МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління
та національної безпеки
Кафедра економічної теорії,
інтелектуальної власності та публічного
управління

Кваліфікаційна робота
на правах рукопису

БЕЗПАЛИЙ БОГДАН РОМАНОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 355.02:004.056(477)
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОКРАЩЕННЯ СТРАТЕГІЙ ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня _бакалавр_____ кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Б .Р. БЕЗПАЛИЙ
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
ВОЙТЕНКО Архип Борисович
(прізвище, ім'я, по батькові)
__кандидат наук з державного управління, професор
(науковий ступінь, вчене звання)

Житомир – 2024

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління за результатами попереднього захисту: **БЕЗПАЛИЙ Богдан Романович** допущений до захисту.

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № _____ від «___» травня 2024 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління

к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

«___» травня 2024 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **БЕЗПАЛИЙ Богдан Романович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за національною шкалою _____

Секретар ЕК

_____ _____ Настасія ПУГАЧОВА
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

АНОТАЦІЯ

БЕЗПАЛИЙ Б. Р. Впровадження інформаційних технологій для покращення стратегій воєнної безпеки України. – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 281 «Публічне управління та адміністрування» – Поліський національний університет, Житомир, 2024.

Кваліфікаційна робота присвячена дослідженню впровадження інформаційних технологій у стратегії воєнної безпеки України. У роботі аналізуються теоретичні основи використання інформаційних технологій у військовій сфері, оцінюється поточний стан інформаційної інфраструктури воєнної безпеки України, а також виявляються основні проблеми та перешкоди у використанні ІТ. Значна увага приділяється аналізу ефективності існуючих стратегій та програм щодо впровадження інформаційних технологій у воєнну безпеку. У роботі розроблено рекомендації щодо удосконалення нормативно-правової бази, запропоновано конкретні заходи та проекти для впровадження сучасних інформаційних технологій у воєнну сферу, а також розглядається створення системи моніторингу та оцінки ефективності впроваджених ІТ. Основний акцент зроблено на необхідності модернізації інформаційної інфраструктури, підвищення кваліфікації фахівців, а також забезпечення постійного моніторингу та оцінки ефективності впроваджених технологій. Реалізація запропонованих заходів сприятиме підвищенню рівня національної безпеки та ефективності військових операцій.

Ключові слова: управління, воєнна безпека, інформаційні технології, кібербезпека, стратегії безпеки, національна безпека, публічно-приватне партнерство.

SUMMARY

BEZPALYI B. Implementation of information technologies to improve Ukraine's military security strategies. – Qualification work for the degree of bachelor in specialty 281 «Public Administration and Management». Polissia National University, Zhytomyr, 2024.

The qualification work is dedicated to researching the implementation of information technologies in Ukraine's military security strategies. The work analyzes the theoretical foundations of using information technologies in the military sphere, assesses the current state of the information infrastructure of Ukraine's military security, and identifies the main problems and obstacles in the use of IT. Significant attention is paid to analyzing the effectiveness of existing strategies and programs for the implementation of information technologies in military security.

The work develops recommendations for improving the legal framework, proposes specific measures and projects for implementing modern information technologies in the military sphere, and considers creating a system for monitoring and evaluating the effectiveness of implemented IT. The main focus is on the necessity of modernizing the information infrastructure, enhancing the qualifications of specialists, and ensuring constant monitoring and evaluation of the effectiveness of the implemented technologies. The implementation of the proposed measures will contribute to increasing national security and the effectiveness of military operations.

Keywords: management, military security, information technologies, cybersecurity, security strategies, national security, public-private partnership.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Сучасні загрози національній безпеці України вимагають ефективного використання новітніх технологій у всіх аспектах воєнної безпеки. Інформаційні технології, які стрімко розвиваються, можуть суттєво підвищити рівень захисту та оперативність реагування на різноманітні виклики та загрози. Особливо важливо це в умовах постійної гібридної війни та кібератак, які потребують нових підходів до захисту інформаційних систем та інфраструктури.

Актуальність роботи також підкреслюється необхідністю модернізації наявних стратегій та підходів до забезпечення воєнної безпеки. Впровадження інформаційних технологій є ключовим фактором у створенні інтегрованої та адаптивної системи воєнної безпеки, яка зможе оперативно реагувати на нові загрози. Дослідження і аналіз існуючих стратегій, а також розробка нових підходів і рекомендацій, сприятимуть підвищенню ефективності оборонних заходів та зміцненню національної безпеки України.

Крім того, дослідження впровадження інформаційних технологій у воєнну безпеку України має важливе значення для покращення співпраці між державними структурами та приватним сектором, що дозволить ефективніше використовувати наявні ресурси та інноваційні рішення для забезпечення безпеки. Таким чином, актуальність цієї роботи обумовлена необхідністю адаптації воєнної стратегії до сучасних викликів та можливостей, які надають інформаційні технології.

Ефективність існуючих стратегій та програм щодо впровадження ІТ у воєнну безпеку аналізують В. Гаврилюк, М. Ломако та інші. Вони оцінюють результати реалізації національних програм розвитку оборонно-промислового комплексу та стратегії кібербезпеки, виявляючи їх сильні та слабкі сторони. Рекомендації щодо удосконалення нормативно-правової бази, конкретні заходи та проекти для впровадження сучасних інформаційних технологій у воєнну сферу, розглядаються в працях Р. Нестерова, О. Василенко та інших. Вони

пропонують конкретні кроки для підвищення ефективності використання ІТ у військових операціях, включаючи розвиток публічно-приватного партнерства, підвищення кваліфікації фахівців, створення систем моніторингу та оцінки впроваджених технологій. Таким чином, аналіз літератури показує, що впровадження інформаційних технологій у стратегії воєнної безпеки України є надзвичайно актуальним і багатогранним завданням. Незважаючи на наявні проблеми та перешкоди, дослідники відзначають великий потенціал інформаційних технологій для підвищення рівня національної безпеки та ефективності військових операцій.

Мета і завдання дослідження є аналіз існуючих стратегій та програм впровадження інформаційних технологій у стратегії воєнної безпеки України, а також розробка рекомендацій щодо вдосконалення нормативно-правової бази та впровадження конкретних заходів і проектів для підвищення ефективності використання ІТ у воєнній сфері.

Реалізація заявленої мети дослідження вимагає розв’язання таких *завдань:*

- дослідити теоретичні основи використання інформаційних технологій у воєнній безпеці;
- проаналізувати сучасний стан і проблеми впровадження інформаційних технологій у стратегії воєнної безпеки України;
- запропонувати напрями вдосконалення впровадження інформаційних технологій для покращення стратегій воєнної безпеки України.

Об'єктом дослідження є процес впровадження інформаційних технологій у стратегії воєнної безпеки України.

Предметом дослідження є конкретні інформаційні технології, їхні властивості, можливості та ефективність у контексті забезпечення воєнної безпеки України.

Методи дослідження (із зазначенням конкретного застосування кожного методу). У даній роботі застосовуються наступні методи дослідження: аналіз та синтез (аналіз літературних джерел, нормативно-

правових актів, стратегічних документів та програм, що стосуються впровадження інформаційних технологій у воєнну безпеку; синтез отриманої інформації для формування загального уявлення про поточний стан і проблеми впровадження ІТ у воєнну безпеку України). Порівняльний аналіз (порівняння міжнародного досвіду впровадження інформаційних технологій у воєнну сферу з українськими реаліями; виявлення сильних та слабких сторін існуючих стратегій та програм в Україні в порівнянні з іншими країнами). Прогностичний метод (прогнозування можливих результатів та ефектів від впровадження запропонованих заходів та проектів; оцінка перспектив розвитку інформаційної інфраструктури воєнної безпеки України).

Перелік публікацій автора за темою дослідження. Результати дослідження публікувались на конференціях поліського національного університету.

Практичне значення отриманих результатів полягає у можливості використання розроблених рекомендацій, заходів та проектів для вдосконалення стратегій воєнної безпеки України. Запропоновані рекомендації щодо удосконалення нормативно-правової бази, конкретні заходи з впровадження сучасних інформаційних технологій, а також система моніторингу та оцінки ефективності можуть бути впроваджені на рівні Міністерства оборони України та інших відповідних органів державної влади. Це сприятиме підвищенню рівня національної безпеки, покращенню координації дій військових підрозділів, оптимізації використання ресурсів та забезпеченню високої ефективності військових операцій.

