігу: критичним є збереження працездатності основних функцій під час інцидентів, деградації мережі та пікових навантажень, а також відновлення у визначені строки. На тактичному рівні питання доступності набуває практичного виміру через нестабільний зв’язок, тому архітектурно й організаційно необхідні режими роботи з обмеженою мережею, локальне збереження та відкладена синхронізація, інакше електронні процедури втрачають надійність саме в ті моменти, коли вони найбільш потрібні.

Інтероперабельність, у свою чергу, не зводиться до технічної інтеграції систем. У військовому управлінні вона означає узгодженість даних, метаданих і процедур, наявність уніфікованих довідників та ідентифікаторів, зрозумілих правил обміну й контролю якості даних під час передачі. За відсутності цих передумов інтеграція породжує дублювання, неточності та суперечності у статусах документів та виконавських ланцюгах, що спотворює управлінську інформацію та підриває довіру до цифрових схем. Особлива увага повинна бути спрямована на взаємодію між класифікованими та некласифікованими доменами: інтероперабельність за таких умов повинна бути забезпечена відповідним розмежуванням доступу та безпечними механізмами міждоменного обміну, а не спрощенням режимних вимог.

Прогрес цифрової трансформації доцільно оцінювати не стільки за кількістю сервісів чи швидкістю документообігу, скільки за їх стійкістю, інтегрованістю та ефективністю в управлінні. Практичну цінність має підхід, що оцінює зрілість цифрового діловодства через три взаємопов’язані виміри: кіберстійкість, інтероперабельність і процесну ефективність. Така рамка допомагає відрізняти реальне прискорення управлінських процесів, технічну та організаційну сумісність, а також здатність сервісів до відновлення у кризових умовах. Вона

дає змогу перейти від загальних декларацій до вимірюваних управлінських рішень і чіткої пріоритизації заходів.

У стратегічній перспективі завершення переходу до керованого, кіберстійкого та інтероперабельного електронного документообігу є передумовою підвищення ефективності оборонного управління під час війни й основою для післявоєнної модернізації військової організації. Це потребує інституційного закріплення відповідальності за процеси та дані, уніфікації правил роботи з інформацією, а також переходу від точкових ІТ-рішень до керованої політики змін, яка має чіткі метрики, власників і механізми контролю виконання.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

АрміяInform. (2024, August 21). *Як з'явилася «Армія+» і що буде з додатком далі: Інтерв'ю.* https://armyinform.com.ua/2024/08/21/yak-zyavylasya-armiya-i-shho-bude-z-dodatkom-dali-intervyu-armiyainform-z-katerynoyu-chernogorenko/

АрміяInform. (2024, December 17). *У Міністерстві оборони розповіли про кількість користувачів «Армія+» та нові можливості переведень.* https://armyinform.com.ua/2024/12/17/u-ministerstvi-oborony-rozpovily-pro-500-tysyach-korystuvachiv-armiya-ta-pro-novi-mozhlyvosti-pereveden/

АрміяInform. (2024, December 21). *Скільки користувачів щоденно користуються застосунком «Резерв+»: Відповідь від Міноборони*. https://armyinform.com.ua/2024/12/21/skilky-korystuvachiv-shhodenno-korystuyutsya-zastosunkom-rezerv-vidpovid-vid-minoborony/

АрміяInform. (2024, December 4*). Міноборони: 12 паперових журналів та книг обліку особового складу скоротили до одного*. https://armyinform.com.ua/2024/12/04/minoborony-12-paperovyh-zhurnaliv-ta-knyg-obliku-osobovogo-skladu-skorotyly-do-odnogo/

АрміяInform. (2024, November 20). *Єдиний реєстр військовослужбовців: У Міноборони пояснили переваги.* https://armyinform.com.ua/2024/11/20/yedynyj-reyestr-vijskovosluzhbovcziv-u-minoborony-poyasnyly-perevagy/?utm_source=chatgpt.com

