СЕКЦІЯ 3. ТЕОРІЯ І МЕТОДИКА ПРОФЕСІЙНОЇ ОСВІТИ

УДК [37-042.4:004:355/359]:005.336.4(100:477)
DOI https://doi.org/10.32999/ksu2413-1865/2025-112-6

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ПІДГОТОВЦІ ФАХІВЦІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ: ВІТЧИЗНЯНИЙ ТА МІЖНАРОДНИЙ ДОСВІД

Богуславський Віктор Володимирович,
кандидат юридичних наук, доцент,
завідувач кафедри спеціальної фізичної підготовки,
Дніпровський державний університет внутрішніх справ
orcid.org/0000-0003-2688-4505
v_bogyslavskiy@icloud.com

Стрімкий розвиток інформаційних технологій (ІТ) докорінно трансформував систему професійної освіти у світі, запровадивши нові формати передачі знань та формування компетентностей. Для України інтеграція інноваційних цифрових засобів у процес професійної підготовки фахівців сектору безпеки та оборони є важливим чинником забезпечення їхньої готовності до виконання службових завдань у сучасних умовах. Мета. Метою дослідження є визначення ролі та ефективності сучасних інформаційних технологій у процесі підготовки майбутніх фахівців сектору безпеки та оборони України на основі аналізу досвіду НАТО, України та провідних країн світу.

Методи. Теоретичний аналіз наукових джерел і нормативних документів; систематизація та порівняльний аналіз вітчизняного та міжнародного досвіду впровадження ІТ у підготовку фахівців безпекового сектору; узагальнення практик застосування віртуальних симуляцій, дистанційного навчання та аналітичних систем. **Результати.** Дослідження показало, що сучасні інформаційні технології є ключовим фактором підвищення якості підготовки фахівців сектору безпеки та оборони. Зокрема: віртуальні симуляції та тренажери (VR/AR) дозволяють відпрацьовувати дії в реалістичних сценаріях без ризику для життя; платформи дистанційного навчання (LMS) забезпечують гнучкість та доступність освітнього процесу; системи штучного інтелекту та аналізу великих даних (Big Data) розвивають аналітичні компетенції та навички прийняття рішень. Аналіз досвіду НАТО (C4ICSR, MIP, ADL, NATO Cyber Range), України (система «Дельта», платформа «ТРО.Освіта», кіберкомандування ЗСУ) та інших країн (США, Ізраїль, Польща) підтвердив ефективність комплексного застосування ІТ для забезпечення бойової готовності та оперативності реагування. Водночас виявлено виклики: недостатня матеріально-технічна база, брак кваліфікованих кадрів для супроводу технологій та потреба в адаптації навчальних програм до цифрових форматів. **Висновки.** Сучасні інформаційні технології є необхідною умовою ефективної підготовки майбутніх фахівців сектору безпеки та оборони України. Їх застосування підвищує якість освіти, забезпечує формування критичного мислення, аналітичних навичок та здатності до швидкої адаптації в умовах цифрового середовища. Досвід провідних країн та НАТО підтверджує необхідність системної інтеграції ІТ у навчальний процес, розвитку цифрової інфраструктури та підвищення кваліфікації викладачів для формування сучасних освітніх стандартів у секторі безпеки та оборони.

Ключові слова: *інформаційні технології, професійна підготовка, сектор безпеки та оборони, гібридна війна, цифрові загрози, симуляції, дистанційне навчання, професійні компетентності.*

MODERN INFORMATION TECHNOLOGIES IN TRAINING SECURITY AND DEFENSE SECTOR SPECIALISTS: NATIONAL AND INTERNATIONAL EXPERIENCE

Boguslavskiy Victor Volodymyrovych,
Candidate of Legal Sciences, Associate Professor,
Head of the Department of Special Physical Training
Dnipro State University of Internal Affairs
orcid.org/0000-0003-2688-4505
v_bogyslavskiy@icloud.com

