Нормативне регулювання супроводження експлуатації інформаційних систем військового призначення: проблеми та шляхи вдосконалення

Regulatory framework for the military information systems support and operation: problems and ways of improvement

Андрій Дядечко
Corresponding author: доктор філософії, начальник науково-дослідного відділу проблем супроводження експлуатації інформаційних систем, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

Галина Руденська
старший науковий співробітник науково-дослідного відділу проблем супроводження експлуатації інформаційних систем, e-mail: rudenska85@ukr.net, ORCID: 0000-0002-4719-3765

Національний університет оборони України, м. Київ, Україна

Andrii Diadechko
Corresponding author: PhD, Head of the Research Department on Information Systems Support and Operation Issues, e-mail: andrewvvs@gmail.com, ORCID: 0000-0003-0191-8326

Galyna Rudenska
Senior Researcher of Research Department on Information Systems Support and Operation Issues, e-mail: rudenska85@ukr.net, ORCID: 0000-0002-4719-3765

National Defense University of Ukraine, Kyiv, Ukraine

Received: April 11, 2025 | Revised: April 23, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.7

Мета роботи: є аналіз проблем нормативного регулювання супроводження експлуатації інформаційних систем військового призначення та обґрунтування необхідності створення узагальненого військового стандарту, який би забезпечив ефективну організацію та управління цими процесами.

Метод дослідження: методи системного аналізу, порівняльного аналізу нормативно-правових документів, а також експертні оцінки ефективності чинного регулювання.

Результати дослідження: визначено ключові проблеми нормативного регулювання супроводження експлуатації інформаційних систем військового призначення, серед яких: фрагментарність нормативної бази, невідповідність сучасним технологічним викликам, відсутність єдиних стандартів безпеки та управління життєвим циклом інформаційних систем. Обґрунтовано необхідність розробки військового стандарту, який би встановлював єдині вимоги до супроводження експлуатації таких систем.

Теоретична цінність дослідження: стаття доповнює наукову базу щодо нормативного забезпечення супроводження експлуатації інформаційних систем військового призначення, пропонуючи системний підхід до їхнього регулювання. Розроблені концептуальні підходи можуть бути використані для формування методологічних основ військових стандартів у цій сфері.

Практична цінність дослідження: результати дослідження можуть бути використані при розробці та вдосконаленні нормативних документів, які регламентують супроводження експлуатації інформаційних систем в оборонному секторі. Запропоновані рішення сприятимуть підвищенню ефективності та безпеки функціонування інформаційних систем військового призначення.

Цінність дослідження: наукова новизна дослідження полягає у комплексному аналізі проблем нормативного забезпечення супроводження експлуатації інформаційних систем військового призначення та обґрунтуванні необхідності створення військового стандарту. Вперше пропонується системний підхід до розробки єдиного нормативного документа, що забезпечить уніфіковане та ефективне управління процесами супроводження експлуатації інформаційних систем в оборонному секторі.

Тип статті: теоретичний з практичними рекомендаціями.

Purpose: is to analyze regulatory challenges in maintaining and operating military information systems and justify the need for a unified military standard to ensure effective organization and management.

Method: system analysis, comparative analysis of regulatory documents, and expert assessments of current regulation effectiveness.

Research results: Key regulatory challenges in maintaining and operating military information systems have been identified, including fragmented regulations, misalignment with modern technological challenges, and the lack of unified security and lifecycle management standards. The need for a military standard establishing uniform requirements for these processes is substantiated.

Theoretical implications: The article contributes to the scientific foundation of regulatory support for maintaining and operating military information systems by proposing a systematic approach to their regulation. The developed conceptual approaches can be used to establish the methodological basis for military standards in this field.

Practical implications: The research findings can be used in the development and improvement of regulatory documents governing the maintenance and operation of information systems in the defense sector. The proposed solutions will enhance the efficiency and security of military information systems.

Originality / Value: The scientific novelty of the study lies in the comprehensive analysis of regulatory challenges in maintaining and operating military information systems and the justification for the creation of a military standard. For the first time, a systematic approach is proposed for developing a unified regulatory document that will ensure standardized and effective management of information system maintenance processes in the defense sector.

Type of article: theoretical with practical recommendations.

Ключові слова: інформаційні системи, супроводження експлуатації, нормативне регулювання, військовий стандарт.

Key words: information systems, operation support, normative regulation, military standard.

Вступ

Супроводження експлуатації інформаційних систем (далі – ІС) військового призначення є невід'ємною складовою їх життєвого циклу, що забезпечує стабільне функціонування, належний рівень інформаційної безпеки, а також своєчасну адаптацію до змін оперативно-тактичних умов. Ефективне управління процесами супроводження потребує наявності чіткої нормативно-правової бази, яка встановлювала б уніфіковані вимоги до організації, моніторингу, модернізації, технічної підтримки та інформаційного захисту таких систем.

Попри наявність окремих нормативних документів, що регламентують специфічні аспекти супроводження ІС, наразі відсутній єдиний інтегрований військовий стандарт, який би системно охоплював усі етапи та компоненти цього процесу. Існуюче нормативне забезпечення має фрагментарний характер, не повною мірою враховує сучасні технологічні виклики, зокрема зростаючу складність архітектури ІС, динамічність бойового середовища та загрозу кібернетичних атак, а також не забезпечує узгодженості дій між усіма суб'єктами супроводу.