Бізнес Цензор. (2025). *Актуальні додатки в Україні: Новини 2025 року*. https://censor.net/biz/tag/5997/dodatok

Верховна Рада України. (2017, October 5). *Про електронну ідентифікацію та електронні довірчі послуги (Закон № 2155-VIII).* https://zakon.rada.gov.ua/laws/show/2155-19#Text

Верховна Рада України. (n.d.). *Про створення та функціонування Єдиного державного реєстру військовослужбовців (Закон № 4497-20)*. https://zakon.rada.gov.ua/laws/show/4497-20

Департамент цифрової трансформації Харківської міської ради. (n.d.). *Досягнення.* https://digital.kharkivrada.gov.ua/dosyagnennya (дата звернення: 12.08.2025).

Коментарі Україна. (n.d.). *Збій у «Резерв+»: Що знову пішло не так*. https://society.comments.ua/ua/news/human-rights/zbiy-u-zastosunku-rezerv-scho-znovu-pishlo-ne-tak-747266.html

Міністерство оборони України. (2025, July 7*). Україна запускає DOT-Chain Defence – цифрову систему для швидкого постачання озброєння*. https://mod.gov.ua/news/ukrayina-zapuskaye-dot-chain-defence-czifrovu-sistemu-dlya-shvidkogo-postachannya-ozbroyennya?utm_source=chatgpt.com

Міністерство оборони України. (2025, October 9). *Міністерства оборони України та Німеччини домовились про довгострокове партнерство у сфері цифровізації*. https://mod.gov.ua/news/ministerstva-oboroni-ukraini-ta-nimechchini-domovilis-pro-dovgostrokove-partnerstvo-u-sferi-cifrovizacii

Міністерство оборони України. (n.d.). *В Армія+ подано 10 000 рапортів*. https://mod.gov.ua/news/v-armiya-podano-10-000-raportiv-pidsumki-dvoh-misyacziv-roboti

Міністерство оборони України. (n.d.). *Мобільний застосунок Резерв+.* https://mod.gov.ua/news/minoboroni-zapuskae-mobilnij-zastosunok-rezerv-dlya-vijskovozobovyazanih-prizovnikiv-ta-rezervistiv

Міністерство оборони України. (n.d.). *Як виправити дані та авторизуватись в застосунку «Армія+».* https://aplus.mod.gov.ua/recover

Незалежний антикорупційний комітет з питань оборони. (2026, January 1). *"Defence Talks": Як відбувається цифровізація оборонного сектора (під час війни)*. https://nako.org.ua/events/defence-talks-yak-vidbuvajetsya-cifrovizaciya-oboronnogo-sektoru-pid-cas-viini

РБК-Україна. (n.d.). *«Резерв+» не працює 19 грудня – стався збій*. https://www.rbc.ua/rus/news/rezerv-stavsya-masshtabniy-zbiy-1734600377.html

РБК-Україна. (n.d.). *Переведення військових через додаток «Армія»: У ССО заявили про технічні проблеми*. https://www.rbc.ua/rus/news/sso-povidomili-tehnichni-problemi-perevedennyam-1733812831.html

Сікало, М. (2025). Методологічні виклики дослідження цифрової трансформації публічного управління: Від інструментальності до субстанційності технологій, концепція транзитивної цифрової державності. *Державне управління: удосконалення та розвиток,* (9). http://doi.org/10.32702/2307-2156.2025.9.13

Сікало, М. (2025). Цифрова трансформація в публічному управлінні Харківщини: Транзитивна модель та практичний досвід. *Інвестиції: практика та досвід,* (18), 243–252. https:// doi.org/10.32702/2306-6814.2025.18.243

Слово і Діло. (2024, December 19). *У застосунку «Резерв+» зафіксували збій*. https://www.slovoidilo.ua/2024/12/19/novyna/suspilstvo/zastosunku-rezerv-zafiksuvaly-zbij