Структура та обсяг роботи. Випускна кваліфікаційна робота містить вступ, три розділи основної частини та висновки до них, висновки та пропозиції, список використаних джерел, додатки. Основний текст роботи викладено на 45 сторінках. Список використаних джерел включає 44 найменування.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ОСНОВИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ВОЄННІЙ БЕЗПЕЦІ

1.1. Поняття та значення воєнної безпеки в сучасних умовах

На прикінкі XX століття інформація стала стратегічно важливим ресурсом для кожної країни, від ефективного використання якого залежить безпека держави та перспективи формування демократичного суспільства.

У контексті переходу суспільства від галузевого до інформаційного зростає важливість навичок ефективної навігації та роботи з постійно зростаючим потоком інформації. Можливості глобальної мережі, які активно використовуються у всіх сферах суспільного життя, базуються на інформаційних ресурсах, які є наборами даних, організованими в інформаційні системи для отримання достовірних даних у різних галузях знань та практики. Але в той же час з ростом ролі розвідки зростає важливість її захисту, що забезпечується за рахунок використання інструментів інформаційної безпеки. Особливо в умовах війни це питання набуває особливої важливості [15].

Воєнна безпека є однією з ключових складових національної безпеки держави, що охоплює захист від зовнішніх військових загроз та забезпечення стабільності в умовах можливих збройних конфліктів. Це поняття включає в себе сукупність заходів, дій та стратегій, спрямованих на захист національних інтересів, територіальної цілісності та суверенітету країни від зовнішніх агресій.

Поняття воєнної безпеки охоплює:

- здатність держави до оборони: підготовка та підтримка збройних сил у високій бойовій готовності, забезпечення їх сучасним озброєнням та технікою;

- стійкість до зовнішніх загроз: здатність ефективно реагувати на зовнішні загрози, зокрема військову агресію, тероризм та гібридні війни;

- захист критичної інфраструктури: забезпечення безпеки стратегічно

важливих об'єктів та інфраструктури, таких як енергетичні системи, транспортні мережі, комунікаційні системи тощо;

- інформаційна безпека: захист інформаційних ресурсів та систем від кібератак, інформаційного впливу та дезінформації [18].

Значення воєнної безпеки в сучасних умовах:

1. Збереження суверенітету та територіальної цілісності: воєнна безпека забезпечує захист кордонів та території держави від зовнішніх агресій, сприяючи збереженню її незалежності та суверенітету.

2. Захист громадян: гарантія безпеки населення від зовнішніх загроз та конфліктів, забезпечення їхнього права на мирне та безпечне життя.

3. Стабільність держави: підтримання внутрішньої стабільності та порядку, що є необхідним для нормального функціонування державних інституцій та економіки.

4. Міжнародний імідж: високий рівень воєнної безпеки підвищує престиж та авторитет держави на міжнародній арені, сприяючи розвитку міжнародних відносин та співпраці.

5. Запобігання конфліктам: ефективні воєнні стратегії та готовність до оборони можуть запобігати виникненню конфліктів та агресій з боку інших держав або недержавних акторів [20].

В сучасних умовах, коли технологічний прогрес значно змінив характер воєнних дій, воєнна безпека вимагає комплексного підходу та впровадження новітніх технологій. Зокрема, асиметричні загрози, такі як кібератаки, інформаційна війна, тероризм, вимагають від держави не лише традиційних військових методів, але й нових підходів до забезпечення безпеки.

Воєнна безпека сьогодні включає у себе не лише фізичний захист від зовнішніх агресій, але й захист інформаційного простору, кібербезпеку, економічну стабільність, та готовність до швидкого реагування на нові виклики та загрози. Це потребує інтеграції сучасних інформаційних технологій, системи моніторингу та аналізу, що дозволяють вчасно виявляти загрози, ефективно управляти ресурсами та забезпечувати координацію між різними структурними

підрозділами, відповідальними за національну безпеку [27].

1.2. Інформаційні технології як інструмент забезпечення воєнної безпеки

Інформаційні технології (IT) сьогодні відіграють ключову роль у забезпеченні воєнної безпеки, оскільки вони дозволяють підвищити ефективність управління військовими операціями, розвідкою, логістикою, а також забезпечують надійний захист інформаційних систем від кібератак. Використання IT у воєнній сфері є важливим елементом модернізації збройних сил і підвищення їх здатності реагувати на сучасні загрози.

1. Основні аспекти використання IT у воєнній безпеці:

Системи командування та управління (C4ISR):

- command and Control (C2): Системи командування і управління забезпечують координацію дій військових підрозділів, надають команди та забезпечують зворотний зв'язок;

- communications (C): Надійні засоби зв'язку забезпечують безперервний обмін інформацією між різними рівнями командування;

- computers (C): Використання комп'ютерних систем для обробки та аналізу даних, що дозволяє приймати обґрунтовані рішення;

- intelligence (I): Системи розвідки збирають, аналізують та поширюють інформацію про супротивника та операційну обстановку;

- surveillance and Reconnaissance (SR): Системи спостереження і розвідки забезпечують моніторинг і оцінку загроз [30].

2. Кібербезпека:

- захист інформаційних систем та мереж від кібератак, зломів та шкідливих програм;

- розробка і впровадження надійних протоколів шифрування для захисту конфіденційних даних;

- системи виявлення та реагування на кібератаки, що дозволяють швидко нейтралізувати загрози і відновити нормальне функціонування систем [11].

3. Безпілотні літальні апарати (БПЛА) та автономні системи:

- використання БПЛА для розвідки, спостереження, цілевказування та проведення операцій без залучення особового складу;

- автономні системи забезпечують виконання завдань з мінімальним втручанням людини, підвищуючи ефективність і знижуючи ризики [19].

4. Інформаційні системи логістики:

- управління логістичними процесами, включаючи постачання, транспортування, зберігання та розподіл ресурсів;

- оптимізація ланцюгів постачання для забезпечення вчасної доставки матеріальних засобів та обладнання [19].

5. Системи моделювання та симуляції:

- використання програмних засобів для моделювання військових операцій та сценаріїв, що дозволяє тренувати особовий склад і відпрацьовувати різні стратегії;

- симуляційні системи забезпечують безпечне і ефективне навчання військових кадрів [18].

6. Геоінформаційні системи (ГІС):

- використання ГІС для картографування, аналізу території та планування військових операцій;

- забезпечення точних даних про місцевість, що дозволяє приймати більш обґрунтовані рішення [20].

Переваги використання ІТ у воєнній безпеці:

- підвищення оперативності та ефективності: ІТ забезпечують швидкий обмін інформацією, що дозволяє швидше реагувати на загрози та приймати оперативні рішення;

- поліпшення координації: інтегровані системи командування та управління забезпечують узгодженість дій різних підрозділів і рівнів командування;

- зменшення людських ризиків: Використання БПЛА та автономних систем знижує ризики для особового складу, дозволяючи виконувати завдання у небезпечних умовах;

- оптимізація ресурсів: інформаційні системи логістики забезпечують ефективне управління ресурсами, що дозволяє знижувати витрати і покращувати забезпечення військових підрозділів [36].

Узагальнюючи, можна зазначити, що інтеграція інформаційних технологій у воєнну сферу є важливим кроком для підвищення обороноздатності та безпеки держави. ІТ забезпечують не лише оперативність та ефективність військових операцій, але й надійний захист від сучасних загроз, включаючи кібернетичні атаки та інформаційний вплив.

1.3. Аналіз міжнародного досвіду впровадження інформаційних технологій у сфері воєнної безпеки

Інформаційні технології відіграють ключову роль у воєнній безпеці багатьох розвинутих країн, забезпечуючи ефективне управління військовими операціями, розвідкою, логістикою та захистом інформаційних систем. Аналіз міжнародного досвіду показує, що інтеграція ІТ у воєнну сферу дозволяє значно підвищити обороноздатність та ефективність військових дій. Нижче розглянемо досвід таких країн, як США, Ізраїль та Німеччина.