The rapid development of information technologies (IT) has fundamentally transformed the professional education system worldwide, introducing new formats for knowledge transfer and competence formation. For Ukraine, the integration of innovative digital tools into the professional training process of security and defense

sector specialists is an important factor in ensuring their readiness to perform official duties in modern conditions**. Purpose.** The purpose of the study is to determine the role and effectiveness of modern information technologies in the training process of future security and defense sector specialists in Ukraine based on the analysis of NATO, Ukrainian, and leading countries' experience. **Methods.** Theoretical analysis of scientific sources and regulatory documents; systematization and comparative analysis of national and international experience in implementing IT in security sector specialist training; generalization of practices in applying virtual simulations, distance learning, and analytical systems. **Results.** The study demonstrated that modern information technologies are a key factor in improving the quality of security and defense sector specialist training. Specifically: virtual simulations and trainers (VR/AR) enable practicing actions in realistic scenarios without risk to life; distance learning platforms (LMS) ensure flexibility and accessibility of the educational process; artificial intelligence systems and Big Data analysis develop analytical competencies and decision-making skills. Analysis of NATO experience (C4ICSR, MIP, ADL, NATO Cyber Range), Ukraine (Delta system, TRO.Osvita platform, Armed Forces Cyber Command) and other countries (USA, Israel, Poland) confirmed the effectiveness of comprehensive IT application for ensuring combat readiness and response efficiency. However, challenges were identified: insufficient material and technical base, lack of qualified personnel for technology support, and the need to adapt educational programs to digital formats. **Conclusions.** Modern information technologies are a necessary condition for effective training of future security and defense sector specialists in Ukraine. Their application improves the quality of education, ensures the formation of critical thinking, analytical skills, and the ability to rapidly adapt in a digital environment. The experience of leading countries and NATO confirms the necessity of systematic IT integration into the educational process, development of digital infrastructure, and improvement of teacher qualifications to form modern educational standards in the security and defense sector.

Keywords: *information technologies, professional training, security and defense sector, virtual simulations, distance learning, cybersecurity, artificial intelligence, NATO experience, digital transformation.*

Вступ. Сучасний світ характеризується стрімким розвитком інформаційних технологій, які дедалі більше інтегруються у всі сфери людської діяльності, зокрема у безпекову сферу (Горлинський & Ананьїн, 2021: 219; Федоренко, 2018: 506). Інформаційні технології (ІТ) включають різноманітні цифрові інструменти, системи збору, обробки та аналізу даних, а також платформи для комунікації та навчання, що формують новий якісний рівень підготовки фахівців. В контексті сектору безпеки та оборони ІТ виступають не лише як засіб оптимізації професійних функцій, а й як фундаментальна складова навчального процессу (Чоп, Дерев'янчук & Козир, 2019: 127; Сокол, 2024: 45).

Підготовка майбутніх співробітників сектору безпеки потребує формування широкого спектру компетенцій, зокрема аналітичних, технічних, комунікативних, а також навичок прийняття швидких і ефективних рішень в умовах ризику. Сучасні інформаційні технології забезпечують необхідні умови для набуття та вдосконалення цих компетенцій через використання інтерактивних навчальних систем, віртуальних тренажерів, дистанційних курсів і систем моделювання реальних бойових чи кризових ситуацій (Davydiuk, Potii, 2024: 23-24; Ukraine Cybersecurity Governance Assessment, 2021). Попри наявні дослідження у сфері застосування інформаційних технологій у підготовці сектору безпеки та оборони, обрана тема залишається недостатньо вивченою та потребує подальшого розвитку, уточнення методичних підходів та впровадження інноваційних рішень у навчальний процес.

Мета дослідження – визначення ролі та ефективності сучасних інформаційних технологій у процесі підготовки майбутніх фахівців сектору безпеки та оборони України на основі аналізу досвіду НАТО, України та провідних країн світу.

