УДК 004.056.53 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.56

І. В. СТОЦЬКИЙ
старший викладач кафедри комп'ютерних інформаційних технологій
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
ORCID: 0000-0002-5898-3228

В. П. КОСТЕНКО
старший викладач кафедри комп'ютерних інформаційних технологій
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
ORCID: 0000-0002-7180-233X

Г. І. НАЛІСНИЙ
викладач кафедри комп'ютерних інформаційних технологій
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
ORCID: 0009-0000-5142-3677

С. А. ШАРНІ
викладач кафедри комп'ютерних інформаційних технологій
Військовий інститут телекомунікацій та інформатизації
імені Героїв Крут
ORCID: 0000-0002-5856-3995

ВИКОРИСТАННЯ АЛГОРИТМІВ AI ДЛЯ ВИЯВЛЕННЯ ТА БЛОКУВАННЯ КІБЕРАТАК НА ВІЙСЬКОВІ ІНФОРМАЦІЙНІ СИСТЕМИ

У сучасному геополітичному контексті, що супроводжується активізацією кіберконфліктів, особливої актуальності набуває проблема забезпечення кібербезпеки військових інформаційних систем. Такі системи є критично важливими для національної оборони, оперативного управління військами та реалізації стратегічних рішень, що робить їх головними цілями як масових, так і таргетованих кібератак. Традиційні підходи до кіберзахисту, орієнтовані на сигнатурний або евристичний аналіз, не можуть забезпечити належний рівень захисту від новітніх загроз, які постійно змінюються, адаптуються та використовують засоби штучного інтелекту.

У цьому контексті використання алгоритмів штучного інтелекту (ШІ, AI), зокрема методів машинного та глибинного навчання, навчання з підкріпленням і обробки природної мови, відкриває нові горизонти для проактивного, адаптивного та автономного кіберзахисту. У статті розглянуто підходи до розробки, впровадження та експлуатації інтелектуальних систем виявлення та блокування атак у військових умовах. Проаналізовано можливості систем виявлення вторгнень нового покоління (Next-Gen IDS), побудованих на базі згорткових нейронних мереж (CNN), які дозволяють виявляти DDoS-атаки, сканування портів та зловмисну активність у реальному часі з високою точністю. Особливу увагу приділено питанням обробки даних з численних джерел у рамках підходу Data Fusion, що критично важливо у бойових умовах, де інформація надходить від сенсорів, безпілотників, супутників тощо.

Окремий акцент зроблено на ролі навчання з підкріпленням у прийнятті рішень в умовах швидкоплинних бойових ситуацій, а також на використанні технологій edge computing, що забезпечують автономність систем у разі втрати зв'язку з центром. Проаналізовано ризики, пов'язані з атаками на самі моделі штучного інтелекту, такі як data poisoning, adversarial input, model inversion, та наведено методи їхньої нейтралізації. Досліджено інтеграцію Explainable AI (XAI) для підвищення довіри до рішень систем, забезпечення прозорості та можливості оперативного контролю.

Показано, що впровадження ШІ у військові інформаційні системи дозволяє реалізувати самонавчальні захисні платформи, які здатні адаптуватися до змін загрозового середовища, генерувати нові сигнатури на основі поточних даних та координувати реагування в межах централізованої командно-інформаційної інфраструктури. У роботі наголошено на важливості міждисциплінарного підходу, залучення фахівців у сфері інформаційної безпеки, військової логістики, розвідки, а також створення цілісної доктрини кібероборони на основі ШІ. Отже, алгоритми ШІ розглядаються не як допоміжний інструмент, а як фундамент майбутньої архітектури стійкого, гнучкого та інтелектуального захисту військових IT-систем.