США є лідером у використанні інформаційних технологій для забезпечення воєнної безпеки. Військові структури цієї країни активно використовують ІТ для підвищення ефективності бойових операцій, розвідки та кібербезпеки. C4ISR-системи: США активно використовують системи командування, управління, зв'язку, комп'ютерів, розвідки, спостереження та розвідки (C4ISR), які дозволяють координувати дії військових підрозділів у реальному часі, збирати та аналізувати розвідувальні дані, що підвищує ситуаційну обізнаність і ефективність прийняття рішень [1].

У 2009 році в США було створено Кіберкомандування (USCYBERCOM), яке відповідає за захист військових інформаційних систем та мереж від кібератак, розробку і впровадження кіберстратегій та проведення наступальних кібероперацій. США є піонером у використанні БПЛА для розвідки, спостереження та проведення точкових ударів. БПЛА, такі як MQ-9 Reaper, використовуються для збору розвідувальних даних та проведення бойових операцій без ризику для особового складу.

Ізраїль також є провідною країною у сфері застосування ІТ для забезпечення воєнної безпеки. Враховуючи складні геополітичні умови, країна постійно вдосконалює свої військові технології. Система «Залізний купол»: Це одна з найвідоміших систем ППО, яка використовує радарні технології та програмне забезпечення для виявлення та перехоплення ракет та артилерійських снарядів, що загрожують населеним пунктам. Ізраїль має розвинуту систему кібербезпеки, включаючи створення Національного кібербюро, яке координує зусилля різних відомств у захисті інформаційних систем країни від кібератак. Ізраїль активно підтримує розвиток стартапів у сфері військових технологій, що дозволяє швидко впроваджувати новітні ІТ-рішення у воєнну сферу [38].

Німеччина також активно впроваджує інформаційні технології для забезпечення своєї воєнної безпеки, орієнтуючись на модернізацію збройних сил та підвищення кібербезпеки. Німеччина створила Центр кібер-операцій (Cyber Operations Command), який відповідає за захист військових інформаційних систем, проведення кіберрозвідки та забезпечення кібербезпеки. Бундесвер активно використовує системи моделювання та симуляції для тренування військових, відпрацювання стратегій та аналізу бойових сценаріїв. Розвиток безпілотних систем: Німеччина впроваджує безпілотні літальні апарати для розвідки та спостереження, що дозволяє підвищити ефективність військових операцій та зменшити ризики для особового складу [27].

Інтеграція ІТ у військові операції: Використання C4ISR-систем, кіберкомандувань та безпілотних систем значно підвищує ефективність

військових дій, покращує ситуаційну обізнаність і забезпечує оперативне управління військовими підрозділами. Захист інформаційних систем від кібератак є ключовим елементом воєнної безпеки, що потребує розробки та впровадження надійних кіберстратегій та створення спеціалізованих підрозділів. Підтримка інновацій та розвиток новітніх технологій дозволяють швидко адаптуватися до нових загроз та забезпечувати перевагу на полі бою. Обмін досвідом і технологіями між країнами сприяє розвитку більш ефективних систем воєнної безпеки та дозволяє краще реагувати на глобальні загрози [14].

Таким чином, міжнародний досвід впровадження інформаційних технологій у воєнну безпеку демонструє важливість комплексного підходу, що включає використання сучасних технологій, кібербезпеки та інновацій для забезпечення національної безпеки та ефективного реагування на виклики сучасного світу.

ВИСНОВКИ ДО РОЗДІЛУ 1

Було розглянуто теоретичні основи використання інформаційних технологій у забезпеченні воєнної безпеки, що дозволяє зрозуміти їхнє значення та роль у сучасних умовах. Ось основні висновки:

Воєнна безпека є критичним елементом національної безпеки, який забезпечує захист країни від зовнішніх та внутрішніх загроз. У сучасних умовах, коли загрози стають все більш комплексними і різноманітними, роль інформаційних технологій у воєнній безпеці зростає.

Використання інформаційних технологій значно підвищує ефективність військових операцій та управління, забезпечуючи швидкий обмін інформацією, точну координацію дій та підвищення оперативної обізнаності. Інформаційні системи, кіберзахист, безпілотні технології та розвідувальні системи є ключовими компонентами сучасних збройних сил.

Аналіз міжнародного досвіду (США, Ізраїль, Німеччина) показує, що успішне впровадження інформаційних технологій у воєнну сферу потребує комплексного підходу, що включає інтеграцію сучасних технологій, розвиток кібербезпеки та інновацій, а також міжнародну співпрацю. Ці країни демонструють ефективність використання інформаційних технологій у військових операціях, що дозволяє досягати високих результатів і забезпечувати надійний захист національних інтересів.

Україна має враховувати успішний досвід інших країн та адаптувати його до власних умов для підвищення ефективності своєї воєнної безпеки. Це включає впровадження сучасних інформаційних систем, розвиток кібербезпеки, а також залучення міжнародних партнерів для обміну досвідом і технологіями.

Загалом, теоретичний аналіз підтверджує, що інформаційні технології є невід'ємною частиною сучасної воєнної безпеки. Вони забезпечують перевагу на полі бою, підвищують ефективність управління військовими операціями та сприяють розвитку обороноздатності держави. Використання міжнародного досвіду та інноваційних підходів дозволить Україні ефективно протистояти сучасним загрозам і забезпечити національну безпеку на високому рівні.

РОЗДІЛ 2.
СУЧАСНИЙ СТАН І ПРОБЛЕМИ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СТРАТЕГІЇ ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

2.1. Оцінка поточного стану інформаційної інфраструктури воєнної безпеки України

Оцінка поточного стану інформаційної інфраструктури воєнної безпеки України є важливим етапом для розуміння існуючих можливостей та виявлення слабких місць, які потребують вдосконалення. Інформаційна інфраструктура включає в себе технічні засоби, програмне забезпечення, системи зв'язку та управління, а також людські ресурси, які забезпечують збирання, обробку, зберігання та передачу інформації, необхідної для забезпечення національної безпеки.

Складові інформаційної інфраструктури воєнної безпеки:

1. *Технічні засоби*: системи зв'язку (радіо, супутниковий зв'язок, інтернет-мережі, захищені канали передачі даних); обчислювальні потужності (дата-центри, сервери, мережеве обладнання); засоби спостереження та розвідки (радіолокаційні станції, безпілотні літальні апарати, космічні супутники); кібербезпека: системи захисту від кібератак, антивірусне програмне забезпечення, міжмережеві екрани.

2. *Програмне забезпечення*: системи управління та командування (програми для планування операцій, контролю виконання завдань, обміну інформацією між підрозділами); аналітичні системи (програми для аналізу розвідувальної інформації, прогнозування загроз, підтримки прийняття рішень); засоби криптографії (програми для шифрування даних та захищеного зв'язку).

3. *Людські ресурси*: кваліфіковані фахівці (інженери, програмісти, аналітики, оператори систем зв'язку та розвідки); навчання та тренування (програми підготовки та підвищення кваліфікації персоналу у сфері

інформаційної безпеки та ІТ) [17].

На сьогоднішній день Україна зробила значні кроки в розвитку своєї інформаційної інфраструктури воєнної безпеки, але залишається низка викликів та проблем:

1. Технічні обмеження: незважаючи на модернізацію, значна частина обладнання залишається застарілою; обмеженість вітчизняних технологій та залежність від іноземного обладнання та програмного забезпечення.

2. Фінансові обмеження: недостатнє фінансування для закупівлі сучасних технологій та підтримки існуючих систем; високі витрати на модернізацію інфраструктури та впровадження нових технологій.

3. Кібербезпека: часті кібернапади на державні та військові об'єкти, що свідчить про необхідність посилення захисту інформаційних систем; недостатній рівень підготовки фахівців у сфері кібербезпеки.

4. Інституційні проблеми: недосконалість нормативно-правової бази, яка регулює використання інформаційних технологій у воєнній сфері; відсутність координації між різними відомствами та підрозділами, що ускладнює ефективне управління інформаційною інфраструктурою.