Відсутність інтегрованого підходу ускладнює координацію між підрозділами, відповідальними за технічне обслуговування, оновлення програмного забезпечення, контроль безпеки та експлуатаційну підтримку. Це, своєю чергою, може призводити до зниження ефективності функціонування ІС, зростання операційних ризиків, зниження готовності систем до роботи в умовах бойових дій.

Метою цієї статті є ідентифікація ключових проблем нормативного забезпечення супроводження експлуатації ІС військового призначення та обґрунтування доцільності розробки уніфікованого військового стандарту, який би забезпечував систематизацію, стандартизацію та ефективне регламентування процесів супроводження з урахуванням специфіки сучасного гібридного та інформаційного протиборства.

Теоретичні основи дослідження

Аналіз чинних нормативних документів [1–39] засвідчив, що нормативне регулювання супроводження експлуатації ІС військового призначення охоплює сукупність стандартів, інструкцій, регламентів і методичних рекомендацій, які визначають вимоги до функціонування, безпеки, модернізації та технічної підтримки таких систем. Основною метою відповідного регулювання є забезпечення стабільної експлуатації ІС, підвищення ефективності їх застосування у військових операціях, а також мінімізація ризиків, пов'язаних з їх використанням в умовах бойових дій.

Нормативні акти, що регламентують супроводження ІС, умовно поділяються на чотири основні категорії:

міжнародні стандарти з управління життєвим циклом ІС;

стандарти з інформаційної безпеки;

стандарти НАТО;

національні нормативні документи (ДСТУ, керівні документи Міністерства оборони України тощо).

Попри наявність зазначених документів, у сфері супроводження експлуатації ІС військового призначення досі відсутній єдиний комплексний нормативний акт, який би системно регламентував усі аспекти супроводження протягом життєвого циклу ІС.

Досвід країн-членів НАТО демонструє ефективність функціонування військових ІС на основі чітких стандартів. Зокрема:

- **AAP-20** *NATO Programme Management Framework (NATO Life Cycle Model)* визначає етапи життєвого циклу військових систем, включаючи експлуатацію, супроводження,

оцінювання технічного стану, обґрунтування модернізації або виведення з експлуатації;

- **STANAG 4728** *System Life Cycle Management* формулює рамкові положення щодо управління життєвим циклом ІС, забезпечуючи їх надійність, адаптивність та відповідність вимогам НАТО;
- **AAP-48** *NATO System Life Cycle Processes* описує процеси, необхідні для підтримання працездатності ІС, включаючи технічне обслуговування, оновлення та модернізацію, а також процедури внесення змін з метою відповідності новим вимогам і технологіям.

У більшості країн-членів Альянсу запроваджено уніфіковані стандарти супроводження, що забезпечують взаємосумісність, узгодженість процесів і оперативну готовність ІС в оборонному секторі.

Аналіз наукової літератури свідчить про розробку окремих підходів до нормативного забезпечення супроводження експлуатації ІС військового призначення. Зокрема:

у [40] досліджено адміністративно-правові засади використання та розвитку інформаційних технологій в умовах воєнного стану, підкреслено важливість адаптації нормативної бази до нових викликів інформаційного простору;

у [41] розглянуто моделі та процеси життєвого циклу ІС управління оборонними ресурсами, з акцентом на виборі оптимальної моделі для ефективного супроводження;

у [42] проаналізовано підходи до розробки спеціалізованого програмного забезпечення для ІС військового призначення з урахуванням вимог до їх нормативної сумісності та функціональної специфіки;

у [43] висвітлено організаційні аспекти інформаційно-аналітичної підтримки проектів розроблення, впровадження та супроводження ІС, з акцентом на необхідності нормативного регламентування процесів управління життєвим циклом;

у [44] представлено сучасні методи організації технологічної підтримки інформаційної інфраструктури Міністерства оборони України, де наголошено на ролі кібербезпеки й інформаційного захисту у виконанні оборонних завдань.

Запропоновані в цих наукових працях концепції можуть бути використані як методологічна основа для розроблення уніфікованого військового стандарту супроводження експлуатації ІС, що сприятиме підвищенню надійності, стійкості та оперативної ефективності систем у Збройних Силах України.

Постановка проблеми

В умовах стрімкого розвитку цифрових технологій, ускладнення кіберзагроз і зростання вимог до оперативного управління оборонними ресурсами, питання ефективного нормативного регулювання процесів супроводження експлуатації ІС військового призначення набуває особливої актуальності.

Аналіз чинної нормативної бази у сфері супроводження ІС дозволяє виокремити низку системних проблем, які суттєво ускладнюють організацію цього процесу:

- **фрагментарність нормативного забезпечення**, що проявляється у відсутності єдиного комплексного документа, який би охоплював усі аспекти супроводження ІС протягом їх життєвого циклу; наявні нормативні акти регламентують лише окремі елементи, не забезпечуючи цілісного підходу;
- **невідповідність сучасним технологічним викликам** – чинні нормативні документи не враховують специфіку використання новітніх технологій, зокрема хмарних обчислень, штучного інтелекту, аналітики великих даних (Big Data) та комплексних систем кіберзахисту;
- **недостатня гармонізація національних стандартів з міжнародними** – існує розрив між національними нормативами та положеннями ключових документів НАТО, таких як

AAP-20, AAP-48, STANAG 4728, що ускладнює сумісну діяльність у рамках багатонаціональних оборонних програм;

- **відсутність уніфікованих вимог до технічного обслуговування, оновлення та модернізації ІС** – чинні нормативи не містять чітко визначених процедур супроводження програмного забезпечення, управління життєвим циклом ІС, а також реагування на технічні збої й несправності;
- **недостатня увага до аспектів кібербезпеки у процесі супроводження** – відсутні комплексні нормативні вимоги щодо оцінки кіберризиків, управління вразливостями, впровадження заходів інформаційного захисту та оперативного реагування на кіберінциденти в процесі експлуатації ІС.

