УДК 342.951
DOI https://doi.org/10.32782/2524-0374/2024-6/49

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В УМОВАХ ВОЄННОГО СТАНУ

ENSURING CYBER SECURITY OF CRITICAL INFRASTRUCTURE OBJECTS BASED ON ARTIFICIAL INTELLIGENCE UNDER THE CONDITIONS OF A STATE OF WAR

Казьмірук С.Д., аспірант
Державна наукова установа Інститут інформації, безпеки і права Національної академії правових наук України

Леонов Б.Д., д.ю.н., професор,
головний науковий співробітник
Міжвідомчий науково-дослідний центр при Раді національної безпеки і оборони України

Омельян О.С., д. філос. з юридичних наук,
суддя
Господарський суд Житомирської області

Стаття присвячена дослідженню проблемних питань забезпечення кібербезпеки об'єктів критичної інфраструктури на основі штучного інтелекту в умовах воєнного стану. Висвітлено роль та місце об'єктів критичної інфраструктури в структурі національної безпеки України. Деталізовані фактори, які впливають на кіберзахищеність об'єктів критичної інфраструктури. Визначено види кіберзагроз, які впливають на кібезахищеність об'єктів критичної інфраструктури в умовах кібервійни. Визначено особливе місце кіберзагроз геополітичного характеру в системі кіберзагроз. Констатується, що застосування штучного інтелекту в системі безпеки об'єктів критичної інфраструктури має значний потенціал для підвищення рівня кіберзахисту. Окреслено засади державної політики у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури. Проведено аналіз законодавства України з питань захисту об'єктів критичної інфраструктури Обґрунтовано доцільність впровадження інтегрованих систем кіберзахисту інформації та забезпечення кібербезпеки об'єктів критичної інфраструктури. Визначено шляхи та напрями забезпечення кібербезпеки об'єктів критичної інфраструктури на основі штучного інтелекту в умовах воєнного стану. Визначено шляхи удосконалення вітчизняного законодавства з питань захисту об'єктів критичної інфраструктури в умовах воєнного стану. На базі аналізу позитивного американського досвіду запропоновані заходи з удосконалення забезпечення кіберзахисту об'єктів критичної інфраструктури України. Запропоновані рекомендації у сфері інформаційної безпеки, що базується на властивостях інформації та досягненнях інформаційно-комунікаційних технологій і систем. Зроблено висновок, що штучний інтелект відіграє ключову роль у зниженні ризиків кіберзагроз об'єктів критичної інфраструктури завдяки можливостям виявлення аномалій, автоматизації реакцій на інциденти, прогнозування та запобігання кіберзагрозам, покращення аутентифікації користувачів, оптимізації управлінням вразливостями, розпізнавання фішингових кібератак та підтримки у розслідуванні кіберінцидентів. Визначено подальші наукові розвідки у сфері кібербезпеки та інформаційної безпеки, серед яких виділяються зміцнення кіберзахисту від ворожих дестабілізаційних операцій, забезпечення координації діяльності усіх суб'єктів забезпечення кібербезпеки, а також розвиток спроможності ударного кіберпотенціалу країни для забезпечення кібербезпеки об'єктів критичної інфраструктури.

Ключові слова: кібератака, кібербезпека, інтегровані системи захисту інформації, штучний інтелект, об'єкти критичної інфраструктури, державна політика у сфері кібербезпеки, національна безпека.