5. Людські ресурси: відтік кваліфікованих кадрів з військової сфери через низький рівень оплати праці та соціального забезпечення; потреба в постійному підвищенні кваліфікації та перепідготовці персоналу [28].

Оцінка поточного стану інформаційної інфраструктури воєнної безпеки України показала, що, незважаючи на значні зусилля з модернізації та впровадження нових технологій, існують суттєві проблеми, які потребують негайного вирішення. Застарілість технічних засобів, недостатнє фінансування, вразливість до кібернападів, інституційні та кадрові проблеми є основними викликами, які стоять на шляху до створення ефективної системи воєнної безпеки. Подолання цих проблем вимагатиме комплексного підходу, включаючи вдосконалення нормативно-правової бази, збільшення фінансування, посилення кібербезпеки та розвиток людських ресурсів.

2.2. Виявлення основних проблем та перешкод у використанні інформаційних технологій

Впровадження інформаційних технологій (ІТ) у сферу воєнної безпеки стикається з рядом проблем та перешкод, які впливають на ефективність використання цих технологій. Ідентифікація та розуміння цих проблем є ключовими для розробки стратегій їх подолання.

В ході дослідження виявили наступні основні проблеми та перешкоди:

1. Технічні проблеми: застаріла інфраструктура (багато компонентів інформаційної інфраструктури є застарілими і не відповідають сучасним вимогам щодо швидкості, надійності та безпеки). Інтеграційні складнощі (відсутність сумісності між новими та старими системами призводить до ускладнень у їх інтеграції та взаємодії). Обмежені можливості для модернізації (високі витрати на оновлення обладнання та програмного забезпечення, що стримує процес модернізації).

2. Фінансові перешкоди: недостатнє фінансування (обмежені бюджетні ресурси призводять до недостатнього фінансування проектів з впровадження ІТ у воєнну сферу). Непередбачуваність фінансування (нестабільне фінансування з боку держави, що ускладнює довгострокове планування та реалізацію ІТ-проєктів).

3. Кадрові проблеми: нестача кваліфікованих фахівців (відсутність достатньої кількості спеціалістів з ІТ у військовій сфері, що впливає на ефективність використання технологій). Відтік кадрів (кваліфіковані фахівці часто залишають державний сектор через низький рівень заробітної плати та кращі умови у приватному секторі).

4. Кібербезпека: високий рівень загроз (зростаюча кількість кібернападів на військові інформаційні системи, що вимагає постійного оновлення засобів захисту та вдосконалення кібербезпеки). Недостатній рівень захисту (відсутність належних заходів з кібербезпеки та недостатня увага до захисту інформаційних систем).

5. Інституційні та нормативно-правові перешкоди: недосконаліть нормативно-правової бази (відсутність чітких законодавчих актів, що регулюють використання ІТ у воєнній сфері, створює правову невизначеність та ускладнює впровадження технологій). Відсутність координації (недостатня координація між різними державними органами та військовими підрозділами у сфері ІТ).

6. Технологічна залежність: залежність від іноземних технологій (відсутність власних розробок та залежність від імпорту технологій створює ризики у випадку обмежень або санкцій з боку інших держав). Обмежений доступ до сучасних технологій (через міжнародні санкції та обмеження Україна має обмежений доступ до деяких сучасних технологій, що ускладнює модернізацію інформаційної інфраструктури) [35].

Наведемо приклади конкретних проблем:

1. Застаріле обладнання та програмне забезпечення: багато військових систем використовують застаріле обладнання, яке не підтримується виробниками, що ускладнює їх обслуговування та модернізацію. Використання старих версій програмного забезпечення, які вразливі до кібернападів та не відповідають сучасним вимогам безпеки.

2. Відсутність інтегрованих систем: різні військові підрозділи використовують несумісні системи, що ускладнює обмін інформацією та координацію дій. Відсутність єдиної платформи для управління військовими операціями, що призводить до втрат інформації та затримок у прийнятті рішень.

3. Фінансові обмеження: недостатнє фінансування проектів з модернізації інформаційних систем та впровадження нових технологій. Непередбачуваність фінансування, що ускладнює планування довгострокових проектів та призводить до їх затримок або відмови від реалізації.

Виявлення основних проблем та перешкод у використанні інформаційних технологій у воєнній безпеці України показує, що для ефективного впровадження ІТ необхідно вирішити низку технічних, фінансових, кадрових,

кібербезпекових та інституційних проблем. Подолання цих перешкод вимагатиме комплексного підходу, який включатиме модернізацію обладнання, збільшення фінансування, розвиток людських ресурсів, посилення кібербезпеки та вдосконалення нормативно-правової бази. Це дозволить створити ефективну та сучасну інформаційну інфраструктуру, яка забезпечить високу рівень воєнної безпеки України.

2.3. Аналіз ефективності існуючих стратегій та програм щодо впровадження ІТ у сфері воєнної безпеки

Аналіз ефективності існуючих стратегій та програм щодо впровадження інформаційних технологій (ІТ) у воєнну безпеку України є важливим етапом для розуміння їх дієвості та визначення напрямків для подальшого вдосконалення. Існуючі стратегії та програми:

1. Стратегія кібербезпеки України: метою цієї стратегії є забезпечення національної безпеки в кіберпросторі шляхом створення ефективної системи кіберзахисту, здатної протидіяти сучасним кіберзагрозам. Включає заходи щодо підвищення кібергігієни, розвиток національних кіберспроможностей, посилення співпраці з міжнародними партнерами. Основні завдання: створення та розвиток національної системи кібербезпеки; запобігання, виявлення та реагування на кіберзагрози; підвищення рівня кібергігієни серед громадян та організацій; розвиток національних кіберспроможностей та кадрового потенціалу; посилення міжнародної співпраці у сфері кібербезпеки [28].

Можемо виділити такі ключові компоненти: технічна інфраструктура (впровадження сучасних технологій для моніторингу та захисту від кіберзагроз); освітні програми (підготовка спеціалістів у галузі кібербезпеки, підвищення рівня обізнаності населення); нормативно-правова база (розробка та вдосконалення законодавства, що регулює питання кібербезпеки);

міжнародна співпраця: Участь у глобальних ініціативах, обмін досвідом та технологіями з іншими країнами [28].

Від впровадження стратегіє результати та досягнення: покращення захищеності критичної інформаційної інфраструктури; зменшення кількості успішних кібератак на державні установи та стратегічні об’єкти; підвищення рівня обізнаності населення про основи кібергігієни [28].

2. *Національна програма розвитку оборонно-промислового комплексу України:п*ередбачає модернізацію оборонних підприємств та впровадження сучасних ІТ-технологій для підвищення їх продуктивності та ефективності. Зокрема, акцентується на розробці та впровадженні новітніх військових технологій, включаючи засоби зв'язку, управління та розвідки. Основні завдання: модернізація виробничих потужностей ОПК; впровадження сучасних інформаційних технологій у виробничі процеси; розробка та виробництво нових видів озброєнь та військової техніки; зміцнення науково-технічного потенціалу оборонної промисловості; підвищення конкурентоспроможності української оборонної продукції на міжнародному ринку [29].

Можемо виділити такі ключові компоненти: інвестиції у виробництво (вкладання коштів у модернізацію підприємств, закупівля новітнього обладнання); наукові дослідження та розробки (підтримка наукових установ, проведення досліджень для створення інноваційних технологій); міжнародна кооперація (співпраця з іноземними партнерами для обміну технологіями та досвідом) [29].

Результати та досягнення: оновлення виробничих потужностей, впровадження сучасних технологій; розробка та виготовлення нових зразків озброєнь, що відповідають міжнародним стандартам; збільшення експорту української оборонної продукції [29].

3. *Стратегія розвитку інформаційного суспільства в Україні*: направлена на розвиток інформаційної інфраструктури, що включає і військову сферу. Стимулює впровадження новітніх інформаційних технологій у різні сектори, включаючи оборонний. Основні завдання: розвиток інформаційної

інфраструктури; підвищення доступності ІКТ для всіх верств населення; вдосконалення системи освіти для підготовки кадрів у сфері ІКТ; стимулювання впровадження ІКТ у різні сектори економіки та державного управління; забезпечення кібербезпеки та захисту інформаційних ресурсів [30].