Завдання дослідження: 1. Проаналізувати теоретичні основи застосування інформаційних технологій у процесі підготовки майбутніх фахівців сектору безпеки та оборони. 2. Оцінити сучасні ІТ-рішення та їх вплив на навчальний процес у відповідних структурах. 3. Визначити практичні аспекти впровадження інформаційних технологій у підготовку майбутніх фахівців сектору безпеки та оборони. 4. Розробити рекомендації щодо удосконалення інтеграції ІТ у навчальний процес.

Методологія та методи. Дослідження здійснювалося на основі системного та комплексного підходів, що дозволяють розглядати навчальний процес як цілісну систему з взаємозв'язаними елементами. Використовувався порівняльно-емпіричний підхід для аналізу вітчизняних і зарубіжних практик інтеграції ІТ у підготовку кадрів. Основні методи включали теоретичний аналіз джерел і нормативів, оцінку сучасних ІТ-рішень, порівняльне вивчення практик та розроблення рекомендацій щодо вдосконалення інтеграції ІТ у навчальний процес.

Результати та дискусії. Теоретичні основи використання ІТ у підготовці фахівців сектору безпеки та оборони присвячено публікацію Горлинського В.В., Ананьїна О.В. (2021) (Горлинський, Ананьїн, 2021: 219). Федоренко О.І. (2018) розглянуто дидактичні особливості застосування ІТ у навчальному процесі,

зокрема в контексті підготовки фахівців для сил охорони правопорядку (Федоренко, 2018: с. 506). Дослідження Чопи Д., Дерев'янчука А. та Козир Н. (2019) висвітлює використання мультимедійних тренажерів, моделювання навчальних ігор та автоматизованих систем оцінки знань у навчальному процесі (Чопа, Дерев'янчук & Козир, 2019: 127).

Одним із ключових напрямів застосування ІТ у підготовці фахівців сектору безпеки є використання симуляційних систем і технологій віртуальної реальності (VR). Віртуальні тренажери дають змогу відпрацьовувати дії у максимально наближеному до реальних умов середовищі без ризику для життя та здоров'я. Завдяки VR-симуляціям можна моделювати різноманітні сценарії, від тактичних операцій до кризового управління, що значно підвищує ефективність навчання та адаптивність майбутніх співробітників.

Дистанційне навчання та електронні платформи, зокрема системи управління навчанням (Learning Management Systems – LMS), забезпечують доступність навчальних матеріалів у будь-який час і в будь-якому місці. Це особливо актуально для підготовки персоналу у військових та правоохоронних структурах, де є потреба у безперервному оновленні знань та навичок. Завдяки таким платформам можна організовувати тематичні курси, тестування, групові дискусії та контроль прогресу у режимі онлайн.

Ще одним перспективним напрямом є застосування систем аналізу великих даних (Big Data) та штучного інтелекту (ШІ) для формування навичок аналітичної роботи. Сучасні ІТ-рішення дозволяють автоматизувати процеси збору, обробки й інтерпретації інформації, що є важливим для оперативного прийняття рішень у сфері безпеки. Крім того, ШІ використовується для створення адаптивних навчальних систем, які підлаштовуються під індивідуальні потреби та рівень підготовки слухачів (Ситник & Орел, 2024: 45).

Військові та спеціальні навчальні заклади активно впроваджують сучасні інформаційні технології у навчальний процесс (Сокол, 2024: 12). Досвід свідчить, що застосування симуляторів, VR-технологій і дистанційних курсів сприяє підвищенню мотивації здобувачів, покращенню засвоєння матеріалу та розвитку критичного мислення. Однак процес інтеграції ІТ також пов'язаний із певними викликами, серед яких – недостатня матеріально-технічна база, потреба у кваліфікованих кадрах для підтримки та супроводу технологій, а також необхідність адаптації навчальних програм до нових цифрових форматів.

Крім того, важливо враховувати психологічні та соціальні аспекти використання ІТ у підготовці, зокрема уникнення інформаційного перевантаження, забезпечення безпеки даних і підтримку міжособистісної взаємодії у цифровому середовищі. Перспективним є поєднання традиційних методів навчання з сучасними ІТ-рішеннями для досягнення максимальної ефективності.