Ключові слова: *штучний інтелект (ШІ), кібербезпека, військові інформаційні системи, системи виявлення вторгнень (IDS), машинне навчання, кібератаки, навчання з підкріпленням, кібергігієна користувачів.*

I. V. STOTSKYI
Senior Lecturer at the Department of Computer Information Technologies
Geroyev Krut Military Institute of Telecommunications and Informatization
ORCID: 0000-0002-5898-3228

V. P. KOSTENKO
Senior Lecturer at the Department of Computer Information Technologies
Geroyev Krut Military Institute of Telecommunications and Informatization
ORCID: 0000-0002-7180-233X

G. I. NALISNYI
Lecturer at the Department of Computer Information Technologies
Geroyev Krut Military Institute of Telecommunications and Informatization
ORCID: 0009-0000-5142-3677

S. A. SHARNIN
Lecturer at the Department of Computer Information Technologies
Geroyev Krut Military Institute of Telecommunications and Informatization
ORCID: 0000-0002-5856-3995

USE OF AI ALGORITHMS FOR DETECTION AND BLOCKING OF CYBER ATTACKS ON MILITARY INFORMATION SYSTEMS

In the modern geopolitical context, accompanied by the intensification of cyber conflicts, the problem of ensuring the cybersecurity of military information systems is of particular relevance. Such systems are critically important for national defense, operational command of troops and the implementation of strategic decisions, which makes them the main targets of both mass and targeted cyberattacks. Traditional approaches to cyberdefense, focused on signature or heuristic analysis, cannot provide an adequate level of protection against the latest threats that are constantly changing, adapting and using artificial intelligence tools. In this context, the use of artificial intelligence (AI) algorithms, in particular machine and deep learning methods, reinforcement learning and natural language processing, opens up new horizons for proactive, adaptive and autonomous cyberdefense. The article considers approaches to the development, implementation and operation of intelligent systems for detecting and blocking attacks in military conditions. The capabilities of Next-Gen IDS systems built on the basis of convolutional neural networks (CNN) are analyzed, which allow detecting DDoS attacks, port scanning and malicious activity in real time with high accuracy. Special attention is paid to the issues of processing data from multiple sources within the Data Fusion approach, which is critically important in combat conditions, where information comes from sensors, drones, satellites, etc.

A special emphasis is placed on the role of reinforcement learning in decision-making in fast-paced combat situations, as well as on the use of edge computing technologies that ensure the autonomy of systems in case of loss of communication with the center. The risks associated with attacks on artificial intelligence models themselves, such as data poisoning, adversarial input, model inversion, are analyzed, and methods for their neutralization are presented. The integration of Explainable AI (XAI) is investigated to increase trust in system decisions, ensure transparency and the possibility of operational control.

It is shown that the implementation of AI in military information systems allows for the implementation of self-learning defense platforms that are able to adapt to changes in the threat environment, generate new signatures based on current data, and coordinate responses within a centralized command and information infrastructure. The paper emphasizes the importance of an interdisciplinary approach, involving specialists in the field of information security, military logistics, and intelligence, as well as the creation of a holistic cyber defense doctrine based on AI. Therefore, AI algorithms are considered not as an auxiliary tool, but as the foundation of the future architecture of sustainable, flexible, and intelligent defense of military IT systems.

Key words: *artificial intelligence (AI), cybersecurity, military information systems, intrusion detection systems (IDS), machine learning, cyber attacks, reinforcement learning, user cyber hygiene.*

Постановка проблеми

У сучасному цифровому середовищі військові інформаційні системи відіграють ключову роль у забезпеченні національної безпеки, оперативного управління військами та здійсненні стратегічного планування. З огляду на глобальну тенденцію до цифровізації та мережевої взаємодії, дані системи є об’єктом інтенсивних кібератак, які можуть призводити до фатальних наслідків для національної безпеки, порушення логістичних ланцюгів, втрати критичних даних і навіть виведення з ладу державні оборонні системи [1].

Класичні методи кіберзахисту, які ґрунтуються на сигнатурному аналізі, не здатні ефективно протистояти складним, багаторівневим і динамічним загрозам, що постійно змінюються. На даний час, інструменти кібератак

використовують соціальну інженерію, шкідливе програмне забезпечення (ПЗ) із функціями штучного інтелекту, автоматизоване сканування вразливостей, а також механізми ухилення від їх виявлення. У зв'язку з цим, виникає потреба у впровадженні адаптивних, інтелектуальних систем захисту, здатних в режимі реального часу аналізувати великий обсяг даних, виявляти аномалії та блокувати потенційні загрози.