The article is devoted to the study of problematic issues of ensuring the cyber security of critical infrastructure objects based on artificial intelligence in martial law conditions. The role and place of critical infrastructure objects in Ukraine's national security structure is highlighted. Detailed factors that affect the cyber security of critical infrastructure objects. The types of cyberthreats that affect the cyber security of critical infrastructure objects in the conditions of cyberwar are determined. The special place of cyber threats of a geopolitical nature is determined, it is stated that the use of artificial intelligence in the security system of critical infrastructure objects has a significant potential for increasing the level of cyber protection. The principles of state policy in ensuring cyber security of critical infrastructure facilities are outlined. An analysis of Ukrainian legislation on the protection of critical infrastructure facilities was carried out. The expediency of implementing integrated systems of cyber protection of information and cyber security of critical infrastructure objects is substantiated. The ways and directions of ensuring the cyber security of critical infrastructure objects based on artificial intelligence in martial law conditions have been determined. Ways to improve domestic legislation on the protection of critical infrastructure facilities under martial law conditions have been identified. Based on the positive American experience analysis, measures are proposed to improve the provision of cyber protection for critical infrastructure objects in Ukraine. Proposed recommendations in the field of information security, based on the properties of information and achievements of information and communication technologies and systems. It was concluded that artificial intelligence plays a key role in reducing the risks of cyber threats to critical infrastructure objects due to the capabilities of detecting anomalies, automating responses to incidents, predicting and preventing cyber threats, improving user authentication, optimizing vulnerability management, recognizing phishing cyber attacks and supporting cyber incident investigations. Further scientific research in the field of cyber security and information security has been determined, among which the strengthening of cyber protection against hostile destabilization operations, ensuring the coordination of the activities of all cyber security actors, as well as the development of the country's cyber strike potential to ensure the cyber security of critical infrastructure facilities are highlighted.

Key words: cyber attack, cyber security, integrated information protection systems, artificial intelligence, critical infrastructure objects, state policy in the field of cyber security, and national security.

Постановка проблеми. Неприкрита збройна агресія Росії проти України грубо порушує міжнародне право і принципи Статуту ООН, підриває європейську та глобальну безпеку й стабільність, а також завдає невимовних страждань українському народові. В умовах воєнного стану кібератаки стали серйозною загрозою для національної безпеки, а зростаюча динаміка науково-технічного прогресу спричинила різке підвищення вимог до швидкості та якості прийняття рішень на усіх рівнях суспільного життя. В умовах формування національного та глобального інформаційного простору прийняття обґрунтованих управлінських рішень потребує значного обсягу інформації щодо суспільних та міжнародних процесів [1, с. 37].

CERT-UA урядова команда реагування на комп'ютерні надзвичайні події (при Держспецзв'язку України) за минулий рік зафіксувала 2543 кіберінциденти, що на 15,9% більше ніж за 2022 рік, коли Україна стикнулася з величезною кількістю атак у зв'язку з повномасштабною

російською агресією проти нашої держави [2]. З цього приводу Держспецзв'язку України зазначає, що «зловмисники найбільше атакують уряд та урядові організації, місцеві органи влади та сектор безпеки та оборони, комерційні організації, енергетичний сектор, телекомунікації та об'єкти критичної інфраструктури. Найпоширенішими типами інцидентів є: розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису та компрометація системи. Метою зловмисників є розвідувальні операції, довготривале шпигунство, знищення даних та інформаційних систем. Кількість ворожих атак продовжує збільшуватися» [2].

Кібербезпека об'єктів критичної інфраструктури в умовах воєнного стану є надзвичайно важливим завданням забезпечення національної безпеки України. Враховуючи зростаючу роль інноваційних технологій на базі штучного інтелекту у сфері кібербезпеки, важливо розглянути нові можливості їх ефективного застосування для забезпечення захисту критичної інфраструктури в умовах війни. В таких умовах загрози для критичної інфраструктури тільки зростають, оскільки зловмисники продовжують сканувати і атакувати мережі, а також намагатися обійти контроль доступу [3, с. 155].

Результати аналізу наукових публікацій. Сучасний стан правової охорони об'єктів критичної інфраструктури в Україні був предметом поглибленого аналізу у працях С. Кучерини, Д. Олейнікова [4], О. Суходолі [5].

