

прийняття рішень. Наприклад, виявлення підозрілих осіб у натовпі за допомогою алгоритмів машинного навчання вже сьогодні є реальністю для багатьох країн.

Однак технологічний прогрес вимагає також відповідного оновлення нормативно-правової бази. У контексті інтеграції України до європейської спільноти особливе значення має гармонізація національного законодавства із загальноприйнятими стандартами ЄС. Це стосується не лише захисту персональних даних, а й забезпечення належного рівня прозорості у використанні біометричних технологій органами безпеки.

Таким чином, інформаційно-аналітичне забезпечення діяльності органів сектору безпеки та оборони України у поєднанні з біометричною ідентифікацією є перспективним напрямом, що сприяє підвищенню ефективності управлінських рішень, боротьбі з злочинністю та зміцненню національної безпеки. Успішна інтеграція цих технологій потребує зваженого підходу, який враховуватиме як технічні, так і правові аспекти їх використання.

Література

1. Розумний, С. М. Судова експертиза як ключовий інструмент забезпечення національної безпеки. 2024 р. URL: <https://er.dduvs.edu.ua/bitstream/123456789/13860/1/14.pdf> (дата звернення: 11.12.2024 року)
2. Негребецький, В. В. Роль цифрової трансформації органів кримінальної юстиції в підвищенні ефективності розслідування воєнних злочинів в Україні. 2022 р. URL: <http://baltijapublishing.lv/omp/index.php/bp/catalog/download/431/11491/24054-1?inline=1> (дата звернення: 11.12.2024 року)
3. Спринцева І.А. Актуальні питання криміналістичних обліків генетичних ознак людини. Молодий вчений. № 9 (85) (2020). URL: <https://molodyivchenyi.ua/index.php/journal/article/view/703/679> (дата звернення: 11.12.2024 року)

Вергун Дмитро Сергійович

курсант 2-го курсу Факультету №3 Донецького державного університету внутрішніх справ

Габорець Ольга Андріївна

доцент кафедри оперативно-розшукової діяльності та інформаційної безпеки, факультету №3 Донецького державного університету внутрішніх справ, доктор філософії, доцент

МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ОБОРОННИХ ПРОЦЕСІВ

У сучасному світі інформація відіграє вирішальну роль у всіх сферах діяльності, особливо в оборонній сфері, де своєчасне отримання, обробка та використання даних визначають успіх операцій і загальну національну безпеку. Геополітична нестабільність, зростання кіберзагроз, активізація гібридних конфліктів та поширення сучасних технологій значно ускладнюють оборонні процеси. У таких умовах модернізація інформаційного забезпечення стає не лише бажаною, а й життєво необхідною для забезпечення ефективного управління військовими структурами, швидкого реагування на загрози та захисту критично важливої інформації.

Основними стратегічними цілями модернізації інформаційного забезпечення є створення умов для оперативного доступу до актуальних даних, інтеграція сучасних технологій у всі рівні оборонних структур, посилення кібербезпеки, підвищення рівня взаємодії між суб'єктами оборони та підтримка наукових досліджень у цій сфері. Перш за все, необхідно забезпечити доступ до інформації в реальному часі, що дозволить командним центрам швидко реагувати на зміни оперативної обстановки.

У процесі модернізації інформаційного забезпечення слід зосередитися на кількох ключових напрямках. Насамперед, це розробка цифрових платформ для управління оборонними процесами, автоматизація збору та обробки даних, використання технологій штучного інтелекту для аналізу загроз та прогнозування їхніх наслідків. Особливої уваги потребує вдосконалення систем розвідки та спостереження, зокрема супутникових технологій і безпілотних літальних апаратів. Крім того, важливо інтегрувати сучасні технології в єдину екосистему, яка забезпечить ефективну взаємодію всіх елементів оборонної системи.

Оборонна реформа, яка триває в Збройних Силах України, передбачає впровадження сучасних інформаційних систем (IC), стандартів, доктрин і рекомендацій НАТО щодо управління військами, оборонними ресурсами та проведення оборонного планування. Одним із пріоритетних напрямів, направлених на підвищення ефективності оборонного планування та управління оборонними ресурсами є впровадження IC управління оборонними ресурсами (Defense Resources Management Information System–DRMIS) [2]. Метою DRMIS є забезпечення органів військового управління інформаційно-аналітичною підтримкою прийняття рішень у сфері управління оборонними ресурсами за функціональними напрямками: особовий склад, організаційна структура, оборонне планування, матеріально-технічне забезпечення, медичне забезпечення, закупівлі, майно, фінанси та бюджет, адміністративна діяльність [1, 59].