Алгоритми штучного інтелекту (ШІ, AI), зокрема машинне навчання, глибинне навчання та обробка природної мови (NLP), мають потенціал стати основою нової парадигми кібербезпеки. Їх застосування у військовій сфері дозволяє створювати системи проактивного захисту, які не лише реагують на атаки, а й передбачають можливі сценарії загроз. Проте, попри потенціал, існують значні виклики щодо інтеграції AI у військові системи, зокрема питання надійності, етичності, прозорості та захисту самих моделей AI від маніпуляцій.

Проблема ускладнюється необхідністю дотримання високого рівня конфіденційності та секретності інформації у військовому секторі. Будь-яке рішення повинне відповідати суворим вимогам до безпеки, масштабованості, автономності та здатності функціонувати в умовах обмежених ресурсів (наприклад, у польових умовах або під час кібервійни) [2, 3].

Таким чином, актуальність теми застосування AI для виявлення та блокування кібератак на військові інформаційні системи зумовлена як зростанням кількості кібератак, так і необхідністю підвищення ефективності засобів кіберзахисту за рахунок інтелектуалізації процесів виявлення загроз. При цьому, загрозлива динаміка розвитку кіберзлочинності, зокрема державного кібертероризму та шкідливих інформаційних операцій, потребує не лише модернізації існуючих рішень, а й створення нових, якісно інших систем захисту. Військові інформаційні системи повинні не просто бути захищеними, а мати можливість до самонавчання, адаптації до нових умов і активного протистояння новітнім формам атак, що можливо реалізувати лише за умов глибокої інтеграції AI-технологій у архітектуру систем кібербезпеки.

Аналіз останніх досліджень і публікацій

Упродовж останнього десятиліття у наукових спільнотах зросла увага до використання штучного інтелекту для забезпечення кібербезпеки, зокрема у військовому контексті. Значна кількість досліджень підтверджує ефективність алгоритмів машинного навчання у виявленні аномалій, класифікації мережевого трафіку та ідентифікації шкідливого ПЗ.

Так, у дослідженнях MIT Lincoln Laboratory та DARPA підкреслюється ефективність глибоких нейронних мереж у виявленні раніше невідомих типів атак, таких як zero-day exploits. Розробка систем на базі LSTM (довготривала короткочасна пам'ять) дозволила досягти високої точності при аналізі мережевого трафіку та передбаченні потенційно небезпечних активностей. У рамках проєкту MADL (Machine Learning for Advanced Defense Logistics) були протестовані моделі, здатні виявляти складні кореляції між різнорідними джерелами даних у реальному часі [4].

У європейських програмах кібербезпеки, таких як ECHO та SPARTA, значну увагу приділено інтеграції AI з класичними системами моніторингу. Наприклад, застосування гібридних моделей – поєднання машинного навчання з логічним аналізом – забезпечує не лише виявлення загроз, а й пояснюваність рішень, що особливо важливо у військовому контексті. Розроблено спеціалізовані платформи, які дозволяють здійснювати багаторівневу ієрархічну оцінку ризиків на основі навчання з підкріпленням (reinforcement learning).

Публікації останніх років, зокрема в IEEE Access, Journal of Cybersecurity, ACM Transactions on Privacy and Security, демонструють успішне впровадження AI в системи IDS/IPS (інструменти виявлення та запобігання вторгнень). Сучасні системи типу «intelligent IDS» поєднують в собі класичні правила, евристичний аналіз та глибоке навчання для обробки великого обсягу даних з низькою затримкою. Ці технології уже застосовуються у пілотних проектах для НАТО та в арміях провідних країн, таких як США, Ізраїль та Велика Британія [5].