З огляду на вищезазначене, виникає об'єктивна необхідність розроблення єдиного військового стандарту, який би нормативно врегулював ключові аспекти супроводження експлуатації ІС військового призначення з урахуванням міжнародного досвіду та сучасних технологічних викликів.

У процесі аналізу існуючих нормативно-правових актів встановлено, що на сьогодні супроводження експлуатації ІС регламентується значною кількістю розрізнених документів, які охоплюють лише окремі етапи або функціональні напрямки. Відсутність систематизованого підходу до реалізації супровідних заходів ускладнює організацію та управління відповідними процесами, що негативно впливає на загальну ефективність експлуатації ІС.

Таким чином, актуальним є:

узагальнення нормативних положень щодо організації та виконання заходів супроводження;

систематизація відповідних процесів супроводу;

інтеграція вимог чинних нормативних актів в єдиний комплексний документ, який регламентуватиме повний спектр заходів супроводження експлуатації ІС військового призначення.

Розробка такого документа дозволить створити уніфіковану нормативну основу для забезпечення ефективного, безпечного та технологічно адаптивного функціонування інформаційних систем у Збройних Силах України.

Методологія дослідження

У статті розглядаються нормативно-правові та організаційно-методичні аспекти супроводження експлуатації ІС військового призначення в Україні. Здійснено аналіз чинних національних нормативних актів, які регламентують відповідні процеси, а також міжнародних стандартів та стандартів НАТО, що можуть бути використані як основа для удосконалення нормативного регулювання у вітчизняній оборонній сфері.

Для проведення дослідження використано такі джерела інформації:

- нормативно-правові акти України, які регламентують супроводження експлуатації ІС;
- міжнародні стандарти *ISO/IEC/IEEE* та стандарти НАТО, що визначають підходи до управління життєвим циклом військових ІС;
- наукові публікації, аналітичні матеріали та експертні огляди, присвячені питанням нормативного забезпечення супроводження ІС;
- результати експертного аналізу сучасних тенденцій і кращих практик у сфері військової інформатизації.

Методологічну основу дослідження становлять такі підходи:

- **системний аналіз**, що застосовується для виявлення ключових недоліків у чинному нормативному регулюванні супроводження експлуатації ІС;
- **порівняльний аналіз**, який дозволяє зіставити національні підходи з міжнародними та стандартами НАТО з метою виявлення прогалин і визначення напрямів удосконалення

нормативної бази;

- **контент-аналіз нормативних документів**, спрямований на оцінку відповідності чинного регулювання сучасним технологічним викликам;
- **метод прогнозування**, який використовується для обґрунтування доцільності розроблення уніфікованого військового стандарту супроводження експлуатації ІС та оцінки його потенційного впливу на ефективність функціонування ІС у сфері оборони.

Дослідження сфокусоване виключно на етапі експлуатації ІС, без розгляду інших фаз життєвого циклу, таких як проєктування, розробка чи виведення з експлуатації. Крім того, аналіз обмежено відкритими офіційними нормативними документами та публічними науковими джерелами, без використання конфіденційної або засекреченої інформації з оборонного сектору.

Результати

Відсутність єдиного нормативного документа, який комплексно регламентує процес супроводження експлуатації ІС військового призначення, ускладнює забезпечення їхньої безперервної, надійної та ефективної роботи в умовах сучасних загроз і технологічних викликів. Існуючі в Україні нормативно-правові акти та технічні стандарти охоплюють лише окремі аспекти цього процесу, що призводить до фрагментації підходів і створює додаткові труднощі у практичному впровадженні заходів експлуатаційної підтримки.

З метою обґрунтування оптимального підходу до нормативного регулювання супроводження експлуатації ІС здійснено аналіз чинної нормативної бази України, міжнародних стандартів управління життєвим циклом ІС, а також відповідних документів НАТО і провідних країн-партнерів. Дослідження охоплювало ключові положення, що стосуються організації експлуатаційної підтримки, управління конфігурацією, технічного обслуговування, забезпечення інформаційної безпеки та удосконалення функціональних характеристик систем у процесі їхньої експлуатації.

На основі результатів аналізу визначено доцільний порядок супроводження експлуатації ІС військового призначення, що включає основні заходи, відповідальних виконавців та нормативно-правову базу, яка забезпечує правове та організаційне підґрунтя (див. таблицю).

Крім того, з урахуванням передового міжнародного досвіду та специфіки функціонування ІС в оборонному секторі, у статті запропоновано структуру військового стандарту, який може бути покладений в основу створення єдиного нормативного документа з питань супроводження експлуатації ІС військового призначення.