Ключові компоненти: інфраструктура (розбудова мережі високошвидкісного Інтернету, забезпечення доступу до ІКТ у віддалених районах); освіта та кадри (розробка освітніх програм для підготовки спеціалістів у сфері ІКТ, підвищення рівня цифрової грамотності населення); електронне урядування (впровадження електронних послуг для громадян та бізнесу, розвиток системи електронного документообігу); інновації та стартами (підтримка інноваційних проектів, створення умов для розвитку стартапів у сфері ІКТ) [30] .

Результати та досягнення: збільшення рівня доступу населення до ІКТ; підвищення якості освіти у сфері ІКТ, збільшення кількості кваліфікованих спеціалістів; впровадження електронних послуг, що спрощують взаємодію громадян з державою; підтримка інноваційних проектів, розвиток стартап-екосистеми.

Кожна з цих стратегій та програм є важливою складовою національної безпеки та розвитку України, сприяючи зміцненню обороноздатності, покращенню кібербезпеки та розвитку інформаційного суспільства.

Можемо навести основні аспекти аналізу ефективності:

1. *Позитивні аспекти* – покращення кібербезпеки (реалізація стратегії кібербезпеки сприяла покращенню захисту критичної інформаційної інфраструктури. Військові об’єкти стали більш захищеними від кібератак). Модернізація військових технологій (національна програма розвитку оборонно-промислового комплексу дозволила оновити частину військових технологій та інтегрувати сучасні ІТ-рішення у військову сферу). Міжнародна співпраця (підвищилася ефективність співпраці з міжнародними партнерами у сфері кібербезпеки та обміну досвідом).

2. *Недоліки та проблеми – н*едостатнє фінансування (багато проєктів

стикаються з фінансовими обмеженнями, що уповільнює їх реалізацію або робить її неможливою). Кадрові обмеження (недостатня кількість кваліфікованих спеціалістів у сфері ІТ та кібербезпеки у військовому секторі). Технологічна відсталість (відсутність доступу до деяких сучасних технологій через міжнародні санкції та обмеження).

3. *Конкретні результати та досягнення* – впровадження нових систем зв'язку (завдяки реалізації програм модернізації, було впроваджено нові системи захищеного зв'язку, що підвищило оперативність та безпеку військових операцій). Покращення інформаційного забезпечення (створення інформаційних платформ для управління військовими операціями, що дозволило покращити координацію дій та прийняття рішень). Навчання та підготовка кадрів (запроваджено програми навчання та підготовки кадрів у сфері кібербезпеки, що підвищило рівень знань та навичок військових спеціалістів).

Для оцінки ефективності існуючих стратегій та програм можна використовувати такі критерії:

1. Рівень реалізації: відсоток реалізованих проектів та заходів від запланованих.

2. Покращення безпеки: зменшення кількості успішних кібернападів та інцидентів у військовій сфері.

3. Економічна ефективність: відношення витрат на впровадження ІТ до досягнутих результатів.

4. Кадровий потенціал: збільшення кількості кваліфікованих фахівців у сфері ІТ та кібербезпеки.

5. Технологічний рівень: підвищення рівня технологічної оснащеності військових підрозділів [23].

Аналіз ефективності існуючих стратегій та програм щодо впровадження ІТ у воєнну безпеку показує, що, незважаючи на певні успіхи, існують значні проблеми та перешкоди, які впливають на їхню дієвість. Основними недоліками є недостатнє фінансування, кадрові обмеження та технологічна

відсталість. Для підвищення ефективності необхідно збільшити фінансування, розвивати кадровий потенціал, активніше впроваджувати сучасні технології та вдосконалювати нормативно-правову базу. Лише комплексний підхід дозволить створити ефективну та сучасну систему воєнної безпеки України.

Цей аналіз демонструє, як Україна працює над вдосконаленням інформаційних технологій у воєнній сфері, але також відзначає важливість подальшого розвитку і вдосконалення стратегій для забезпечення національної безпеки.

ВИСНОВКИ ДО РОЗДІЛУ 2

В розділі біло проаналізовано поточний стан і проблеми впровадження інформаційних технологій (ІТ) у стратегії воєнної безпеки України. Дослідження показує, що впровадження ІТ у військову сферу є актуальним напрямом, однак існують значні виклики, які потребують уваги та вирішення.

Згідно з проведеною оцінкою, інформаційна інфраструктура воєнної безпеки України відзначається певними досягненнями у сфері кіберзахисту та комунікаційних технологій. Однак існують недоліки у відстеженні та захисті від сучасних кіберзагроз, що потребує подальшого удосконалення інфраструктури.

Основними проблемами впровадження ІТ у військову безпеку України є недостатня координація між різними військовими відомствами, складність інтеграції новітніх технологій через відсутність стандартизації та високі витрати на модернізацію.

Стратегії та програми, спрямовані на вдосконалення ІТ-інфраструктури воєнної безпеки, показують певні досягнення, зокрема у напрямку кібербезпеки та модернізації телекомунікаційних систем. Проте вони потребують систематичної оцінки та адаптації до сучасних загроз і технологічних вимог.

Загальний висновок полягає в тому, що впровадження інформаційних

технологій у стратегію воєнної безпеки України є необхідним і перспективним напрямком, який вимагає комплексного підходу та уваги до всіх аспектів, від кіберзахисту до модернізації інфраструктури. Для досягнення успіху необхідне подальше вдосконалення стратегій, підвищення координації та інтеграції з міжнародними партнерами, що сприятиме забезпеченню національної безпеки в умовах сучасних глобальних загроз.

РОЗДІЛ 3.
НАПРЯМИ ВДОСКОНАЛЕННЯ ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПОКРАЩЕННЯ СТРАТЕГІЙ ВОЄННОЇ БЕЗПЕКИ УКРАЇНИ

3.1. Розробка рекомендацій щодо удосконалення нормативно-правової бази

Для забезпечення ефективного впровадження та використання інформаційних технологій у воєнній сфері необхідно створити належну нормативно-правову базу. Це дозволить не лише регулювати процеси, пов'язані з ІТ, але й забезпечити захист інформації та сприяти розвитку технологічних інновацій. Розглянемо основні рекомендації щодо удосконалення нормативно-правової бази.

Рекомендації, щодо оновлення та розширення законодавства у сфері кібербезпеки: прийняття нових законів та вдосконалення існуючих, що регулюють питання кібербезпеки, з урахуванням сучасних загроз та технологій; впровадження чітких вимог до захисту інформаційних систем та даних у державних установах та приватних компаніях, що співпрацюють з оборонним сектором; запровадження обов'язкових стандартів безпеки для всіх критичних інформаційних інфраструктур; створення механізмів для швидкого реагування на кіберінциденти та координації дій між державними органами та приватним сектором [38].

Рекомендації, щодо розробки нормативно-правових актів для стимулювання інновацій у воєнній сфері: створення правових умов для підтримки досліджень і розробок у сфері інформаційних технологій для оборони; запровадження механізмів державного фінансування та грантів для інноваційних проектів у галузі оборонних технологій; надання податкових пільг для підприємств, що займаються розробкою та впровадженням нових інформаційних технологій у воєнній сфері; встановлення процедур для

швидкого патентування та ліцензування новітніх технологій [34].

Рекомендації, щодо регулювання взаємодії між державними структурами та приватним сектором: впровадження прозорих механізмів державно-приватного партнерства для розвитку та впровадження інформаційних технологій у військовій сфері; розробка нормативно-правових актів, що забезпечують захист комерційної таємниці та інтелектуальної власності у співпраці з державою; встановлення чітких правил для обміну інформацією між державними органами та приватними компаніями, що співпрацюють у сфері оборони; розробка стандартів для інтеграції технологічних рішень, що пропонуються приватним сектором, у державні інформаційні системи [31].

Рекомендації, щодо вдосконалення системи підготовки та сертифікації кадрів: розробка нормативних актів, що встановлюють вимоги до підготовки та сертифікації фахівців у сфері інформаційної безпеки; запровадження програм підвищення кваліфікації для військових і цивільних фахівців у галузі інформаційних технологій; створення умов для участі українських фахівців у міжнародних програмах та навчаннях з кібербезпеки та IT [28].