Правові та організаційні засади забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак висвітлено у роботах Я. Мануілова [6], С. Цяпи [7], О. Алексеєвої [8]. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США) досліджувався Леоновим Б.Д., Шостаком Р.М. та Серьогіним В.С. [9]. Вагомий внесок у розроблення технологій ідентифікації об'єктів критичної інфраструктури зроблено зарубіжними вченими. Це, зокрема, праці Д. Дуденхофера, П. Педерсена, М. Пермана та М. Маніка.

Водночас, низка проблемних аспектів забезпечення кібербезпеки об'єктів критичної інфраструктури на основі ШІ залишаються недостатньо дослідженими в умовах воєнного стану. Це підкреслює актуальність тематики цієї статті.

Мета статті полягає у визначенні на базі аналізу позитивного зарубіжного досвіду шляхів підвищення ефективності забезпечення кібербезпеки об'єктів критичної інфраструктури держави з використанням інтегрованих технологій ШІ в умовах воєнного стану.

Виклад основного матеріалу дослідження. Питання забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах особливого періоду та воєнного стану викликає жваву дискусію у юридичній літературі**.** Особливу гостроту це питання набуває у зв'язку з агресією рф.

З цього приводу Я. Мануілов пише: «В сучасних умовах стійкі тенденції збільшення кількості загроз національній безпеці у кіберпросторі, які спостерігались протягом останніх років, лише посилились у зв'язку із здійсненням військової агресії РФ проти України. Так, повномасштабне вторгнення російських військ на територію України, що триває із 24 лютого 2022 року, супроводжується численними актами агресії у кіберпросторі. Триває масштабна кібервійна Російської Федерації проти України, важливим елементом якої є також акції кібервпливу, залишаючись найбільшою загрозою національній безпеці держави. В цьому контексті важливою складовою функціонування національної системи кібербезпеки є забезпечення безпеки об'єктів критичної інфраструктури, посилення спроможностей складових сектору безпеки і оборони, державних органів адекватно реагувати на кіберзагрози» [6, с. 155].

Заступник голови Держспецзв'язку О. Потій справедливо підкреслює: «Ворог постійно шукає слабкі місця у системі нашого кіберзахисту. І місцеві органи влади – серед основних цілей російських хакерів. Тож сьогодні як ніколи важливо вміти ефективно і оперативно реагувати на кіберзагрози на всіх рівнях: не тільки на загальнодержавному, а й на регіональному, місцевому» [10].

Схожої точки зору додержується К. Черногоренко, яка зауважує: «Заходи з кібербезпеки повинні бути системними та постійно вдосконалюватись. Тому нова політика передбачає систематичний перегляд та оновлення вимог Міністерства у сфері кібербезпеки» [11].

На важливість вироблення такої політики звертає увагу О. Алексеєва, яка зазначає: «Проблемою є фактична відсутність дієвої узгодженої політики у сфері захисту таких об'єктів, що зумовлюється як відсутністю системного підходу на національному рівні, так і законодавчою невизначеністю форм взаємодії державних органів між собою» [8, с. 169].

Зауважимо, що державна політика у сфері захисту об'єктів критичної інфраструктури та забезпечення їх кібербезпеки формується на основі нормативно-правових актів, які визначають основні принципи, вимоги та процедури кіберзахисту об'єктів критичної інфраструктури. Серед ключових нормативних актів у цій сфері виділяється: Стратегія кібербезпеки України [12], закони України «Про основні засади кібербезпеки України» [13], «Про національну безпеку України» [14], «Про критичну інфраструктуру» [15] тощо.

Законом України «Про критичну інфраструктуру» визначено об'єкти критичної інфраструктури. Це об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [15]. До критичної інфраструктури належать й особливо небезпечні виробництва, аварії на яких викликані будь-якими причинами (природними або техногенними надзвичайними ситуаціями), також можуть обернутися катастрофічними для певних територій і їх населення наслідками [15]. Сьогодні держава активно опікується питаннями впровадження інноваційних інтегрованих технологій для забезпечення об'єктів критичної інфраструктури в умовах кібервійни.