Таблиця 1 – Порядок супроводження експлуатації інформаційних систем

№ п/п	Етап супроводження	Основні заходи	Відповідальні суб'єкти	Нормативна основа
1.	Планування супроводження експлуатації ІС	- Формування плану супроводження; - Категоризація ІС за рівнем критичності; - Розробка регламентів та інструкцій.	Органи управління, розпорядники ІС	ЗУ "Про захист інформації в ІКС", ДСТУ ISO/IEC/IEEE 12207:2018, ДСТУ ISO/IEC/IEEE 15288:2016, ДСТУ В 15.003:2021, AAP-48, ДСТУ ISO/IEC 27005, ADatP-4774, ADatP-4778, ДСТУ ISO/IEC/IEEE 27001:2023, ДСТУ ISO/IEC 20000, MC 0458/4

№ п/п	Етап супроводження	Основні заходи	Відповідальні суб'єкти	Нормативна основа
2.	Організація технічного супроводження	- Моніторинг та діагностика стану ІС; - Регламентні роботи та технічне обслуговування; - Виявлення та усунення несправностей; - Резервне копіювання та відновлення.	Органи управління, розпорядники ІС, служби технічної підтримки підрозділів ІКС	ДСТУ ISO/IEC 27035, ДСТУ ISO/IEC 27002, ДСТУ ISO/IEC 20000, ДСТУ ISO/IEC 14764, STANAG 4728, ДСТУ В 15.003:2021, ДСТУ ISO/IEC/IEEE 12207:2018, ДСТУ ISO/IEC 27031, ДСТУ EN ISO 22301, ДСТУ ISO/IEC/IEEE 27001, Наказ МОУ № 240/нм від 17.04.24
3.	Управління оновленнями та модернізація ІС	- Політика керування оновленням; - Адаптація ІС до нових вимог.	Органи управління, розпорядники ІС, розробники ІС, підрядники	ДСТУ ISO/IEC 14764, ДСТУ ISO/IEC 20000, NIST SP 800-128, ДСТУ В 15.003:2021, ДСТУ ISO/IEC/IEEE 12207:2018, ДСТУ ISO/IEC/IEEE 15288:2016, AAP-48, COBIT 2019
4.	Кібербезпека під час супроводження експлуатації ІС	- Управління доступом та автентифікація; - Управління вразливостями та реагування на інциденти; - Контроль безпеки каналів передачі даних; - Організація безперервного підвищення рівня безпеки	Органи управління, розпорядники ІС, підрозділи кібербезпеки, служби захисту інформації	ЗУ "Про захист інформації в ІКС", ПКМУ № 518 від 19.06.2019, ДСТУ ISO/IEC/IEEE 27001:2023, ДСТУ ISO/IEC 27002, NIST SP 800-53, NIST SP 800-61, NIST SP 800-77, NIST SP 800-184, ДСТУ ISO/IEC 27035, ДСТУ ISO/IEC 15408, ДСТУ ISO/IEC 27033, ДСТУ ISO/IEC 29128, ДСТУ ISO/IEC 27005, ДСТУ ISO/IEC 27032
5.	Інформаційно-аналітичне забезпечення супроводження експлуатації ІС	- Збирання та обробка експлуатаційних даних; - Аналіз ефективності роботи ІС та її компонентів; - Формування рекомендацій щодо вдосконалення супроводження експлуатації; - Ведення бази даних щодо історії технічного обслуговування та інцидентів; - Використання методів прогнозування для оптимізації процесів супроводження.	Органи управління, розпорядники ІС, служби технічної підтримки підрозділів ІКС, аналітичні підрозділи	ЗУ "Про захист інформації в ІКС", ЗУ "Про інформацію", ДСТУ ISO/IEC 27004, NIST SP 800-137, AAP-20

№ п/п	Етап супроводження	Основні заходи	Відповідальні суб'єкти	Нормативна основа
6.	Контроль та аудит процесів супроводження експлуатації ІС	- Регулярний моніторинг стану ІС; - Періодичні аудити та перевірки; - Аналіз вразливостей та ризиків; - Удосконалення процесів супроводження.	Органи управління, розпорядники ІС, підрозділи кібербезпеки, внутрішні аудитори та інспекційні органи	ДСТУ ISO/IEC 27001, ДСТУ ISO/IEC 27002, ДСТУ ISO/IEC 27007, ДСТУ ISO/IEC 27008, ДСТУ ISO/IEC 20000, COBIT 2019, NIST SP 800-53
7.	Фінансово-економічне забезпечення супроводження експлуатації ІС	- Планування витрат; - Контроль бюджетування.	Органи управління, розпорядники ІС, фінансово-економічні підрозділи	Закон України "Про публічні закупівлі", ПКМУ № 339 від 27.05.2015, ПКМУ № 262 від 08.03.2024, ПКМУ № 544 від 23.08.2016, ДСТУ ISO/IEC 38500

На основі визначеного порядку супроводження експлуатації інформаційних систем (ІС) військового призначення запропоновано структуру військового стандарту, що забезпечить комплексне нормативне регулювання відповідних процесів. Такий стандарт має на меті уніфікацію вимог, процедур і відповідальності на всіх етапах експлуатаційної підтримки ІС з урахуванням сучасних технологічних викликів та міжнародного досвіду.