Інформаційні технології (ІТ) у сфері безпеки та оборони представляють собою сукупність технічних програмних і організаційних засобів, що забезпечують збір, збереження, обробку, передавання, аналіз і захист інформації, яка є необхідною для підтримки стабільного функціонування органів безпеки, оборони, правопорядку та управління кризовими ситуаціями. Їхнє застосування спрямоване на підвищення ефективності реагування на загрози, забезпечення контрою за різноманітними подіями в реальному часі, а також удосконалення процесів прийняття управлінських і тактичних рішень.

Ключовими ознаками ІТ у сфері безпеки та оборони є: 1) орієнтація на високий ступінь надійності та безвідмовності; здатність до обробки великих обсягів інформації в режимі реального часу; 3) інтеграція з фізичними системами безпеки (відеоспостереження, дрони, сенсори); 4) наявність механізмів кіберзахисту й криптографічної безпеки; 5) можливість прогнозування загроз на основі моделювання та аналізу даних (Ситник, Орел, 2024: 45). У табл. 1 наведено характеристику ІТ-технологій для без пекового напрямку.

Таким чином, сучасні інформаційні технології в сфері безпеки та оборони – це багатофункціональний інструмент, який охоплює різні рівні управління, взаємодії та навчання. Їх класифікація дозволяє краще орієнтуватись в їх можливостях, а також забезпечити цілеспрямовану підготовку майбутніх фахівців відповідно до специфіки завдань, які стоять перед структурами безпеки та оборони.

Наступним кроком дослідження слугувало вивчення практичних механізмів застосування ІТ у безпековій сфері з урахуванням досвіду НАТО, України та інших країн, що дозволить виокремити найбільш результативні підходи та інноваційні рішення.

У країнах-членах НАТО цифровізація оборонного сектору являється пріоритетним напрямом. Військові підрозділи Альянсу активно використовують:

1. Систему C4ICSR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance), що являє собою інтегровану систему для управління військами, збору розвідданих та обміну інформацією в реальному часі.

2. MIP (Multilateral Interoperability Programme), представляє ініціативу зі стандартизації інформаційного обміну між арміями країн НАТО, яка дозволяє оперативно координувати дії у багатонаціональних операціях.

Таблиця 1

Класифікація сучасних інформаційних технологій у сфері безпеки

Характеристика	Мета/призначення
1. За функціональним призначенням	
Аналітичні системи	Для збору, обробки й аналізу даних (Big Data Analytics, OSINT-платформи тощо)
Оперативні системи	Для підтримки управлінських рішень в реальному часі (Command & Control Systems – C2)
Навчальні технології	Для підготовки фахівців (системи віртуальної реальності, моделювання ситуацій, LMS)
Інформаційно-пошукові системи	Бази даних, архіви, оперативний доступ відомостей
Технології зв'язку та передачі даних	Захищені канали, тактичні мережі, супутниковий зв'язок
Системи кібербезпеки	Антивірусне програмне забезпечення, фаєрволи, технології виявлення атак (IDS/IPS)
2. За рівнем інтеграції	
Автономні системи	Функціонують окремо (наприклад, програмне забезпечення тренувань персоналу)
Інтегровані системи	Пов'язані в єдину мережу з обміном даними між підрозділами (центри ситуаційного моніторингу, мультиагентні системи)
3. За типом доступу	
Локальні	Застосовуються в межах одного об'єкта чи організації
Хмарні (Cloud-based)	Забезпечують мобільність й доступ до ресурсів з будь-якої точки світу з відповідним рівнем захисту
Гібридні	Поєднують елементи локального й хмарного зберігання/обробки інформації
4. За рівнем автоматизації	
Ручні IT-засоби	Програми, що потребують значної участі людини в управлінні
Напівавтоматизовані системи	Автоматизують окремі етапи, зберігаючи контроль оператора
Автономні IT-системи з елементами ШІ	Здатні до самостійного прийняття рішень або адаптації до змін середовища (наприклад, автономні дрони зі штучним інтелектом)

3. ADL (Advanced Distributed Learning) складається з платформи дистанційного навчання для підготовки офіцерів із сержантського складу, що є доступним як у навчальних закладах, так і безпосередньо у зоні бойових дій.