Рекомендації, щодо міжнародна співпраця та гармонізація законодавства: гармонізація національного законодавства з міжнародними стандартами у сфері кібербезпеки та інформаційних технологій; розробка угод про співпрацю з іншими країнами та міжнародними організаціями у сфері інформаційної безпеки; впровадження механізмів для участі у міжнародних програмах обміну інформацією та досвідом у сфері кібербезпеки [27].

Удосконалення нормативно-правової бази є ключовим елементом для ефективного впровадження інформаційних технологій у воєнну сферу. Це дозволить не лише забезпечити правову підтримку технологічних ініціатив, але й створити сприятливі умови для розвитку інновацій та захисту інформаційної інфраструктури країни. Реалізація запропонованих рекомендацій сприятиме зміцненню національної безпеки та підвищенню обороноздатності України.

3.2. Впровадження сучасних інформаційних технологій у воєнну сферу: конкретні заходи та проєкти

Для забезпечення ефективності та надійності воєнної безпеки України важливо активно впроваджувати сучасні інформаційні технології у різні аспекти військової діяльності. Ці технології можуть значно підвищити оперативність, точність та безпеку військових операцій. Розглянемо конкретні заходи та проекти, які можуть бути реалізовані для вдосконалення воєнної сфери.

Створення єдиної інформаційно-комунікаційної платформи для Збройних Сил України: забезпечити інтеграцію всіх інформаційних потоків та комунікаційних засобів для підвищення ефективності управління військовими операціями. Конкретні заходи: розробка та впровадження єдиної платформи для обміну інформацією між різними підрозділами Збройних Сил України; встановлення захищених каналів зв’язку для оперативного обміну інформацією; інтеграція платформи з існуючими системами управління та контролю [14].

Впровадження системи кіберзахисту військових інформаційних ресурсів забезпечити захист військових інформаційних систем та мереж від кіберзагроз. Конкретні заходи: встановлення багаторівневої системи кіберзахисту, включаючи засоби виявлення та запобігання вторгненням; розробка та впровадження політик безпеки для захисту інформаційних систем; підготовка та навчання спеціалістів з кібербезпеки для забезпечення постійного моніторингу та реагування на кіберінциденти [24].

Використання технологій штучного інтелекту та машинного навчання підвищення ефективності аналізу та прийняття рішень у військовій сфері. Конкретні заходи: розробка та впровадження систем аналізу великих даних для прогнозування загроз та планування операцій; використання штучного інтелекту для автоматизації процесів виявлення та класифікації об’єктів на полі бою; інтеграція технологій машинного навчання для аналізу розвідувальної

інформації та підтримки прийняття рішень [14].

Розробка та впровадження безпілотних літальних апаратів (БПЛА): забезпечення розвідувальних операцій та моніторингу в реальному часі. Конкретні заходи: виробництво та закупівля сучасних безпілотних літальних апаратів для військових цілей; розробка систем управління БПЛА та інтеграція їх у загальну систему командування та контролю; підготовка операторів для ефективного управління та використання БПЛА [18].

Впровадження системи супутникового зв'язку та спостереження: забезпечити надійний зв'язок та спостереження за будь-яких умов. Конкретні заходи: запуск власних військових супутників для забезпечення незалежності від зовнішніх постачальників; інтеграція супутникових систем з наземними та повітряними підрозділами для забезпечення комплексного спостереження; розробка системи передачі даних в режимі реального часу для оперативного реагування на загрози [20].

Впровадження мобільних командних центрів: забезпечити мобільність та оперативність управління військовими операціями. Конкретні заходи: розробка та оснащення мобільних командних центрів з сучасними засобами зв'язку та управління; інтеграція мобільних центрів у загальну систему командування для забезпечення координації дій у різних умовах; підготовка особового складу для ефективного використання мобільних командних центрів [23].

Створення національної мережі центрів кібербезпеки: забезпечити координацію та швидке реагування на кіберзагрози на національному рівні. Конкретні заходи: відкриття регіональних центрів кібербезпеки для моніторингу та реагування на інциденти; забезпечення центрів сучасними технологіями для аналізу та нейтралізації кіберзагроз; підготовка фахівців з кібербезпеки для роботи у центрах та забезпечення їх постійного підвищення кваліфікації [18].

Впровадження сучасних інформаційних технологій у воєнну сферу є ключовим елементом для підвищення обороноздатності України. Реалізація зазначених заходів та проектів сприятиме підвищенню ефективності управління

військовими операціями, забезпечить надійний захист інформаційних систем та створить умови для швидкого реагування на загрози. Це дозволить Україні бути на крок попереду у технологічному розвитку та забезпечити високий рівень воєнної безпеки.

3.3. Створення системи моніторингу та оцінки ефективності впроваджених інформаційних технологій

Для забезпечення постійного підвищення ефективності впроваджених інформаційних технологій у сфері воєнної безпеки, необхідно створити систему моніторингу та оцінки цих технологій. Це дозволить своєчасно виявляти недоліки, коригувати стратегії та забезпечити максимальну результативність використання ІТ-рішень.

Головною метою створення системи моніторингу та оцінки є забезпечення безперервного контролю за станом та результативністю впроваджених інформаційних технологій, що дозволить оперативно реагувати на зміни та вдосконалювати існуючі процеси [8].

Основні компоненти системи моніторингу та оцінки:

1. Автоматизовані системи збору та аналізу даних: впровадження автоматизованих систем для збору даних з різних джерел, включаючи мережеву інфраструктуру, системи управління та контролю. Використання технологій штучного інтелекту та машинного навчання для аналізу зібраних даних та виявлення аномалій.

2. Інтеграція з існуючими системами: інтеграція системи моніторингу з наявними системами управління та контролю для забезпечення комплексного підходу до оцінки ефективності. Використання єдиних стандартів та протоколів для забезпечення сумісності різних компонентів системи.

3. Розробка індикаторів ефективності (KPI): визначення ключових показників ефективності для оцінки впроваджених інформаційних технологій.

Регулярний перегляд та оновлення KPI відповідно до змін у воєнній доктрині та технологічному середовищі.

4. Побудова системи звітності: створення механізмів для регулярного формування звітів про стан та ефективність використання інформаційних технологій. Використання візуалізацій та дашбордів для зручного відображення результатів моніторингу.

5. Навчання та підготовка персоналу: проведення тренінгів та навчальних курсів для підготовки персоналу до роботи з системами моніторингу та оцінки.

Забезпечення постійного підвищення кваліфікації працівників для ефективного використання нових технологій.

Процедури та методи моніторингу

Постійний моніторинг: організація цілодобового моніторингу критичних систем та мереж для виявлення потенційних загроз та порушень. Використання інструментів реального часу для аналізу трафіку та виявлення підозрілої активності.

Регулярні аудити та оцінки: проведення регулярних аудитів інформаційних систем та інфраструктури для оцінки їхньої відповідності встановленим стандартам та вимогам. Використання зовнішніх аудиторів для забезпечення незалежної оцінки ефективності.

Тестування та симуляції: проведення регулярних тестів на проникнення для виявлення вразливостей та перевірки готовності до кібератак. Використання симуляційних вправ для перевірки готовності персоналу до реагування на інциденти.

Оцінка ефективності від запроваджених заходів:

Аналіз даних: використання зібраних даних для аналізу ефективності впроваджених технологій та визначення їхнього впливу на воєнну безпеку. Порівняння фактичних результатів з встановленими KPI та виявлення відхилень.

Зворотний зв'язок: отримання зворотного зв'язку від користувачів інформаційних систем для виявлення проблем та недоліків. Використання

опитувань та анкетування для збору даних про задоволеність користувачів та їхні пропозиції щодо вдосконалення.

Коригувальні заходи: розробка та впровадження коригувальних заходів на основі результатів моніторингу та оцінки. Постійне вдосконалення системи моніторингу для забезпечення максимальної ефективності.