Проєкт структури військового стандарту ВСТ 600.XXX.XXX:20XX

1. Загальні положення

1.1. Призначення стандарту

1.2. Сфера застосування

1.3. Нормативні посилання

1.4. Терміни, визначення та скорочення

2. Загальні вимоги до супроводження експлуатації ІС

2.1. Принципи супроводження

2.2. Класифікація ІС за рівнем критичності та її вплив на супроводження

2.3. Види супроводження (профілактичне, коригувальне, адаптаційне, удосконалювальне)

2.4. Взаємодія між розробником, експлуатуючою організацією та користувачами

3. Організація процесів супроводження експлуатації ІС

3.1. Планування та організація супроводження

3.2. Вимоги до технічного супроводу

3.3. Контроль працездатності та управління інцидентами

3.4. Взаємодія з користувачами та функціонування служби підтримки

4. Технічна підтримка та обслуговування ІС

4.1. Моніторинг і діагностика стану ІС

.2. Проведення регламентних робіт та технічного обслуговування

4.3. Виявлення, аналіз та усунення відмов

4.4. Оцінка продуктивності ІС і виявлення "вузьких місць"

4.5. Забезпечення безперервного функціонування та аварійного відновлення

5. Кібербезпека в процесі супроводження ІС

5.1. Вимоги до захисту інформації

5.2. Політики доступу, автентифікації та управління привілеями

5.3. Управління вразливостями та реагування на кіберінциденти

5.4. Захист каналів передачі даних

5.5. Резервне копіювання та відновлення даних

6. Оновлення та модернізація ІС під час експлуатації

6.1. Класифікація оновлень (функціональні, безпекові, технічні)

6.2. Політика управління оновленнями та порядок попереднього тестування

6.3. Забезпечення зворотної сумісності

6.4. Документування змін

7. Інформаційно-аналітичне забезпечення супроводження

7.1. Системи збору та аналізу даних про функціонування ІС

7.2. Прогнозування відмов і оцінка ризиків

7.3. Використання автоматизованих систем управління супроводженням

7.4. Застосування технологій штучного інтелекту для підтримки прийняття рішень

8. Підготовка персоналу та навчання

8.1. Програми підготовки користувачів

8.2. Підвищення кваліфікації технічного персоналу

8.3. Навчання реагуванню на інциденти

8.4. Оцінювання результативності підготовки

9. Контроль та аудит процесів супроводження

9.1. Критерії оцінювання ефективності супроводження

9.2. Порядок проведення внутрішнього аудиту

9.3. Забезпечення якості процесів супроводження

9.4. Документування та звітування за результатами аудиту

10. Фінансово-економічне забезпечення супроводження

10.1. Планування витрат на супроводження

10.2. Оптимізація витрат і оцінка економічної ефективності

10.3. Контроль бюджетного використання ресурсів

10.4. Альтернативні моделі фінансування (аутсорсинг, державно-приватне партнерство)

Запропонована структура охоплює всі ключові компоненти процесу супроводження експлуатації ІС військового призначення, створюючи підґрунтя для уніфікації підходів, підвищення ефективності, забезпечення надійності та кіберстійкості систем в умовах гібридних загроз та швидких технологічних змін.

Висновки

Таким чином, у ході проведеного дослідження здійснено комплексний аналіз нормативно-правового забезпечення супроводження експлуатації інформаційних систем військового призначення. Виявлено ключові проблеми, зокрема — відсутність єдиного нормативного документа, який би регламентував відповідні процеси та забезпечував уніфікацію підходів до їх реалізації.

На підставі аналізу міжнародного досвіду, зокрема стандартів НАТО та ISO, ідентифіковано основні напрями вдосконалення нормативної бази у сфері супроводження експлуатації ІС. У цьому контексті обґрунтовано доцільність розроблення військового стандарту, що охоплює всі ключові аспекти супроводження, включаючи технічне обслуговування, забезпечення інформаційної безпеки, управління оновленнями, кадрову підготовку та логістичну підтримку.

У межах дослідження розроблено проект структури зазначеного військового стандарту, що включає основні розділи та положення, спрямовані на нормативне регламентування процесів супроводження експлуатації ІС. Запропонована структура забезпечує системний і комплексний підхід до організації відповідної діяльності та сприяє підвищенню ефективності управління інформаційними системами військового призначення.