4. NATO Cyber Range репрезентує віртуальні полігони для навчання кіберзахисту, де відпрацьовуються сценарії захисту критичної інфраструктури від цифрових атак (Norfolk (VA): NATO ADL Initiative, 2023; Brussels: NATO, 2024: 19).

Доцільно акцентувати увагу на вітчизняному практичному досвіді та підходах. Після 2014 року Україна здійснила значний прогрес у сфері цифрової трансформації оборонного сектору, а саме: 1) Система «Дельта», яка функціонує як інтегрована ситуаційна система, що забезпечує командирів цих рівнів актуальними розвідувальними та бойовими даними у реальному часі, та об'єднує інформацію з дронів, камер спостереження, супутників й інших джерел; 2) цифрові платформи підготовки Сил територіальної оборони, що містять в собі платформи дистанційного навчання (наприклад, «ТРО.Освіта»), які мають в своєму складі курси з тактики, домедичної підготовки, мінної безпеки, зв'язку тощо; 3) співпраця з країнами-партнерами (США, Великобританія, Литва), які надають програмне забезпечення, системи безпілотного моніторингу, засоби радіоелектронної боротьби й тренажерів; 4) кіберкомандування ЗСУ, яке створене у 2020 році з метою захисту від кібератак і розвитку можливостей у кібероперацій (Міністерство оборони України, 2021; Указ № 447/2021 «Про Стратегію кібербезпеки України», 2021; Bondar, 2024; Cooperative Cyber Defence Centre of Excellence, 2024).

Слід реально розглянути підходи застосування інформаційних технологій, що реалізо-

вані в інших країнах. Загалом, Ізраїль визнаний як світовий лідер у сфері кібербезпеки та використання IT в обороні. Служба оборони (IDF) широко використовує автономні дрони з елементами штучного інтелекту, систему Iron Dome, яка функціонує в напівавтоматичному режимі для перехоплення ракет.

У США активно застосовують віртуальні симулятори (наприклад, VBS3, Fort Irwin) для підготовки до боїв у міських умовах, а також розвивають проект Project Convergence, що об'єднує штучний інтелект, сенсори, дрони та автоматизоване управління в єдину систему.

Стосовно Польщі та кран Балтії, вони інтегрують системи кіберзахисту у структурі територіальної оборони, у тісній взаємодії співпрацюють з НАТО в частині стандартизації IT-рішень й відпрацювання спільних сценаріїв на навчання Locked Shields (кібернавчання) (Norfolk (VA): NATO ADL Initiative, 2023: 120).

Висновки.

1. Інтеграція сучасних інформаційних технологій у процес підготовки фахівців сектору безпеки та оборони є необхідною умовою забезпечення їхньої готовності до виконання професійних завдань у цифровому середовищі та адаптації до нових викликів сучасності.

2. Використання віртуальних симуляцій, мультимедійних тренажерів, систем дистанційного навчання (LMS), технологій штучного інтелекту та аналізу великих даних (Big Data) сприяє підвищенню якості навчання, розвитку аналітичних компетенцій та готовності майбутніх співробітників до реальних умов служби.

3. Досвід НАТО (системи C4ICSR, MIP, ADL, NATO Cyber Range), України (система «Дельта», платформи «ТРО.Освіта», кіберкомандування ЗСУ) та інших країн (Ізраїль, США, Польща, країни Балтії) засвідчує ефективність застосування інформаційних технологій для забезпечення високої бойової готовності, швидкості реагування та здатності до дій у сучасних умовах конфліктів.