Слово і Діло. (2025, February 8). *У застосунку «Резерв+» стався збій: Пояснення Міноборони.*https://www.slovoidilo.ua/2025/02/08/novyna/suspilstvo/zastosunku-rezerv-stavsya-zbij-poyasnennya-minoborony

Страшкулич, А. (2024, August 12). *Українська паперова армія: Як Міноборони намагається цифровізувати військо. Українська правда*. https://www.pravda.com.ua/longread/2024/08/12/7469836/

Суспільне Новини. (n.d.). *«Резерв+»: У застосунку стався збій, роботу відновлено*. https://suspilne.media/1121616-u-zastosunku-rezerv-stavsa-zbij-so-vidomo/

Суспільне Новини. (n.d.). *Міноборони: Застосунок «Резерв+» зараз налічує майже 4,5 млн користувачів*. https://suspilne.media/1042995-zastosunok-rezerv-vze-nalicue-majze-45-mln-koristuvaciv-cernogorenko/

Суспільне Новини. (n.d.). *У «Резерв+» стався збій – Міноборони*. https://suspilne.media/871135-u-rezerv-stavsa-zbij-minoboroni/

ТСН. (n.d.). *Застосунок «Армія+»: Скільки військових встигли авторизуватись*. https://tsn.ua/ukrayina/u-minoboroni-rozpovili-skilki-viyskovih-proyshli-avtorizaciyu-u-zastosunku-armiya-2639820.html

ТСН. (n.d.). *Помилка у застосунку «Армія+»: У Міноборони пояснили, що робити.* https://tsn.ua/ukrayina/pomilka-v-zastosunku-armiya-minoboroni-nadalo-instrukciyu-yak-vipraviti-2642049.html

Черногоренко, К. (2024, August 15). *Через «Армія+» вже подали 1100 електронних рапортів. Міністерство оборони України.* https://mod.gov.ua/news/cherez-armiya-vzhe-podali-1100-elektronnih-raportiv

Boyd, A. (2017, May 11). *Enterprise view: How Army HQ is going paperless in under a year.* Federal Times. https://www.federaltimes.com/it-networks/2017/05/11/enterprise-view-how-army-hq-is-going-paperless-in-under-a-year/

Breaking Defense. (2025, January 29). *Blockchain, big data and genAI: US Army uses novel tech to track billions in Ukraine aid*. https://breakingdefense.com/2025/01/blockchain-big-data-and-genai-us-army-uses-novel-tech-to-track-billions-in-ukraine-aid/?utm_source=chatgpt.com

CERT-UA. (2025). *Аналітичний звіт CERT-UA*. Держспецзв'язку. https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua

DOU. (n.d.). *Реєстр військовозобов'язаних "Оберіг": Як працює і які містить дані*. https://dou.ua/lenta/articles/electronic-register-oberig/

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). Digital era governance: IT corporations, the state, and e-government. *Journal of Public Administration Research and Theory*, 16(3), 467–494

European Commission. (2017). *European interoperability framework – Implementation strategy*. Publications Office of the European Union.

Foreign Policy Research Institute. (2024, October). https://www.fpri.org/article/2024/10/inside-estonias-defense-tech-ecosystem/

Frantzman, S. (2021, July 23). *Israel pushes military digital transformation in the age of "artificial intelligence war."* C4ISRNet. https://www.c4isrnet.com/it-networks/2021/07/23/israel-pushes-military-digital-transformation-in-the-age-of-artificial-intelligence-war/

Gwara Media. (2025). *Міноборони створили Центр реагування на кіберінциденти*. https://gwaramedia.com/minoborony-stvoryly-tsentr-reahuvannia-na-kiberintsydenty/

Interfax-Ukraine. (2025). Нову цифрову систему обліку військовослужбовців "Імпульс" розгортають у ЗСУ – Міноборони. https://interfax.com.ua/news/general/1112088.html

Interfax-Ukraine. (n.d.). *В «Армія+» уже понад 1 млн користувачів, Міноборони запускає новий етап розвитку застосунку*. https://interfax.com.ua/news/general/1126767.html