У межах публікацій щодо специфіки військових інформаційних систем підкреслюється, що моделі AI повинні враховувати динаміку середовища, мобільність вузлів, змінні умови доступу та складність топології мереж. Наприклад, у дослідженнях RAND Corporation та NATO CCDCOE досліджуються аспекти застосування адаптивних AI-алгоритмів у середовищі без стабільного підключення до мережі, що характерно для бойових умов [6].

Значну увагу також приділено питанням атак на самі моделі AI. Такі загрози, як отруєння даних (data poisoning), атаки на цілісність моделі та зворотне проектування (model inversion) розглядаються як серйозні виклики, що потребують побудови захищених архітектур машинного навчання. Пропонуються механізми валідації навчальних даних, використання генеративних моделей для перевірки цілісності та побудова автономних верифікаторів рішень моделі.

Підсумовуючи, можна зазначити, що наукове середовище активно досліджує потенціал AI у військовій кібербезпеці. Водночас існує потреба у стандартизації підходів, визначенні протоколів взаємодії та забезпеченні прозорості у використанні таких рішень, особливо в умовах критичної інфраструктури. Тенденції свідчать про швидкий розвиток міжпредметних досліджень на перетині кібербезпеки, AI, військової логістики та стратегічного аналізу загроз.

Формулювання мети дослідження

Мета статті – дослідження алгоритмів штучного інтелекту для виявлення, запобігання та нейтралізації кібератак на військові інформаційні системи з урахуванням сучасних технологічних рішень, особливостей військового середовища та вимог до кіберстійкості.

Викладення основного матеріалу дослідження

Практична реалізація алгоритмів штучного інтелекту для виявлення та блокування кібератак на військові інформаційні системи полягає у використанні комплексного підходу, що включає розробку, тестування, впровадження та експлуатацію технологій на базі машинного навчання, обробки великих даних, обчислень на краю мережі (edge computing) та кіберфізичних систем. Військовий контекст висуває особливі вимоги до стійкості систем, швидкості реакції, автономності рішень та здатності до самонавчання.

Однією з ключових технологій є системи виявлення вторгнень нового покоління (Next-Gen IDS), які об'єднують алгоритми глибокого навчання (Deep Learning) з класичними методами аналізу мережевого трафіку. Такі системи здатні не лише фіксувати аномальні шаблони поведінки, але й класифікувати їх за типами загроз. Наприклад, використання згорткових нейронних мереж (CNN) для аналізу трафіку в реальному часі дозволяє виявити DDoS-атаки, сканування портів, зловмисні пакети та активність ботнетів із точністю понад 95 %.

Іншим напрямком є обробка телеметричних даних з багатьох джерел одночасно – так званий підхід Data Fusion. Військові системи часто працюють у середовищі, де доступна інформація з сенсорів, супутників, систем командного зв'язку та мобільних пристроїв. Застосування моделей кластеризації (наприклад, алгоритмів K-means або DBSCAN) дозволяє інтегрувати ці дані, виявляти відхилення, створювати профілі звичайної поведінки системи і оперативно виявляти невідповідності.

Важливою складовою системи захисту є механізми прийняття рішень на основі навчання з підкріпленням (Reinforcement Learning). У військових умовах, коли зміна параметрів середовища відбувається дуже швидко, агенти RL можуть навчатися ефективним стратегіям відповіді на загрози, вибираючи між ізоляцією вузла, реконфігурацією мережі, зміною маршрутів передачі даних або активацією резервних систем. Наприклад, алгоритм DQN (Deep Q Network) застосовується для моделювання сценаріїв атаки та формування оптимальних дій у відповідь [5].

Крім цього, системи кіберзахисту з ШІ повинні містити модулі самонавчання на основі аналізу нових даних про загрози, отриманих з відкритих джерел (OSINT), військової розвідки та партнерських мереж безпеки. Нейронні мережі типу Transformer (наприклад, BERT, GPT) використовуються для обробки текстових повідомлень про нові загрози, автоматичного створення сигнатур та формування попереджень у системах реагування.

Успішна імплементація AI вимагає створення спеціального циклу DevSecOps, адаптованого до потреб військових операцій. Такий цикл має включати: автоматизоване тестування моделей на стійкість до атак; перевірку навчальних даних на чистоту; впровадження механізмів Explainable AI (XAI) для пояснення рішень; резервування критичних елементів та впровадження механізмів відновлення після атак.