4. Подальший розвиток інтеграції IT у навчальний процес потребує вирішення таких викликів, як удосконалення матеріально-технічної бази, підготовка кваліфікованих кадрів для супроводу технологій, адаптація навчальних програм до цифрових форматів, а також забезпечення кібербезпеки та психологічної підтримки слухачів у цифровому середовищі.

Таким чином, ефективне використання сучасних інформаційних технологій у сфері безпеки та оборони дозволяє не тільки удосконалити процеси підготовки кадрів, а й забезпечити формування критичного мислення, аналітичних навичок та здатності до швидкої адаптації в умовах постійних змін цифрового середовища, що є критично важливим для успішного виконання професійних завдань у сучасних умовах.

Перспективи подальших досліджень у цьому напрямку плануються в розробці адаптивної програми з загальної та спеціальної фізичної підготовки майбутніх фахівців сектору безпеки та оборони.

ЛІТЕРАТУРА:

1. Горлинський, В. В., & Ананьїн, В. О. Аналіз ключових чинників формування системи компетентностей фахівців у галузі кібербезпеки. *Information Technology and Security*, 2021, 9(2), 219–227. https://doi.org/10.20535/2411-1031.2021.9.2.249976.

2. Міністерство оборони України. Що таке система DELTA і як вона задає тренди для країн НАТО? [Електронний ресурс]. 30.03.2024. Дата звернення: 24.05.2025.

3. Президент України. Указ № 447/2021 «Про Стратегію кібербезпеки України» [Електронний ресурс]. Київ, 14.05.2021. Дата звернення: 24.05.2025.

4. Федоренко, О. І. Використання інформаційних технологій освіти у підготовці фахівців сектору безпеки і охорони України. *Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України* : тези XI Всеукр. наук.-практ. конф. 2018. С. 506–508. Хмельницький : Вид-во НАДПСУ.

5. Чопа, Д. А., Дерев'янчук, А. Й., & Козир, Н. М. Основні інноваційні напрями застосування сучасних інформаційних технологій у підготовці військових фахівців. *Сучасні інформаційні технології у сфері безпеки та оборони*, 2019, 36(3), 127–134. https://doi.org/10.33099/2311-7249/2019-36-3-127-134

6. Ситник, Г. П., & Орел, М. Г. Національна безпека в контексті інформаційно-комунікаційних технологій. *Освіта і наука у сфері національної безпеки: проблеми та перспективи розвитку.* 2024. С. 45–58. Донецьк : ДонДУВС.

7. Сокол, В. О. (2024). Розроблення професійних стандартів для військових професій у контексті національної безпеки України. *Розроблення професійних стандартів для військових професій у контексті національної безпеки України* (с. 12–25). Харків : ХНУВС.

8. Bondar K. Ukraine's Delta: Lessons for Software-Defined Warfare [Електронний ресурс]. Washington (D.C.) : CSIS, 2024. Дата звернення: 24.05.2025.

9. Davydiuk P., Potii O. National Cybersecurity Governance: Ukraine [Електронний ресурс]. Tallinn : NATO CCDCOE, 2024. 72 с. Дата звернення: 24.05.2025.

10. The NATO Advanced Distributed Learning Handbook [Електронний ресурс]. Norfolk (VA) : NATO ADL Initiative, 2023. 206 с. Режим доступу: електрон. дані. Дата звернення: 24.05.2025.

11. Cooperative Cyber Defence Centre of Excellence. Locked Shields 2024 exercise gathered 4000 cyber experts from 40 nations [Електронний ресурс]. 2024. Дата звернення: 24.05.2025.

12. NATO Interoperability Standards and Profiles (NISP). Vol. 3, v14 [Електронний ресурс]. Brussels : NATO, 2024. 80 с. Дата звернення: 24.05.2025.

13. Ukraine Cybersecurity Governance Assessment [Електронний ресурс]. Geneva : DCAF, 2021. 90 с. Дата звернення: 24.05.2025.