ITC.ua. (n.d.). *«Резерв+» помилково записав у розшук понад 700 тис. українців: Застосунок чекає трансформація*. https://itc.ua/ua/novini/rezerv-pomylkovo-zapysav-u-rozshuk-ponad-700-tys-ukrayintsiv-zastosunok-chekaye-transformatsiya-z-avtomatychnym-vzyattyam-na-vijskovyj-oblik/

Kovalenko, M., Sikalo, M., Kovalova, T., Radchenko, O., Velychko, L., Nakisko, O., Grybko, O., Maistro, S., & Ryzhikova, N. (2025). Development of an integrated quality management model in the context of digital transformation: public administration, education, economy. *Technology Audit and Production Reserves*, *6*(4(86), 46–61. https://doi.org/10.15587/2706-5448.2025.348540

LB.ua. (2024, September 11). За місяць у «Армія+» зареєструвались майже 200 тисяч користувачів. https://lb.ua/society/2024/09/11/634287_misyats_armiya_zareiestruvalis.html

MediaSapiens. (2024, July 12). *Дані в застосунку «Резерв+» оновили вже 2,7 мільйона українців.* https://ms.detector.media/withoutsection/post/35525/2024-07-12-dani-v-zastosunku-rezerv-onovyly-vzhe-27-milyona-ukraintsiv/

MediaSapiens. (2024, November 11*). За два дні онлайн-відстрочку в «Резерв+» отримали 40 тисяч громадян*. https://ms.detector.media/internet/post/36681/2024-11-11-za-dva-dni-onlayn-vidstrochku-v-rezerv-otrymaly-40-tysyach-gromadyan/

MediaSapiens. (2025, May 18). *Кількість користувачів «Резерв+» перевищила 4 мільйони*. https://ms.detector.media/internet/post/37953/2025-05-18-kilkist-korystuvachiv-rezerv-perevyshchyla-4-milyony/

Mitnick, J. (2020, February 8). *Here's how the Israeli army is embracing digital transformation. CIO*. https://www.cio.com/article/193993/heres-how-the-israeli-army-is-embracing-digital-transformation.html

NATO. (2024, October 17). *NATO's digital transformation implementation strategy*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy

Organisation for Economic Co-operation and Development. (2014). *Recommendation of the Council on Digital Government Strategies*. OECD Publishing.

U.S. Department of Defense. (2019, January 2). *DoD Instruction 8170.01: Online information management and electronic messaging* (Change 1, August 24, 2021).https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Personnel_Related/22-F-0350_DODI_8170.01-_Online_Information_Management_and_Electronic_Messaging_2Jan2019_CH-1_24Aug2021.pdf

United Nations in Ukraine. (n.d.). *Attacks on Ukraine's energy infrastructure: Harm to the civilian population.* https://ukraine.un.org/en/278992-attacks-ukraine%E2%80%99s-energy-infrastructure-harm-civilian-population

Wikipedia contributors. (n.d.). *Backup site*. Wikipedia. https://en.wikipedia.org/wiki/Backup_site?utm_source=chatgpt.com

Wikipedia contributors. (n.d.). *IT disaster recovery*. Wikipedia. https://en.wikipedia.org/wiki/IT_disaster_recovery?utm_source=chatgpt.com

REFERENCES

ArmyInform. (2024, August 21). How Army+ was created and what comes next: Interview. https://armyinform.com.ua/2024/08/21/yak-zyavylasya-armiya-i-shho-bude-z-dodatkom-dali-intervyu-armiyainform-z-katerynoyu-chernogorenko/

ArmyInform. (2024, December 17). The Ministry of Defense reported the number of Army+ users and new transfer options. https://armyinform.com.ua/2024/12/17/u-ministerstvi-oborony-rozpovily-pro-500-tysyach-korystuvachiv-armiya-ta-pro-novi-mozhlyvosti-pereveden/