Реальне розгортання таких систем можливе завдяки використанню edge-computing – систем розподіленого аналізу даних на місці збору (на пристроях, дронах, сенсорах). Це забезпечує мінімальну затримку в обробці інформації та дозволяє знизити залежність від каналів зв'язку, які можуть бути зруйновані під час бойових дій. Наприклад, інтеграція моделі CNN у військовий дрон дозволяє розпізнавати підозрілу активність у зоні бойових дій без потреби передавати відео в центр обробки.

Значну роль у блокуванні атак відіграють методи динамічної реконфігурації архітектури військової мережі. За допомогою предиктивного аналізу на основі рекурентних нейронних мереж (RNN) система може прогнозувати, яка частина інфраструктури найімовірніше стане об'єктом атаки, та автоматично переналаштовувати маршрути даних, активувати додаткове шифрування або виводити з експлуатації вразливі вузли.

Питання кібергігієни користувачів військових систем також вирішуються за допомогою AI. Алгоритми поведінкового аналізу створюють індивідуальні профілі користувачів і виявляють дії, нехарактерні для конкретного оператора (наприклад, доступ до незвичних файлів, запити в незвичний час, введення команд із нових пристроїв), що може свідчити про компрометацію облікового запису.

Особливе значення має захист самих моделей AI. Військові системи мають бути захищені від атак типу adversarial input, які змінюють вхідні дані з метою викликати помилку в рішенні моделі. Для цього використовуються методи захисту, такі як distillation, adversarial training та використання додаткових мереж-детекторів, що виявляють підозрілі входи. Дослідження демонструють, що інтеграція таких механізмів дозволяє знизити ймовірність маніпуляції на понад 80 % [6].

У контексті оперативного управління всі ці елементи мають бути інтегровані в єдину командно-інформаційну систему. Наприклад, розробка центру кібероперацій з використанням централізованої платформи, яка акумулює дані, проводить аналіз, генерує рекомендації та керує контрзаходами в автоматичному або напівавтоматичному режимі.

Виходячи з цього, можна констатувати значний практичний потенціал використання AI в системах кіберзахисту військових структур. Однак ефективність впровадження таких рішень залежить від узгодженості між технічними фахівцями, командуванням, аналітиками розвідки та політичним керівництвом. Тільки інтегрований підхід до розробки та використання AI в умовах війни забезпечить необхідний рівень стійкості до кібератак та інформаційного терору.

Висновки

Застосування алгоритмів штучного інтелекту для виявлення та блокування кібератак на військові інформаційні системи є стратегічно важливим напрямом розвитку оборонних технологій. Перш за все, алгоритми AI дозволяють значно

підвищити точність і швидкість виявлення кіберзагроз. Традиційні системи, що ґрунтуються на сигнатурах, виявляють лише відомі типи атак, у той час як AI здатен виявляти нові та модифіковані форми загроз шляхом аналізу поведінкових патернів, аномалій та кореляцій у великих обсягах даних. Завдяки використанню методів глибокого навчання, кластеризації, підкріплення та трансформерів, військові системи отримують інструменти проактивного захисту.

Крім цього, системи, підкріплені AI, виявляють гнучкість і адаптивність до змінного середовища бойових дій. Алгоритми навчання з підкріпленням можуть обирати оптимальні стратегії реагування, забезпечуючи ефективну ізоляцію, реконфігурацію чи протидію загрозам в режимі реального часу. Це критично важливо в умовах обмежених ресурсів і високої динаміки подій.

Також, важливим досягненням є застосування технологій edge-computing, які дозволяють обробляти дані безпосередньо на місці подій, зменшуючи залежність від централізованих ресурсів та підвищуючи автономність систем. Зокрема, автономні дрони, сенсори, командно-штабні комплекси можуть функціонувати незалежно від центра зв'язку, що робить систему менш вразливою до атак на інфраструктуру.