Критичним елементом соціально-економічної безпеки будь-якої країни є Національна стратегія кібербезпеки (National Cybersecurity Strategy, NCS) [3]. Саме в ній кібербезпека та інформаційна безпека визнані як одні з головних пріоритетів у протидії загрозам національній безпеці. Кібербезпека займає ключове місце серед пріоритетів, адже сучасні конфлікти все частіше переносяться у цифровий простір. Захист інформаційних систем від зовнішніх і внутрішніх загроз є важливим аспектом стратегії національної безпеки. Також необхідно створити уніфіковані стандарти для забезпечення злагодженої роботи між військовими, цивільними та міжнародними партнерами. Підтримка наукових досліджень у сфері оборонної інформатики сприятиме розробці інноваційних рішень, що дозволять випереджати супротивника у технологічній гонці. Деталізацію реалізації Стратегії кібербезпеки відображено у щорічних планах уряду, в яких з боку органів влади передбачено заходи щодо запобігання і підготовки реагування на можливі кіберінциденти у рамках створення ефективної національної системи кібербезпеки [4, 151].

У сучасному світі, де військові конфлікти та оборонні стратегії еволюціонують з надзвичайною швидкістю, критично важливою стає потреба в адаптації та трансформації системи військової освіти [5, 467]. Створення та розвиток інтегрованого інтелектуального освітнього простору (E-learning) у рамках як формальної, так і неформальної військової освіти, що базується на досягненнях сучасних цифрових технологій і глибокій інтеграції цих технологій у повсякденне життя, видається особливо актуальним [5, 472]. Таким чином, інтеграція цифрових технологій в систему військової освіти не тільки сприятиме оптимізації навчального процесу та підвищенню ефективності

управління, але й забезпечить формування необхідних компетентностей у військово-службовців, дозволяючи їм успішно адаптуватися та діяти в умовах інформаційного суспільства [5, 474].

Але слід зазначити, що процес модернізації інформаційного забезпечення супроводжується численними викликами та ризиками. Серед основних — високі фінансові витрати, необхідні для розробки і впровадження технологій, а також ризики кіберзагроз, які можуть виникати під час впровадження нових систем. Нестача кваліфікованих кадрів може стати значним бар'єром, а інертність організаційних структур уповільнити впровадження змін.

Очікуваними результатами модернізації стануть підвищення оперативності та точності управління оборонними процесами, ефективна протидія сучасним загрозам, а також зміцнення обороноздатності держави. У висновку сучасні технології дозволять скоротити час реагування, підвищити ефективність взаємодії між різними рівнями командування та сприяти інтеграції з міжнародними партнерами.

Література

1. Руденська, Г. В. (2020). Моделі та процеси життєвого циклу інформаційної системи управління оборонними ресурсами. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняхівського, 59-65.
2. Концепція інформатизації Міністерства оборони України : затв. наказом Міністра оборони України від 17.09.2014 р. No 650.
3. National Strategies. [Електронний ресурс]. Режим доступу: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx>
4. Трофименко, О. Г., Прокоп, Ю. В., Логінова, Н. І., & Задерейко, О. В. (2019). Кібербезпека України: аналіз сучасного стану. *Ukrainian Information Security Research Journal*, 21(3), 150-157.
5. Носенко, Ю. (2024). СУЧАСНІ ЦИФРОВІ ВИКЛИКИ В СИСТЕМІ ВІЙСЬКОВОЇ ОСВІТИ. *Перспективи та інновації науки*, (3 (37)).

Войтюк Олеся Романівна

здобувач вищої освіти спеціальності 126 «Інформаційні системи та технології» Львівського державного університету внутрішніх справ

Магеровська Тетяна Валеріївна

доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, кандидат фізико-математичних наук, доцент

АНАЛІЗ ДАНИХ ТА НАДАННЯ ПІДТРИМКИ В ПРОЦЕСІ ПРИЙНЯТТЯ РІШЕНЬ У ПРАКТИЧНІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Анотація. Дана стаття досліджує важливість використання сучасних аналітичних методів і технологій для підтримки прийняття рішень у роботі правоохоронних органів. Особлива увага приділяється збору, обробці та аналізу великих обсягів даних, що дозволяють підвищити ефективність оперативної діяльності, виявляти кримінальні тенденції, прогнозувати злочинність та забезпечувати безпеку громадян. Стаття також