Отримані результати можуть бути використані в процесі розроблення нормативно-правових актів, що регламентують супроводження експлуатації інформаційних систем у Міністерстві оборони України та інших структурах сектору безпеки і оборони.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Про захист інформації в інформаційно-комунікаційних системах: Закон України № 80/94-ВР від 05.07.1994 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/80/94-вр. (Дата звернення: 10.03.2025).
2. Про інформацію: Закон України № 2657-XII від 02.10.1992 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2657-12. (Дата звернення 10.03.2025).
3. Про публічні закупівлі: Закон України № 922-VIII від 25.12.2015 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/922-19. (Дата звернення 11.03.2025).
4. Про затвердження вимог до кіберзахисту об’єктів критичної інфраструктури: Постанова Каб. Міністрів України № 518 від 19.06.2019 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/518-2019. (Дата звернення 25.03.2025).
5. Про затвердження Порядку фінансового забезпечення потреб національної оборони держави, мобілізаційної підготовки, заходів з мобілізації та Збройних Сил за рахунок благодійних пожертв фізичних та юридичних осіб: Постанова Каб. Міністрів України № 339 від 27.05.2015. URL: https://zakon.rada.gov.ua/laws/show/339-2015. (Дата звернення 14.03.2025).
6. Деякі питання забезпечення розвитку інновацій та технологій для потреб оборони: Постанова Каб. Міністрів України № 262 від 08.03.2024. URL: https://zakon.rada.gov.ua/laws/show/262-2024. (Дата звернення 18.03.2025).
7. Про затвердження Порядку використання коштів, передбачених у державному бюджеті для виконання державних цільових програм реформування та розвитку оборонно-промислового комплексу, розроблення, освоєння і впровадження нових технологій, нарощування наявних виробничих потужностей для виготовлення продукції оборонного призначення: Постанова Каб. Міністрів України № 544 від 23.08.2016 (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/544-2016. (Дата звернення 18.03.2025).
8. Про затвердження Порядку організації в системі Міністерства оборони України технічної підтримки інформаційних (автоматизованих), інформаційно-комунікаційних, електронних комунікаційних систем, систем спеціального зв'язку та користувачів таких систем: Наказ Міністерства оборони України № 240/нм від 17.04.2024. URL: https://zakon.rada.gov.ua/rada/show/v0240322-24. (Дата звернення 19.03.2025).
9. ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018. 252 с.
10. ДСТУ ISO/IEC/IEEE 12207:2018. Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів. Дійсний з 15.08.2018. ДП «УкрНДНЦ», 2018.
11. ДСТУ ISO/IEC/IEEE 15288:2016. Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем. Дійсний з 01.01.2018. ДП «УкрНДНЦ», 2016.

12. ДСТУ ISO/IEC/IEEE 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. Дійсий з 22.08.2023. ДП «УкрНДНЦ», 2023.
13. ДСТУ ISO/IEC 27002:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Засоби контролювання інформаційної безпеки. Дійсний з 22.08.2023. ДП «УкрНДНЦ», 2023.
14. ДСТУ ISO/IEC 27004:2018 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Моніторинг, вимірювання, аналізування та оцінювання. Дійсний з 01.10.2018. ДП «УкрНДНЦ», 2018.
15. ДСТУ ISO/IEC 27005:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки. Дійсний з 22.08.2023. ДП «УкрНДНЦ», 2023.
16. ДСТУ ISO/IEC 27007:2018. Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою. Дійсний з 01.01.2019. ДП «УкрНДНЦ», 2018.
17. ДСТУ ISO/IEC TS 27008:2019. Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. Дійсний з 01.11.2019. ДП «УкрНДНЦ», 2019.
18. ДСТУ ISO/IEC 27031:2015. Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. Чинний з 01.01.2016. ДП «УкрНДНЦ», 2015.
19. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. Дійсний з 01.02.2025. ДП «УкрНДНЦ», 2024.
20. Серія стандартів ДСТУ ISO/IEC 27033. Інформаційні технології. Методи захисту. Захист мережі. Частини 1 – 6. ДП «УкрНДНЦ».
21. Серія стандартів ДСТУ ISO/IEC 27035. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частини 1 – 3. ДП «УкрНДНЦ».
22. Серія стандартів ДСТУ ISO/IEC 20000. Інформаційні технології. Керування послугами. Частини 1 – 12. ДП «УкрНДНЦ».
23. ДСТУ ISO/IEC 14764:2014. Інженерія програмного забезпечення. Процеси життєвого циклу програмного забезпечення. Технічне обслуговування. Дійсний з 01.01.2016. ДП «УкрНДНЦ», 2014.
24. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги. Чинний з 01.09.2022. ДП «УкрНДНЦ», 2021.
25. Серія стандартів ДСТУ ISO/IEC 15408. Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частини 1 – 5. ДП «УкрНДНЦ».
26. ДСТУ ISO/IEC 29128-1:2024 Інформаційна безпека, кібербезпека та захист конфіденційності. Перевірка криптографічних протоколів. Частина 1. Структура. Дійсний з 01.02.2025. ДП «УкрНДНЦ», 2024.
27. ДСТУ ISO/IEC 38500:2016 Інформаційні технології. Управління ІТ в організації. Дійсний з 01.10.2017. ДП «УкрНДНЦ», 2016.
28. ДСТУ В 15.003:2021. Система розроблення і поставлення на виробництво озброєння та військової техніки. Процеси життєвого циклу озброєння та військової техніки. Дійсний з 01.09.2022. ДП «УкрНДНЦ», 2021.
29. AAP-20. NATO Programme Management Framework (NATO Life Cycle Model). Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2015, 78 p.
30. AAP-48. NATO System Life Cycle Processes. Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2022, 202 p.
31. STANAG 4728. System Life Cycle Management. Ed. 2. NSO, Brussels, 1110 Belgium, 2022, 5 p.
32. ADatP-4774. Confidentiality metadata. Label Syntax. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2017, 108 p.