Вцілому, інтеграція AI в системи кіберзахисту дозволяє реалізовувати принципи самоадаптації та безперервного навчання. Це забезпечує постійне оновлення знань про загрози, автоматичну побудову моделей нових атак та формування ефективних протидій без прямого втручання людини. Таким чином досягається висока стійкість до тактик «0-day» атак.

Значним фактором є зростання значення Explainable AI (XAI) – пояснюваного штучного інтелекту, який дає змогу операторам та командуванню розуміти логіку дій системи та приймати обґрунтовані рішення. У військовому контексті прозорість алгоритмів AI є надзвичайно важливою для збереження контролю та запобігання фатальним помилкам. Тому критично важливим є впровадження багаторівневих механізмів захисту, регулярне тестування, а також побудова архітектур із надлишковими елементами та можливістю швидкого відновлення.

У контексті даної роботи, можна зазначити, що ефективне використання AI в кібербезпеці військових структур можливе лише за наявності спеціалістів, які володіють знаннями як у сфері інформаційної безпеки, так і в алгоритмах машинного навчання. Необхідна системна робота з підготовки офіцерів-кібернетиків, аналітиків загроз, інженерів із впровадження та адміністрування таких систем.

Підсумовуючи вищезазначене, слід відзначити, що алгоритми штучного інтелекту є не лише допоміжним інструментом, а й основою майбутніх платформ кібероборони. Їх впровадження у військові інформаційні системи – це вже не питання вибору, а питання національної безпеки. Надалі необхідно зосередитися на створенні адаптивних, стійких, прозорих і здатних до самонавчання кіберсистем, які зможуть забезпечити ефективну протидію як традиційним, так і новітнім гібридним загрозам.

Список використаної літератури

1. Гулак Г. М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ : Видавництво НА СБ України, 2021. 256 с.
2. Даник Ю. Г., Воробієнко П. П., Чернега В. М. Основи кібербезпеки та кібероборони: підручник. Одеса : ОНАЗ ім. О. С. Попова, 2019. 320 с.
3. Толюпа С. В., Штаненко С. С., Берестовенко Г. Класифікаційні ознаки систем виявлення атак та напрямки їх побудови. Збірник наукових праць Військового інституту телекомунікацій та інформатизації імені Героїв Крут. 2018. Вип. № 3. С. 56–66.
4. Solomon M. Building a Secure & Privacy-Focused IoT Network. Cambridge: MIT Press, 2021. 370 p.
5. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2020. 840 p.
6. Zhou H., Liu C. Deep Learning in Cybersecurity. San Francisco : Elsevier, 2020. 242 p.

References

1. Hulak, H. M. Metodolohiia zakhystu informatsii. (2021). Aspekty kiberbezpeky: pidruchnyk. Kyiv : Vydavnytstvo NA SB Ukrainy, 256 s. [in Ukrainian].
2. Danyk, Yu. H., Vorobiienko, P. P., Cherneha, V. M. (2019). Osnovy kiberbezpeky ta kiberoborony: pidruchnyk. Odesa : ONAZ im. O. S. Popova, 320 s. [in Ukrainian].
3. Toliupa, S. V., Shtanenko, S. S., Berestovenko, H. (2018). Klasyfikatsiini oznaky system vyiavlennia atak ta napriamky yikh pobudovy. Zbirnyk naukovykh prats Viiskovoho instytutu telekomunikatsii ta informatyzatsii imeni Heroiv Krut, Vyp. № 3. S. 56–66.[in Ukrainian].
4. Solomon M. (2021) Building a Secure & Privacy-Focused IoT Network. Cambridge: MIT Press, 370 p.
5. Stallings W. (2020) Cryptography and Network Security: Principles and Practice. Pearson, 840 p.
6. Zhou H., Liu C. (2020) Deep Learning in Cybersecurity. – San Francisco: Elsevier,.242 p.

Дата першого надходження рукопису до видання: 28.09.2025
Дата прийнятого до друку рукопису після рецензування: 24.10.2025
Дата публікації: 28.11.2025