Аналізуючи зміст таких загроз, слід розрізняти їх види. По-перше, це технічні загрози: зловмисне програмне забезпечення, різноманітні типи шкідливого програмного забезпечення, атаки на мережеву інфраструктуру, DDoS-атаки тощо. По-друге, це внутрішні загрози: несанкціоновані дії персоналу, порушення законодавства і політик безпеки тощо. По-третє, це загрози геополітичного характеру: кібертероризм, кібердиверсія, втручання в процеси виробництва або постачання критичних компонентів та послуг тощо.

З приводу останнього слід зауважити, що кіберзагрози геополітичного характеру є найбільш небезпечними, оскільки спрямовані на створення паніки, страху, порушення нормальної життєдіяльності управління та заподіяння значної економічної шкоди шляхом виведення з ладу об'єктів критичної інфраструктури. Йдеться, зокрема, про адресні кібератаки, спрямовані на викрадення конфіденційної інформації, шпигунство за об'єктами критичної інфраструктури, втручання в процеси виробництва або постачання критичних компонентів та послуг для порушення їх функціональності та забезпечення несанкціонованого доступу до основних систем. Зазначені загрози можуть мати руйнівні наслідки для національної безпеки, економіки та суспільства у цілому.

Усі ці загрози зумовлюють потребу вироблення єдиної державної політики у сфері забезпечення кібербезпеки об'єктів критичної інфраструктури, реалізація якої перед-

бачає законодавчі, організаційні, технічні, освітні та інші заходи. Розглянемо більш детально ці заходи.

Серед технічних заходів виділяються: 1) формування системи виявлення та запобігання загрозам (IDS/IPS); 2) сегментація мережі; 3) регулярне оновлення програмного забезпечення та операційних систем; 4) шифрування даних; 5) аутентифікація та управління доступом; 6) резервне копіювання та відновлення; 7) регулярне створення резервних копій критичних даних і планів відновлення.

Організаційні заходи передбачають: 1) наявність спеціальних процедур з кібербезпеки; 2) інцидент-менеджмент, створення та підтримка процедур для виявлення, реагування та усунення наслідків кіберінцидентів; 3) регулярний аудит та тестування; 4) взаємодія приватного сектору з державними органами у сфері кібербезпеки.

Не менш важливими є освітні, правові та превентивні заходи, зміст яких спрямований на: 1) навчання та підвищення компетенції персоналу; 2) зниження ризиків, пов'язаних з атаками соціальної інженерії; 3) контроль та моніторинг поточної ситуації у кіберпросторі; 4) дотримання законодавства у сфері кібербезпеки.

Аналіз цих заходів свідчить про те, що кіберзахищеність об'єктів критичної інфраструктури на основі ШІ вимагає комплексного підходу і потребує особливої уваги в умовах воєнного стану. Створення інтегрованої системи кіберзахисту, здатної протидіяти сучасним інформаційним викликам і кіберзагрозам об'єктів критичної інфраструктури, передбачає: багаторівневий захист, постійний моніторинг, резервне копіювання, навчання персоналу, шифрування даних, контроль доступу, застосування інноваційних технологій, співпрацю з міжнародними партнерами та контроль за дотриманням законодавства.

У зв'язку з цим важливе значення набувають інноваційні аспекти впровадження інтегрованих систем кібербезпеки об'єктів критичної інфраструктури на базі ШІ. Сучасний генеративний ШІ або інтелектуальний ШІ забезпечує багато переваг у сфері кібербезпеки – від автоматизації завдань і зменшення помилок персоналу до використання прогнозової аналітики для підтримки виявлення загроз.

ШІ також необхідний для автоматизації оперативного реагування на інциденти безпеки. Прогнозуючий ШІ може оптимізувати механізм виявлення загроз і створювати ефективні рішення з кібербезпеки, узгоджені з ландшафтом загроз, які постійно змінюється. Ці системи ШІ, по-перше, самоконтролюються та самонавчаються, а, по-друге, можуть застосовувати аналіз у непередбачуваних ситуаціях і приймати рішення на основі власних спостережень. Інтеграція інтелектуальних систем дозволяє автоматизувати виявлення кіберзагроз, а використання алгоритмів машинного навчання підвищує ефективність комплексних заходів з протидії кібератакам.