ArmyInform. (2024, December 21). Daily number of Reserve+ users: Response from the Ministry of Defense. https://armyinform.com.ua/2024/12/21/skilky-korystuvachiv-shhodenno-korystuyutsya-zastosunkom-rezerv-vidpovid-vid-minoborony/

ArmyInform. (2024, December 4). Ministry of Defense: 12 paper logs and personnel record books were reduced to one. https://armyinform.com.ua/2024/12/04/minoborony-12-paperovyh-zhurnaliv-ta-knyg-obliku-osobovogo-skladu-skorotyly-do-odnogo/

ArmyInform. (2024, November 20). Unified register of military personnel: The Ministry of Defense explained the advantages. https://armyinform.com.ua/2024/11/20/yedynyj-reyestr-vijskovosluzhbovcziv-u-minoborony-poyasnyly-perevagy/

Boyd, A. (2017, May 11). Enterprise view: How Army HQ is going paperless in under a year. *Federal Times.* https://www.federaltimes.com/it-networks/2017/05/11/enterprise-view-how-army-hq-is-going-paperless-in-under-a-year/

Breaking Defense. (2025, January 29). Blockchain, big data and genAI: US Army uses novel tech to track billions in Ukraine aid. https://breakingdefense.com/2025/01/blockchain-big-data-and-genai-us-army-uses-novel-tech-to-track-billions-in-ukraine-aid/

Business Censor. (2025). Current applications in Ukraine: 2025 news. https://censor.net/biz/tag/5997/dodatok

CERT-UA. (2025). CERT-UA analytical report. State Service of Special Communications and Information Protection of Ukraine. https://cip.gov.ua/ua/news/intensivnist-fishingovikh-atak-zrosla-ale-lyudi-stali-bilsh-obiznanimi-v-pitannyakh-kibergigiyeni-analitichnii-zvit-cert-ua

Chernogorenko, K. (2024, August 15). *1,100 electronic reports have already been submitted via Army+.* Ministry of Defense of Ukraine. https://mod.gov.ua/news/cherez-armiya-vzhe-podali-1100-elektronnih-raportiv

Department of Digital Transformation of Kharkiv City Council. (n.d.). Achievements. https://digital.kharkivrada.gov.ua/dosyagnennya

DOU. (n.d.). "Oberih" register of persons liable for military service: How it works and what data it contains. https://dou.ua/lenta/articles/electronic-register-oberig/

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). Digital era governance: IT corporations, the state, and e-government. *Journal of Public Administration Research and Theory*, 16(3), 467–494.

European Commission. (2017). European interoperability framework – Implementation strategy. Publications Office of the European Union.

Foreign Policy Research Institute. (2024, October). Inside Estonia's defense-tech ecosystem. https://www.fpri.org/article/2024/10/inside-estonias-defense-tech-ecosystem/

Frantzman, S. (2021, July 23). *Israel pushes military digital transformation in the age of "artificial intelligence war."* C4ISRNet. https://www.c4isrnet.com/it-networks/2021/07/23/israel-pushes-military-digital-transformation-in-the-age-of-artificial-intelligence-war/

Gwara Media. (2025). The Ministry of Defense established a Cyber Incident Response Center. https://gwaramedia.com/minoborony-stvoryly-tsentr-reahuvannia-na-kiberintsydenty/

Independent Anti-Corruption Committee on Defense. (2026, January 1). "Defence Talks": How the digitalization of the defense sector is taking place (during wartime). https://nako.org.ua/events/defence-talks-yak-vidbuvajetsya-cifrovizaciya-oboronnogo-sektoru-pid-cas-viini

Interfax-Ukraine. (2025). A new digital system for accounting military personnel ("Impulse") is being deployed in the Armed Forces of Ukraine – Ministry of Defense. https://interfax.com.ua/news/general/1112088.html

Interfax-Ukraine. (n.d.). Army+ has surpassed 1 million users; the Ministry of Defense launches a new stage of application development. https://interfax.com.ua/news/general/1126767.html