REFERENCES:

1. Horlinskyi, V. V., & Ananiin, V. O. (2021). Analiz klyuchovykh chynnykiv formuvannia systemy kompetentnostei fakhlivtsiv u haluzi kiberbezpeky [Analysis of key factors in forming competence system of cybersecurity specialists]. *Information Technology and Security*, 9(2), 219–227. https://doi.org/10.20535/2411-1031.2021.9.2.249976 [in Ukrainian].

2. Ministerstvo oborony Ukrainy. (2024, March 30). Shcho take systema DELTA i yak vona zadaie trendy dlia krain NATO? [What is the DELTA system and how does it set trends for NATO countries?] [Electronic resource]. Accessed May 24, 2025 [in Ukrainian].

3. Prezydent Ukrainy. (2021, May 14). Ukaz № 447/2021 "Pro Stratehiiu kiberbezpeky Ukrainy" [Decree No. 447/2021 "On the Cybersecurity Strategy of Ukraine"] [Electronic resource]. Accessed May 24, 2025 [in Ukrainian].

4. Fedorenko, O. I. (2018). Vykorystannia informatsiinykh tekhnolohii osvity u pidhotovtsi fakhlivtsiv sektoru bezpeky i okhorony Ukrainy [Use of information technologies in training security and defense specialists in Ukraine]. In *Osvitno-naukove zabezpechennia diialnosti skladovykh sektoru bezpeky i oborony Ukrainy*: Tezy XI Vseukr. nauk.-prakt. konf. (pp. 506–508). Khmelnytskyi: NADPSU [in Ukrainian].

5. Chopa, D. A., Derevianchuk, A. I., & Kozyr, N. M. (2019). Osnovni innovatsiini napriamy zastosuvannia suchasnykh informatsiinykh tekhnolohii u pidhotovtsi viiskovykh fakhlivtsiv [Main innovative directions of modern IT use in military training]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*, 36(3), 127–134. https://doi.org/10.33099/2311-7249/2019-36-3-127-134 [in Ukrainian].

6. Sytnyk, H. P., & Orel, M. H. (2024). Natsionalna bezpeka v konteksti informatsiino-komunikatsiinykh tekhnolohii [National securit y in the context of information and communication technologies]. In *Osvita i nauka u sferi natsionalnoi bezpeky: problemy ta perspektyvy rozvytku* (pp. 45–58). Donetsk: DonDUVS [in Ukrainian].

7. Sokol, V. O. (2024). Rozroblennia profesiinykh standartiv dlia viiskovykh profesii v konteksti natsionalnoi bezpeky Ukrainy [Development of professional standards for military professions in the context of Ukraine's national security]. In *Rozroblennia profesiinykh standartiv dlia viiskovykh profesii v konteksti natsionalnoi bezpeky Ukrainy* (pp. 12–25). Kharkiv: KNUVS [in Ukrainian].

8. Bondar, K. (2024). Ukraine's Delta: Lessons for Software-Defined Warfare [Electronic resource]. Washington, D.C.: CSIS. Accessed May 24, 2025 [in English]/

9. Davydiuk, P., & Potii, O. (2024). National Cybersecurity Governance: Ukraine [Electronic resource]. Tallinn: NATO CCDCOE. Accessed May 24, 2025 [in English].

10. NATO ADL Initiative. (2023). The NATO Advanced Distributed Learning Handbook [Electronic resource]. Norfolk, VA: NATO ADL Initiative. Accessed May 24, 2025 [in English].

11. Cooperative Cyber Defence Centre of Excellence. (2024). Locked Shields 2024 exercise gathered 4000 cyber experts from 40 nations [Electronic resource]. Accessed May 24, 2025 [in English].

12. NATO. (2024). NATO Interoperability Standards and Profiles (NISP), Vol. 3, v14 [Electronic resource]. Brussels: NATO. Accessed May 24, 2025 [in English].

13. DCAF. (2021). Ukraine Cybersecurity Governance Assessment [Electronic resource]. Geneva: DCAF. Accessed May 24, 2025 [in English].

Стаття надійшла до редакції: 22.09.2025
Прийнята до друку: 21.10.2025
Опублікована: 26.12.2025