Застосування ШІ в системі безпеки об'єктів критичної інфраструктури має значний потенціал для підвищення рівня кіберзахисту, про що свідчить аналіз зарубіжного досвіду. Наприклад, Агентство з кібербезпеки та захисту інфраструктури США (Cybersecurity and Infrastructure Security Agency, CISA) використовує ШІ для аналізу мережевої активності, що дозволило знизити час реагування на кіберінциденти на 40%. Держспецзв'язку та CISA – відповідальні органи України та США в сфері безпеки критичної кіберінфраструктури. Їхнє співробітництво, як справедливо відзначив заступник Голови Місії, представник Посольства США в Україні Кевін Коверт: «зразок того, як ми можемо об'єднуватись задля розробки інноваційних стратегій, що просувають наші спільні пріоритети та перешкоджають кіберзагрозам» [16].

Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security, ENISA) застосовує ШІ для прогнозування кіберзагроз, що допомогло знизити кількість атак на об'єкти критичної інфраструктури на 30%. Агентство національної безпеки (National Security Agency, NSA) впровадило системи ШІ для автоматизації виявлення та реагування на кіберзагрози, що зменшило кількість вторгнень на 50% [17, 18].

Наведемо інші приклади. Darktrace Holdings Limited – британська компанія, яка спеціалізується на кібербезпеці, використовує ШІ для виявлення аномальної активності у мережах, що дозволяє знизити кількість кібератак на 92%. Американська компанія IBM (International Business Machines Corporation), Watson for Cyber Security аналізує великі обсяги даних для прогнозування нових типів кіберзагроз, що допомагає скоротити час виявлення кіберзагроз на 60%. У свою чергу, американська компанія Palo Alto Networks, Inc. (American multinational cybersecurity) за допомогою ШІ протидіє фішинговим кібератакам, знижуючи ймовірність фішингових кібератак на 86% [19]. Ці приклади демонструють, як зарубіжні державні органи, неурядові організації та комерційні структури успішно застосовують ШІ для захисту об'єктів критичної інфраструктури та мінімізації збитків від кібератак.

Отже, ШІ відіграє ключову роль у зниженні ризиків кіберзагроз об'єктів критичної інфраструктури завдяки можливостям виявлення аномалій, автоматизації реакцій на інциденти, прогнозування та запобігання кіберзагрозам, покращення аутентифікації користувачів, оптимізації управлінням вразливостями, розпізнавання фішингових кібератак та підтримки у розслідуванні кіберінцидентів. Аналізуючи великі обсяги даних у реальному часі, ШІ забезпечує швидке виявлення та блокування загроз, що підвищує ефективність захисту своїх систем та мінімізує шкоду від кібератак. Надійна кібербезпека стала як ніколи важливою в сучасну цифрову епоху в умовах, що постійно змінюються. Як і в багатьох інших сферах, в перспективі роль ШІ у кібербезпеці стане ще більш важливою [20].

Запровадження ШІ є необхідним еволюційним кроком для забезпечення всебічного, ефективного кіберзахисту з урахуванням економічної доцільності. Його застосування дозволить значно покращити стан забезпечення кібербезпеки, підвищити захищеність інформаційних ресурсів та інформаційно-комунікаційних систем об'єктів критичної інфраструктури держави для того, щоб швидко реагувати на існуючи кіберзагрози, завчасно їх нейтралізувати.

В контексті впровадження інтегрованих систем кіберзахисту важливою є координація між державними органами, приватним сектором і міжнародними партнерами з питань протидії сучасним кіберзагрозам. Слід зауважити, що впровадження інтегрованих систем кіберзахисту інформації та кібербезпеки об'єктів критичної інфраструктури здійснюється з урахуванням: 1) комплексного підходу до захисту об'єктів критичної інфраструктури; 2) централізованого управління кібербезпекою; 3) постійного підвищення фахового рівня персоналу таких об'єктів.