33. ADatP-4778. Metadata Binding Mechanism. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2018, 72 p.
34. MC 0458/4. NATO Education, Training, Exercises and Evaluation Policy. NATO, 2023, 48 p.
35. NIST SP 800-37 Rev. 2. Risk Management Framework (RMF) For Information System and Organizations. A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology, U.S., Gaithersburg, 2018, 183 p.
36. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information System and Organizations. National Institute of Standards and Technology, U.S., Gaithersburg, 2020, 492 p.
37. NIST SP 800-83 Rev. 1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology, U.S., Gaithersburg, 2013, 47 p.
38. NIST SP 800-128. Guide for Security – Focused Configuration Management of Information System. National Institute of Standards and Technology, U.S., Gaithersburg, 2019, 99 p.
39. NIST SP 800-160 V. 1, Rev. 1. Engineering Trustworthy Secure System. National Institute of Standards and Technology, U.S., Gaithersburg, 2022, 195 p.
40. Серебро М.В. Особливості адміністративно-правового регулювання використання та розвитку інформаційних технологій в умовах воєнного стану. Київський часопис права, № 3, 2024, с. 177-183. https://doi.org/10.32782/klj/2024.3.26.
41. Руденська Г.В. Моделі та процеси життєвого циклу інформаційної системи управління оборонними ресурсами. Збірник наукових праць ЦВСД, № 1(68), Київ, НУОУ, 2020, с. 59-65. https://doi.org/10.33099/2304-2745/2020-0/59-65.
42. Рибидайло А., Галаган В., Васюхно С., Мулявка А., Руденська Г. Порядок організації створення спеціального програмного забезпечення для інформаційних систем військового призначення. Збірник наукових праць ЦВСД, № 1(77), Київ, НУОУ, 2023, с. 69-78. https://doi.org/10.33099/2304-2745/2023-1-77/69-78.
43. Бондарчук С., Васюхно С., Галаган В., Гріненко О. Пропозиції щодо організації інформаційно-аналітичної підтримки ведення проєктів інформатизації. Збірник наукових праць ЦВСД, № 3(73), Київ, НУОУ, 2021, с. 67-72. https://doi.org/10.33099/2304-2745/2021-3-73/68-73.
44. Андрій Дядечко, Іван Даценко, Олександр Головченко. Концептуальні аспекти технологічної підтримки інформаційної інфраструктури Міністерства оборони України. Сучасні інформаційні технології у сфері безпеки та оборони, № 51(3), Київ, НУОУ, 2024, с. 96-107. https://doi.org/10.33099/2311-7249/2024-51-3-96-107.

References

1. On the Protection of Information in Information and Communication Systems: Law of Ukraine No. 80/94-BP dated 05.07.1994 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/80/94-вр. (Date of access: 10.03.2025).
2. For information: Law of Ukraine No. 2657-XII of 02.10.1992 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/2657-12. (Date of access 10.03.2025).
3. On public procurement: Law of Ukraine No. 922-VIII of 25.12.2015 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/922-19. (Date of access 11.03.2025).
4. On approval of requirements for cyber protection of critical infrastructure facilities: Resolution of the Cabinet of Ministers of Ukraine No. 518 of 19.06.2019 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/518-2019. (Date of access 25.03.2025).
5. On approval of the Procedure for financial support of the needs of the national defense of the state, mobilization training, mobilization measures and the Armed Forces at the expense of charitable donations from individuals and legal entities: Resolution of the Cabinet of Ministers of Ukraine No. 339 of 27.05.2015. Available from : https://zakon.rada.gov.ua/laws/show/339-2015. (Date of application 14.03.2025).

6. Some issues of ensuring the development of innovations and technologies for defense needs: Resolution of the Cabinet of Ministers of Ukraine No. 262 of 08.03.2024. Available from : https://zakon.rada.gov.ua/laws/show/262-2024. (Date of access 18.03.2025).
7. On approval of the Procedure for the use of funds provided for in the state budget for the implementation of state target programs for the reform and development of the defense-industrial complex, the development, mastering and implementation of new technologies, and the expansion of existing production capacities for the manufacture of defense products: Resolution of the Cabinet of Ministers of Ukraine No. 544 of 23.08.2016 (as amended). Available from : https://zakon.rada.gov.ua/laws/show/544-2016. (Date of application 18.03.2025).
8. On approval of the Procedure for organizing technical support of information (automated), information and communication, electronic communication systems, special communication systems and users of such systems in the system of the Ministry of Defense of Ukraine: Order of the Ministry of Defense of Ukraine No. 240/nm dated 17.04.2024. Available from : https://zakon.rada.gov.ua/rada/show/v0240322-24. (Date of application 19.03.2025).
9. ISACA. COBIT 2019 Framework: Governance and Management Objectives. ISACA, 2018. 252 p.
10. DSTU ISO/IEC/IEEE 12207:2018. Systems and software engineering. Software life cycle processes. Valid from 15.08.2018. "UkrNDNC", 2018.
11. DSTU ISO/IEC/IEEE 15288:2016. Systems and Software Engineering. Systems Life Cycle Processes. Valid from 01.01.2018. "UkrNDNC", 2016.
12. DSTU ISO/IEC/IEEE 27001:2023. Information security, cybersecurity and privacy protection. Information security management systems. Requirements. Valid from 22.08.2023. "UkrNDNC", 2023.
13. DSTU ISO/IEC 27002:2023. Information security, cybersecurity and privacy protection. Information security controls. Valid from 22.08.023. "UkrNDNC", 2023.
14. DSTU ISO/IEC 27004:2018 Information technologies. Protection methods. Information security management systems. Monitoring, measurement, analysis and evaluation. Valid from 01.10.2018. "UkrNDNC", 2018.
15. DSTU ISO/IEC 27005:2023. Information security, cybersecurity and privacy protection. Information security risk management guidance. Valid from 22.08.2023. "UkrNDNC", 2023.
16. DSTU ISO/IEC 27007:2018. Information technologies. Protection methods. Guidance on auditing information security management systems. Valid from 01.01.2019. "UkrNDNC", 2018.
17. DSTU ISO/IEC TS 27008:2019. Information technologies. Protection methods. Guidance on assessing information security protection. Valid from 01.11.2019. "UkrNDNC", 2019.
18. DSTU ISO/IEC 27031:2015. Information technologies. Protection methods. Guidelines for the readiness of information and communication technologies for business continuity. Valid from 01.01.2016. "UkrNDNC", 2015.
19. DSTU ISO/IEC 27032:2024 Information technology. Protection methods. Guidelines for cybersecurity. Valid from 01.02.2025. "UkrNDNC", 2024.
20. Series of standards DSTU ISO/IEC 27033. Information technologies. Protection methods. Network protection. Parts 1 – 6. "UkrNDNC".
21. Series of standards DSTU ISO/IEC 27035. Information technologies. Protection methods. Information security incident management. Parts 1 – 3. "UkrNDNC".
22. DSTU ISO/IEC 20000 series of standards. Information technology. Service management. Parts 1 – 12. "UkrNDNC".
23. DSTU ISO/IEC 14764:2014. Software engineering. Software life cycle processes. Maintenance. Valid from 01.01.2016. "UkrNDNC", 2014.
24. DSTU EN ISO 22301:2021. Security and stability. Business continuity management systems. Requirements. Effective from 01.09.2022. "UkrNDNC", 2021.