ITC.ua. (n.d.). Reserve+ mistakenly marked more than 700,000 Ukrainians as wanted: The application is to undergo transformation. https://itc.ua/ua/novini/rezerv-pomylkovo-zapysav-u-rozshuk-ponad-700-tys-ukrayintsiv-zastosunok-chekaye-transformatsiya-z-avtomatychnym-vzyattyam-na-vijskovyj-oblik/

Komentari Ukraina. (n.d.). Reserve+ outage: What went wrong again? https://society.comments.ua/ua/news/human-rights/zbiy-u-zastosunku-rezerv-scho-znovu-pishlo-ne-tak-747266.html

Kovalenko, M., Sikalo, M., Kovalova, T., Radchenko, O., Velychko, L., Nakisko, O., Grybko, O., Maistro, S., & Ryzhikova, N. (2025). Development of an integrated quality management model in the context of digital transformation: Public administration, education, economics. *Technology Audit and Production Reserves*, 6(4(86)), 46–61. https://doi.org/10.15587/2706-5448.2025.348540

LB.ua. (2024, September 11). Almost 200,000 users registered in Army+ within a month. https://lb.ua/society/2024/09/11/634287_misyats_armiya_zareiestruvalis.html

MediaSapiens. (2024, July 12). Data in the Reserve+ application were updated by 2.7 million Ukrainians. https://ms.detector.media/withoutsection/post/35525/2024-07-12-dani-v-zastosunku-rezerv-onovyly-vzhe-27-milyona-ukraintsiv/

MediaSapiens. (2024, November 11). In two days, 40,000 citizens received online deferment in Reserve+. https://ms.detector.media/internet/post/36681/2024-11-11-za-dva-dni-onlayn-vidstrochku-v-rezerv-otrymaly-40-tysyach-gromadyan/

MediaSapiens. (2025, May 18). The number of Reserve+ users exceeded 4 million. https://ms.detector.media/internet/post/37953/2025-05-18-kilkist-korystuvachiv-rezerv-perevyshchyla-4-milyony/

Ministry of Defense of Ukraine. (2025, July 7). Ukraine launches DOT-Chain Defence–a digital system for rapid weapons supply. https://mod.gov.ua/news/ukrayina-zapuskaye-dot-chain-defence-czifrovu-sistemu-dlya-shvidkogo-postachannya-ozbroyennya

Ministry of Defense of Ukraine. (2025, October 9). The Ministries of Defense of Ukraine and Germany agreed on a long-term partnership in digitalization. https://mod.gov.ua/news/ministerstva-oboroni-ukraini-ta-nimechchini-domovilis-pro-dovgostrokove-partnerstvo-u-sferi-cifrovizacii

Ministry of Defense of Ukraine. (n.d.). 10,000 reports submitted in Army+. https://mod.gov.ua/news/v-armiya-podano-10-000-raportiv-pidsumki-dvoh-misyacziv-roboti

Ministry of Defense of Ukraine. (n.d.). How to correct data and authorize in the Army+ application. https://aplus.mod.gov.ua/recover

Ministry of Defense of Ukraine. (n.d.). Reserve+ mobile application. https://mod.gov.ua/news/minoboroni-zapuskae-mobilnij-zastosunok-rezerv-dlya-vijskovozobovyazanih-prizovnikiv-ta-rezervistiv

Mitnick, J. (2020, February 8). *Here's how the Israeli army is embracing digital transformation.* CIO. https://www.cio.com/article/193993/heres-how-the-israeli-army-is-embracing-digital-transformation.html

NATO. (2024, October 17). NATO's digital transformation implementation strategy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/10/17/natos-digital-transformation-implementation-strategy

Organisation for Economic Co-operation and Development. (2014). Recommendation of the Council on Digital Government Strategies. OECD Publishing.