Такий підхід вимагає застосування ШІ для: виявлення та реагування на кіберзагрози в реальному часі; автоматизації заходів кіберзахисту, фахової підготовки персоналу, системного захисту даних; швидкого відновлення після кібератак, а також для сприяння співпраці з міжнародними партнерами у цій сфері. В контексті зазначеного ШІ може аналізувати аномальну поведінку персоналу, автоматично реагувати на інциденти, оновлювати програмне забезпечення, шифрувати дані, здійснювати моніторинг інформації, оцінювати наслідки кібератак та координувати дії відповідних структур.

З цього приводу заслуговує на увагу позитивний досвід провідних країн світу щодо підвищення ефективності забезпечення кіберзахисту об'єктів критичної інфраструктури. У багатьох розвинутих країнах світу, зокрема у США, забезпечення кібербезпеки об'єктів кри-

тичної інфраструктури визнано пріоритетним напрямом політики національної безпеки, в рамках якого активно формуються національні системи із забезпечення кіберзахисту таких об'єктів, ухвалюються законодавчі акти для регламентації діяльності учасників цієї системи, готуються відповідні кадри, налагоджуються партнерські відносини з приватним сектором, здійснюються освітні заходи серед населення тощо. У зв'язку з цим зростає необхідність створення кібервійськ, метою яких є не лише захист об'єктів критичної інфраструктури від кібератак, але й проведення превентивних наступальних операцій у кіберпросторі.

Привертають увагу сформовані на базі аналізу позитивного досвіду США у сфері антитерористичного та кібернетичного захисту об'єктів критичної інфраструктури висновки щодо забезпечення кібербезпеки об'єктів в Україні за такими напрямами: 1) ідентифікації та градації об'єктів критичної інфраструктури; 2) проведення аналізу кіберризиків та узагальнення вимог до рівнів захищеності; 3) аналізу та визначення найбільш ймовірних сценаріїв кібератак на об'єкти критичної інфраструктури; 4) розробки та запровадження системи індикаторів стану кібербезпеки, що включатиме базові індикатори стану кібербезпеки, індикатори розвитку національної системи кібербезпеки та індикатори стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації; 5) розробки актуальних вимог та політик кіберзахисту для об'єктів різного функціонального призначення [9, с. 94].

Впровадження цих напрямів з урахуванням досвіду США підвищить рівень кібербезпеки об'єктів критичної інфраструктури держави. Це дозволить запровадити новітні підходи та технології, які ефективно застосовуються державами-членами НАТО. Такий підхід враховуватиме найкращі європейські практики й світові стандарти та сприятиме подальшій системній інтеграції України до Європейського Союзу та НАТО.

Висновки. Кіберзахищеність об'єктів критичної інфраструктури є критично важливою сферою державної політики у сфері кібербезпеки, забезпечення якої залежить від низки заходів, які можна поділити на технічні, організаційні, правові, превентивні та освітні.

Посилення кіберзахисту об'єктів критичної інфраструктури в умовах активних російських кібератак вимагає застосування комплексного підходу, зміст якого передбачає поєднання інноваційних підходів з комплексом технічних, організаційних, освітніх та міжнародних заходів тощо. Застосування на основі ШІ інноваційних технологій у поєднанні з ефективною координацією дозволить забезпечити надійний захист об'єктів критичної інфраструктури та мінімізувати існуючі ризики кібератак.