Створення системи моніторингу та оцінки ефективності впроваджених інформаційних технологій є критично важливим для забезпечення високого рівня воєнної безпеки України. Така система дозволить вчасно виявляти та усувати недоліки, оптимізувати використання ресурсів та забезпечити постійне вдосконалення ІТ-рішень. Реалізація запропонованих заходів сприятиме підвищенню надійності та ефективності військових операцій, що в кінцевому результаті зміцнить обороноздатність країни.

ВИСНОВКИ ДО РОЗДІЛУ 3

У даному розділі було розглянуто напрями вдосконалення впровадження інформаційних технологій для покращення стратегій воєнної безпеки України. На основі проведеного аналізу зроблено такі висновки:

Нормативно-правова база є основою для ефективного використання інформаційних технологій у воєнній сфері. Запропоновано удосконалити законодавство шляхом впровадження нових законодавчих актів, що регулюють кібербезпеку та інформаційну інфраструктуру. Це включає розробку нових стандартів, протоколів та процедур для захисту інформаційних систем від кіберзагроз.

Важливим є гармонізація національного законодавства з міжнародними стандартами та практиками, що сприятиме підвищенню рівня кібербезпеки та інтеграції України у світову систему безпеки.

Запропоновано конкретні заходи для впровадження сучасних інформаційних технологій у воєнну сферу. Це включає модернізацію існуючої

інфраструктури, впровадження нових систем управління та контролю, використання технологій штучного інтелекту та машинного навчання для аналізу даних та прийняття рішень.

Впровадження проектів, спрямованих на покращення кібербезпеки, таких як створення спеціалізованих центрів кібербезпеки, розробка навчальних програм для підготовки фахівців з кібербезпеки та підвищення їхньої кваліфікації.

Розробка та впровадження системи моніторингу та оцінки ефективності є критично важливим кроком для забезпечення постійного підвищення ефективності використання інформаційних технологій. Це включає впровадження автоматизованих систем збору та аналізу даних, розробку індикаторів ефективності (KPI), побудову системи звітності та проведення регулярних аудитів.

Система моніторингу дозволить оперативно реагувати на виявлені проблеми та коригувати стратегії, що сприятиме підвищенню надійності та результативності військових операцій.

Загалом, реалізація запропонованих заходів сприятиме підвищенню рівня воєнної безпеки України шляхом вдосконалення використання інформаційних технологій. Важливими аспектами є вдосконалення нормативно-правової бази, впровадження сучасних технологій та створення ефективної системи моніторингу. Це дозволить Україні бути краще підготовленою до сучасних викликів та загроз у воєнній сфері.

ВИСНОВКИ

У ході дослідження було розглянуто теоретичні та практичні аспекти впровадження інформаційних технологій у стратегії воєнної безпеки України. На основі проведеного аналізу та досліджень зроблено наступні загальні висновки:

Було розглянуто теоретичні основи використання інформаційних технологій у забезпеченні воєнної безпеки, що дозволяє зрозуміти їхнє значення та роль у сучасних умовах. Ось основні висновки:

Воєнна безпека є критичним елементом національної безпеки, який забезпечує захист країни від зовнішніх та внутрішніх загроз. У сучасних умовах, коли загрози стають все більш комплексними і різноманітними, роль інформаційних технологій у воєнній безпеці зростає.

Використання інформаційних технологій значно підвищує ефективність військових операцій та управління, забезпечуючи швидкий обмін інформацією, точну координацію дій та підвищення оперативної обізнаності. Інформаційні системи, кіберзахист, безпілотні технології та розвідувальні системи є ключовими компонентами сучасних збройних сил.

Аналіз міжнародного досвіду (США, Ізраїль, Німеччина) показує, що успішне впровадження інформаційних технологій у воєнну сферу потребує комплексного підходу, що включає інтеграцію сучасних технологій, розвиток кібербезпеки та інновацій, а також міжнародну співпрацю. Ці країни демонструють ефективність використання інформаційних технологій у військових операціях, що дозволяє досягати високих результатів і забезпечувати надійний захист національних інтересів.

Україна має враховувати успішний досвід інших країн та адаптувати його до власних умов для підвищення ефективності своєї воєнної безпеки. Це включає впровадження сучасних інформаційних систем, розвиток кібербезпеки, а також залучення міжнародних партнерів для обміну досвідом і технологіями.

Загалом, теоретичний аналіз підтверджує, що інформаційні технології є

невід'ємною частиною сучасної воєнної безпеки. Вони забезпечують перевагу на полі бою, підвищують ефективність управління військовими операціями та сприяють розвитку обороноздатності держави. Використання міжнародного досвіду та інноваційних підходів дозволить Україні ефективно протистояти сучасним загрозам і забезпечити національну безпеку на високому рівні.

Згідно з проведеною оцінкою, інформаційна інфраструктура воєнної безпеки України відзначається певними досягненнями у сфері кіберзахисту та комунікаційних технологій. Однак існують недоліки у відстеженні та захисті від сучасних кіберзагроз, що потребує подальшого удосконалення інфраструктури.

Основними проблемами впровадження ІТ у військову безпеку України є недостатня координація між різними військовими відомствами, складність інтеграції новітніх технологій через відсутність стандартизації та високі витрати на модернізацію.

Стратегії та програми, спрямовані на вдосконалення ІТ-інфраструктури воєнної безпеки, показують певні досягнення, зокрема у напрямку кібербезпеки та модернізації телекомунікаційних систем. Проте вони потребують систематичної оцінки та адаптації до сучасних загроз і технологічних вимог.

Загальний висновок полягає в тому, що впровадження інформаційних технологій у стратегію воєнної безпеки України є необхідним і перспективним напрямком, який вимагає комплексного підходу та уваги до всіх аспектів, від кіберзахисту до модернізації інфраструктури. Для досягнення успіху необхідне подальше вдосконалення стратегій, підвищення координації та інтеграції з міжнародними партнерами, що сприятиме забезпеченню національної безпеки в умовах сучасних глобальних загроз.

Нормативно-правова база є основою для ефективного використання інформаційних технологій у воєнній сфері. Запропоновано удосконалити законодавство шляхом впровадження нових законодавчих актів, що регулюють кібербезпеку та інформаційну інфраструктуру. Це включає розробку нових стандартів, протоколів та процедур для захисту інформаційних систем від

кіберзагроз.

Важливим є гармонізація національного законодавства з міжнародними стандартами та практиками, що сприятиме підвищенню рівня кібербезпеки та інтеграції України у світову систему безпеки.

Запропоновано конкретні заходи для впровадження сучасних інформаційних технологій у воєнну сферу. Це включає модернізацію існуючої інфраструктури, впровадження нових систем управління та контролю, використання технологій штучного інтелекту та машинного навчання для аналізу даних та прийняття рішень.

Впровадження проєктів, спрямованих на покращення кібербезпеки, таких як створення спеціалізованих центрів кібербезпеки, розробка навчальних програм для підготовки фахівців з кібербезпеки та підвищення їхньої кваліфікації.

Розробка та впровадження системи моніторингу та оцінки ефективності є критично важливим кроком для забезпечення постійного підвищення ефективності використання інформаційних технологій. Це включає впровадження автоматизованих систем збору та аналізу даних, розробку індикаторів ефективності (KPI), побудову системи звітності та проведення регулярних аудитів.

Система моніторингу дозволить оперативно реагувати на виявлені проблеми та коригувати стратегії, що сприятиме підвищенню надійності та результативності військових операцій.

Загалом, реалізація запропонованих заходів сприятиме підвищенню рівня воєнної безпеки України шляхом вдосконалення використання інформаційних технологій. Важливими аспектами є вдосконалення нормативно-правової бази, впровадження сучасних технологій та створення ефективної системи моніторингу. Це дозволить Україні бути краще підготовленою до сучасних викликів та загроз у воєнній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Bertalanffy, L. von. (1968). *General System Theory: Foundations, Development, Applications.* N.Y.: George Braziller.

2. Brauch, H. G. (2005). *Threats, Challenges, Vulnerabilities and Risks in Environmental and Human Security.* United Nation University – Institute for Environment and Human Security. Bonn, Germany.

3. Habron, G. (2003). Role of Adaptive Management for Watershed Councils. *Environmental Management, 31*(1), 29–41. doi: 10.1007/s00267-002-2763-

Holling, C. S. (1978). *Adaptive Environmental Assessment and Management.* London: Wiley.