25. DSTU ISO/IEC 15408 series of standards. Information technologies. Cybersecurity and privacy protection. IT security assessment criteria. Parts 1 – 5. "UkrNDNC".
26. DSTU ISO/IEC 29128-1:2024 Information security, cybersecurity and privacy protection. Verification of cryptographic protocols. Part 1. Structure. Valid from 01.02.2025. "UkrNDNC", 2024.
27. DSTU ISO/IEC 38500:2016 Information technology. IT management in the organization. Valid from 01.10.2017. "UkrNDNC", 2016.
28. DSTU V 15.003:2021. System for the development and commissioning of weapons and military equipment. Life cycle processes of weapons and military equipment. Effective from 01.09.2022. "UkrNDNC", 2021.
29. AAP-20. NATO Programme Management Framework (NATO Life Cycle Model). Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2015, 78 p.
30. AAP-48. NATO System Life Cycle Processes. Ed. C, v. 1. NSO, Brussels, 1110 Belgium, 2022, 202 p.
31. STANAG 4728. System Life Cycle Management. Ed. 2. NSO, Brussels, 1110 Belgium, 2022, 5 p.
32. ADatP-4774. Confidentiality metadata. Label Syntax. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2017, 108 p.
33. ADatP-4778. Metadata Binding Mechanism. Ed. A, Ver. 1. NATO, Allied Data Processing Publication, 2018, 72 p.
34. MC 0458/4. NATO Education, Training, Exercises and Evaluation Policy. NATO, 2023, 48 p.
35. NIST SP 800-37 Rev. 2. Risk Management Framework (RMF) For Information System and Organizations. A System Life Cycle Approach for Security and Privacy. National Institute of Standards and Technology, U.S., Gaithersburg, 2018, 183 p.
36. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information System and Organizations. National Institute of Standards and Technology, U.S., Gaithersburg, 2020, 492 p.
37. NIST SP 800-83 Rev. 1. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. National Institute of Standards and Technology, U.S., Gaithersburg, 2013, 47 p.
38. NIST SP 800-128. Guide for Security – Focused Configuration Management of Information System. National Institute of Standards and Technology, U.S., Gaithersburg, 2019, 99 p.
39. NIST SP 800-160 V. 1, Rev. 1. Engineering Trustworthy Secure System. National Institute of Standards and Technology, U.S., Gaithersburg, 2022, 195 p.
40. Serebro M.V. Peculiarities of administrative and legal regulation of the use and development of information technologies under martial law. Kyiv Law Journal, No. 3, 2024, pp. 177-183. https://doi.org/10.32782/klj/2024.3.26.
41. Rudenska G.V. Models and processes of the life cycle of the information system for managing defense resources. Collection of scientific papers of the Central Scientific and Technical University of Ukraine, No. 1(68), Kyiv, NUOU, 2020, pp. 59-65. https://doi.org/10.33099/2304-2745/2020-0/59-65.
42. Rybydaylo A., Galahan V., Vasyukhno S., Mulyavka A., Rudenska G. The procedure for organizing the creation of special software for military information systems. Collection of scientific works of the Central Scientific and Technological Center, No. 1(77), Kyiv, NUOU, 2023, pp. 69-78. https://doi.org/10.33099/2304-2745/2023-1-77/69-78.
43. Bondarchuk S., Vasyukhno S., Galahan V., Grinenko O. Proposals for the organization of information and analytical support for conducting informatization projects. Collection of scientific works of the Central Scientific and Technological Center, No. 3(73), Kyiv, NUOU, 2021, pp. 67-72. https://doi.org/10.33099/2304-2745/2021-3-73/68-73.
44. Andrii Diadechko, Ivan Datsenko, Oleksandr Holovchenko. Conceptual aspects of technological support of the information infrastructure of the Ministry of Defense of Ukraine. Modern information technologies in the sphere of security and defense, No. 51(3), Kyiv, NUOU, 2024, pp. 96-107. https://doi.org/10.33099/2311-7249/2024-51-3-96-107.