На підставі аналізу позитивного досвіду США у сфері кіберзахисту об'єктів критичної інфраструктури вважаємо за доцільне забезпечити в Україні реалізацію таких ключових напрямів: зміцнення партнерства з питань обміну інформацією між зацікавленими органами та забезпечення координації захисних кіберзаходів, розвиток критичної інфраструктури за допомогою залучення інвестицій у модернізацію об'єктів критичної інфраструктури, застосування ШІ для моніторингу та реагування на кіберзагрози, створення центрів реагування на кіберзагрози (SOC), удосконалення законодавства у сфері кібербезпеки України в контексті імплементації міжнародних та європейських стандартів, міжнародна співпраця з питань обміну досвідом та технологіями, у т.ч. забезпечення фахової підготовки та перепідготовки персоналу. Актуальним напрямом залишається запровадження інтегрованих комп'ютерних систем виявлення прихованої і недостовірної інформації шляхом проведення психофізіологічного дослідження із застосуванням поліграфа (polygraph instrument) для перевірки персоналу із критичними рівнями доступу з урахуванням досвіду та стандартів держав-членів НАТО [21, с. 218; 22; 23].

З урахуванням викладеного, а також того, що ключові аспекти інформаційної безпеки базуються на властивостях самої інформації, перспективними вважаємо наступні напрями: 1) врахування під час кіберзахисту властивостей інформації, а також причинно-наслідкових результатів її застосування; 2) забезпечення інформаційної безпеки на основі розвитку інформаційно-комунікаційних технологій і систем, які стосуються кіберзахисту об'єктів критичної інфраструктури; 3) застосування відповідних вітчизняних операційних систем та систем управління базами даних; 4) постійний моніторинг поточної ситуації у кіберпросторі; 5) забезпечення комплексного підходу у протидії кібератакам; 6) запровадження єдиного понятійно-термінологічного апарату у сфері кібербезпеки; 7) дослідження потенціалу кібердипломатії та її впливу на майбутнє міжнародних відносин в умовах швидкого технологічного прогресу; 8) удосконалення нормативно-правового забезпечення у сфері кібербезпеки, зокрема, шляхом доповнення Стратегії кібербезпкеки України новими заходами із застосуванням ШІ для: своєчасного виявлення кіберзагроз, системного оновлення програмного забезпечення, підвищення кваліфікації персоналу, захисту даних за допомогою шифрування та моніторингу, швидкого відновлення систем після кібератак та сприяння співпраці з міжнародними партнерами. Впровадження цих напрямів сприятиме ефективному захисту об'єктів критичної інфраструктури Україні від кібератак в умовах воєнного стану.

Отже, застосування ШІ – це перспективний інноваційний напрям у сфері інформаційної безпеки, який зумовлює запровадження інтегрованих інформаційно-аналітичних систем на основі ШІ для підвищення ефективності кіберзахисту, оперативного реагування та протидії кібератакам на об'єкти критичної інфраструктури держави [24].

Перспективними вбачаються подальші наукові розвідки у сфері кібербезпеки та інформаційної безпеки: зміцнення кіберзахисту від ворожих дестабілізаційних операцій, забезпечення координації діяльності усіх суб'єктів забезпечення кібербезпеки, а також розвиток спроможності ударного кіберпотенціалу країни для забезпечення кібербезпеки об'єктів критичної інфраструктури на основі ШІ. Передусім, це стосується подальшого пошуку балансу щодо фахової взаємодії персоналу з ШІ та формування державно-правових гарантій захисту прав, свобод і безпеки людини в умовах розвитку і застосування інформаційних технологій на основі ШІ.

ЛІТЕРАТУРА

1. Пилипчук В. Г., Андрійович Б.О., Гиляка О.С. Проблема правового регулювання у сфері ШІ в контексті розвитку законодавства Європейського союзу. *Вісник Національної академії правових наук України.* 2022. № 2. С. 36–62. URL: http://visnyk.kh.ua/uk/article/problema-pravovogo-regulyuvannya-u-sferi-shtuchnogo-intelektu-v-konteksti-rozvitku-zakonodavstva-yevropeyskogo-soyuzu.

2. Державна служба спеціального зв'язку та захисту інформації України. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. Новини. 08.02.2024. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti.

3. Кібербезпека в інформаційному суспільстві. Інформаційно-аналітичний дайджест. *Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»*. 2024. № 2 (лютий). 253 с. URL: https://ippi.org.ua/sites/default/files/2024-2.pdf.