4. Walters, C. J. (1986). *Adaptive Management of Renewable Resources.* New York: McGraw Hill.

5. Алімпієв А.М., Пєвцов Г.В. Особливості гібридної війни рф проти України. Досвід, що отриманий Повітряними Силами Збройних Сил України. Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 19–25. https://doi.org/10.30748/nitps.2017.27.03.

6. Белай С. В. Дослідження механізмів моніторингу загроз національній безпеці України соціально-економічного характеру. *Університетські наукові записки*. 2013. № 4 (48). С. 481–488.

7. Бжезинський З. Україна і Європа. Національна безпека і оборона. 2000. № 7. С. 11–20.

8. Богданович В. Ю. Теоретико-методологічні основи забезпечення національної безпеки України: монографія : у 7 т. – Т. 4 : Воєнна безпека держави і шляхи її забезпечення / В. Ю. Богданович, І. Ю. Свида, Є. Д. Скулиш; за заг. ред. Є. Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. 464 с.

9. Богданович В. Ю., Семенченко А. І., Кучма Д. Я., Дацюк А. В.. Методика реагування на виклики, небезпеки та загрози національній безпеці держави : навч. посіб. К. : НАДУ, 2009. 40 с.

10. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М.Ю., 2021. 558 с. ISBN 978-617-7664-71-9.

11. Воєнна доктрина України: Указ Президента України № 555 від 24 вересня 2015 р. – К. : АПУ, 2015. – 27 с.

12. Гбур З. В. Можливість адаптації Ізраїльського досвіду використання штучного інтелекту у бойових діях на Сході. Інвестиції: практика та досвід № 12/202. URL: http://www.investplan.com.ua/pdf/12_2021/11.pdf.

13. Глобальна та національна безпека : підручник / В. І. Абрамов, Г. П. Ситник, В. Ф Смолянюк; за заг. ред. Г. П. Ситника. К. : НАДУ, 2016. –784 с.

14. Кизим М. О., Хаустова В. Є., Шпілєвський В. В., Шпілєвський О. В. Військово-тактичні та економічні передумови розвитку оборонної промисловості України. Проблеми економіки № 3 (53), 2022. URL: file:///C:/Users/38067/Downloads/PE_03_2022-35-44.pdf.

15. Князєва О. А. Стратегічні вектори економічного розвитку країни у післявоєнний час. Науковий вісник Одеського національного економічного університету. Збірник наукових праць №3-4 (292-293), 2022. URL: http://n-visnik.oneu.edu.ua/collections/2022/292-293/pdf/94-100.pdf.

16. Кобко Є. В. Моніторинг загроз національній безпеці держави: зарубіжний досвід та українські реалії публічно-правового забезпечення. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 1 (106). С. 122–133.

17. Ковалевський С.М., Пєвцов Г.В., Худов Г.В. Пропозиції щодо створення скритого маловисотного радіолокаційного поля в умовах ведення сучасних мережецентричних та гібридних війн. Наука і техніка Повітряних Сил Збройних Сил України. 2015. № 1(18). С. 77–81.

18. Концепція розвитку сектору безпеки і оборони України : затверджена Указом Президента України [№ 92/2016 від 14 березня 2016 р.]. – К. : АПУ, 2016. – 17 с.

19. Костенко О.В. Аналіз національних стратегій розвитку штучного інтелекту. Інформація і право. № 2(41)/ 2022. URL: file:///C:/Users/38067/Downloads/270365-%D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B0%D1%82%D1%82%D1%96-623224-1-10-20221226.pdf

20. Кучеренко Ю.Ф., Гузько О.М. Деякі особливості сучасних локальних війн. Збірник наукових праць Харківського університету Повітряних Сил. 2008. № 2(17). С. 20–23.

21. Кушнір О.І., Давикоза О.П., Кучеренко Ю.Ф. Аналіз впливу "гібридної" війни на розвиток автоматизованої системи управління авіацією та ППО Збройних Сил України. Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 116–120. https://doi.org/10.30748/nitps.2017.27.22.

22. Медведєв В.К., Кучеренко Ю.Ф., Гузько О.М. Сучасна інформаційна війна та її обрис. Системи озброєння і військова техніка. 2008. № 1(13). С. 52–54.

23. Понад 60 країн погодилися з необхідністю контролю за зброєю зі штучним інтелектом. URL: https://noworries.news/ponad-60-krayin-pogodylysya-z-neobhidnistyu-kontrolyu-za-zbroyeyu-zi-shtuchnym-intelektom/?fbclid=IwAR2r89Bt9-lKvGOFPAsue5wkACAFWNXpGEoxKbhWsZc5QlEJlE1jYJk7dnk.

24. Про затвердження плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021-2024 роки: Розпорядження Кабінет Міністрів України від 12 травня 2021 р. № 438-р. URL: https://zakon.rada.gov.ua/laws/show/438-2021-%D1%80#Text.

25. Про національну безпеку України: Закон України № 2469-VIII від 21 червня 2018 р. [Електронний ресурс]. Режим доступу : http://zakon3.rada.gov.ua/laws/show/2469-19.

26. Про Стратегію воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021. URL: https://www.president.gov.ua/documents/1212021-3766.

27. Про Стратегію воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021.

28. Про Стратегію забезпечення державної безпеки: Указ Президент України від 16 лютого 2022 року № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5.

29. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.

30. Про Стратегію інформаційної безпеки: Указ Президента України від 28 грудня 2021 року № 685/2021.

31. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013.

32. Про Стратегію кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021.

33. Про Стратегію національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020.

34. Резнікова, О. О., Войтовський, К. Є., Лепіхов, А. В. (2020). *Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України :* аналіт. доповідь / за заг. ред. О. О. Резнікової. Київ : НІСД, 84.

35. Саганок Ф.В., Фролов В.С., Павленко В.І. та ін. Сектор безпеки і оборони: стратегічне керівництво та військове управління: монографія / за ред. д.військ.н. проф. І.С. Руснака. Київ: ЦЗ МО та ГШ ЗС України, 2018. 230 с.

36. Семенченко А. І. Механізм стратегічного управління забезпеченням національної безпеки у кризових та надзвичайних ситуаціях. *Проблеми національної безпеки й оборони. Стратегічні пріоритети*. 2007. № 1 (2). С. 105–116.

37. Стратегія національної безпеки України : затверджена Указом Президента України № 287/2015 від 26 травня 2015 року // Урядовий кур'єр. – № 95. – 2015. – 29.05.

38. Стратегія національної безпеки України: Указ Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text.

39. Стратегія розвитку оборонно-промислового комплексу України: Указ Президента України від 20 серпня 2021 року № 372/2021. URL: https://zakon.rada.gov.ua/laws/show/372/2021#Text.

40. Угода між Україною та Європейським Союзом про участь України у програмі Європейського Союзу "Цифрова Європа" (2021 - 2027): Закон України від 23 лютого 2023 року. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/41298.

41. Хаустова В. Є., Решетняк О. І., Хаустов М. М., Зінченко В. А. Напрямки розвитку технологій штучного інтелекту в забезпеченні обороноздатності країни. БІЗНЕСІНФОРМ № 3, 2022. С. 17-26. URL: file:///C:/Users/38067/Downloads/_BI3%20(3).pdf

42. Худов Г.В., Таран І.А. Методика синтезу раціональної структури підсистеми розвідки системи протиповітряної оборони з використанням генетичного алгоритму. Наука і техніка Повітряних Сил Збройних Сил України. 2016. № 2(23). С. 25–31.

43. Четверта промислова революція : зміна напрямів міжнародних інвестиційних потоків: монографія / А. І. Крисоватий, О. М. Сохацька, І. В. Скавронська [та ін.] ; за наук. ред. А. І. Крисоватого та О. М. Сохацької. Тернопіль : Осадца Ю. В., 2018. 480 с. URL: http://dspace.tneu.edu.ua/handle/316497/33661

44. Ярош С. П. Теоретичні основи побудови та застосування розвідувально-управляючих інформаційних систем протиповітряної оборони. Харків: ХУПС, 2012. 512 с.