RBC-Ukraine. (n.d.). Military transfers via the Army application: Special Operations Forces reported technical issues. https://www.rbc.ua/rus/news/sso-povidomili-tehnichni-problemi-perevedennyam-1733812831.html

RBC-Ukraine. (n.d.). Reserve+ did not work on December 19–an outage occurred. https://www.rbc.ua/rus/news/rezerv-stavsya-masshtabniy-zbiy-1734600377.html

Sikalo, M. (2025a). Methodological challenges in studying digital transformation of public administration: From instrumentality to substantiality of technologies and the concept of transitive digital statehood. *Public Administration: Improvement and Development*, (9). https://doi.org/10.32702/2307-2156.2025.9.13

Sikalo, M. (2025b). Digital transformation in public administration of Kharkiv region: Transitive model and practical experience. *Investments: Practice and Experience*, (18), 243–252. https://doi.org/10.32702/2306-6814.2025.18.243

Slovo i Dilo. (2024, December 19). An outage was recorded in the Reserve+ application. https://www.slovoidilo.ua/2024/12/19/novyna/suspilstvo/zastosunku-rezerv-zafiksuvaly-zbij

Slovo i Dilo. (2025, February 8). Reserve+ outage: The Ministry of Defense provided an explanation. https://www.slovoidilo.ua/2025/02/08/novyna/suspilstvo/zastosunku-rezerv-stavsya-zbij-poyasnennya-minoborony

Strashkulich, A. (2024, August 12). Ukraine's paper army: How the Ministry of Defense is trying to digitalize the military. *Ukrainska Pravda*. https://www.pravda.com.ua/longread/2024/08/12/7469836/

Suspilne News. (n.d.). An outage occurred in Reserve+–Ministry of Defense. https://suspilne.media/871135-u-rezerv-stavsa-zbij-minoboroni/

Suspilne News. (n.d.). Ministry of Defense: The Reserve+ application currently has nearly 4.5 million users. https://suspilne.media/1042995-zastosunok-rezerv-vze-nalicue-majze-45-mln-koristuvaciv-cernogorenko/

Suspilne News. (n.d.). Reserve+: An outage occurred in the application; the service has been restored. https://suspilne.media/1121616-u-zastosunku-rezerv-stavsa-zbij-so-vidomo/

TSN. (n.d.). Army+ application: How many service members have authorized. https://tsn.ua/ukrayina/u-minoboroni-rozpovili-skilki-viyskovih-proyshli-avtorizaciyu-u-zastosunku-armiya-2639820.html

TSN. (n.d.). Error in the Army+ application: The Ministry of Defense explained what to do. https://tsn.ua/ukrayina/pomilka-v-zastosunku-armiya-minoboroni-nadalo-instrukciyu-yak-vipraviti-2642049.html

U.S. Department of Defense. (2019, January 2). DoD Instruction 8170.01: Online information management and electronic messaging (Change 1, August 24, 2021). https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Personnel_Related/22-F-0350_DODI_8170.01-_Online_Information_Management_and_Electronic_Messaging_2Jan2019_CH-1_24Aug2021.pdf

United Nations in Ukraine. (n.d.). Attacks on Ukraine's energy infrastructure: Harm to the civilian population. https://ukraine.un.org/en/278992-attacks-ukraine%E2%80%99s-energy-infrastructure-harm-civilian-population

Verkhovna Rada of Ukraine. (2017, October 5). On electronic identification and electronic trust services (Law No. 2155-VIII). https://zakon.rada.gov.ua/laws/show/2155-19#Text

Verkhovna Rada of Ukraine. (n.d.). On the establishment and functioning of the Unified State Register of Military Personnel (Law No. 4497-20). https://zakon.rada.gov.ua/laws/show/4497-20

Wikipedia contributors. (n.d.). Backup site. Wikipedia. https://en.wikipedia.org/wiki/Backup_site

Wikipedia contributors. (n.d.). IT disaster recovery. Wikipedia. https://en.wikipedia.org/wiki/IT_disaster_recovery