4. Кучерина С.Є., Олейніков Д.О. Сучасний стан кримінально-правової охорони об'єктів критичної інфраструктури. *Інформація і право*. 2021. № 1(36). С. 90–98.

5. Суходоля О.М. Захист критичної інфраструктури в умовах гібридної війни: проблеми та пріоритети державної політики України. *Стратегічні пріоритети*. 2016. № 3. С. 62–76.

6. Мануілов Я.С., Забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах кібервійни. *Інформація і право*. 2023. № 1(44). С. 154–167. URL:https://ippi.org.ua/manuilov-yas-zabezpechennya-kiberbezpeki-ob%E2%80%99%D1%94ktiv-kritichnoi-infrastrukturi-v-umovakh-kiberviini-s-1

7. Цяпа С.М. Правове та організаційне забезпечення захисту об'єктів критичної інформаційної інфраструктури від кібератак. *Інформація і право*. 2021. № 4(39). С. 121–128.

8. Алексеєва О.А. Правове забезпечення кібербезпеки об'єктів критичної інфраструктури. *Інформація і право*. 2023. № 4(47) С. 169–176. URL: http://il.ippi.org.ua/article/view/291633.

9. Леонов Б.Д., Шостак Р.М., Серьогін В.С. Розвиток методичного забезпечення антитерористичної захищеності об'єктів критичної інфраструктури (на прикладі США). *Інформація і право*. 2020. № 3(34). С. 94–99. URL: https://ippi.org.ua/sites/default/files/12_18.pdf.

10. Кіберзахист у місцевих органах влади: Держспецзв'язку провела кібернавчання «CIREX. CYBER. Ransomware». Новини. 22.06.2023. URL: https://cip.gov.ua/ua/news/kiberzakhist-u-miscevikh-organakh-vladi-derzhspeczv-yazku-provela-kibernavchannya-cirex-cyber-ransomware.

11. Єдині стандарти кібербезпеки: Міноборони зміцнює захист інформаційних систем у відповідності до стандартів НАТО. Новини. 22.04.2024. URL: https://www.mil.gov.ua/news/2024/04/22/i-minoboroni-uhvalilo-nakaz/.

12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.2021 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

14. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

15. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882. URL: https://ips.ligazakon.net/document/T211882

16. Держспецзв'язку та Агентство з кібербезпеки та захисту інфраструктури США відзначили першу річницю співпраці. Новини. 15.08.2023. URL: https://armyinform.com.ua/2023/08/15/derzhspeczzvyazku-ta-agentstvo-z-kiberbezpeky-ta-zahystu-infrastruktury-ssha-vidznachyly-pershu-richnyczyu-spivpraczi/.

17. Security Intelligence (CNAS). URL: https://securityintelligence.com/articles/security-automation-save-data-breach/

18. Soldier Systems Daily. URL: https://soldiersystems.net/2023/12/24/nsa-focuses-on-talent-as-pace-of-technology-quickens/.

19. Palo Alto Networks, Inc. URL: https://www.paloaltonetworks.com/.

20. American Chamber of Commerce in Ukraine. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. *BDO Global*. 05.02.2024. URL: https://chamber.ua/ua/news/rol-shtuchnoho-intelektu-v-kiberbezpetsi-peredbachennia-ta-zapobihannia-atakam/

21. Казьмірук С.Д., Морган К.Ч., Міщенко В.О. Правові основи запровадження інноваційних систем виявлення прихованої і недостовірної інформації та комп'ютерних поліграфів у секторі безпеки і оборони України. *Часопис Київського університету права*. 2022. №1. С. 218-221. URL: https://chasprava.com.ua/index.php/journal/issue/view/86/108

22. American Polygraph Association. URL: https://www.polygraph.org/.

23. ASTM International. URL: https://www.astm.org/.

24. Microsoft. Визначення ШІ для кібербезпеки. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-ai-for-cybersecurity