УДК 004.89
JEL: D83; D89; L86; M15
DOI: https://doi.org/10.32983/2222-4459-2024-1-81-86

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ЕРУ ШТУЧНОГО ІНТЕЛЕКТУ: АНАЛІЗ ТЕХНОЛОГІЧНИХ ПІДХОДІВ ТА СТРАТЕГІЙ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

©2024 ЯЩИК О. Б., СИМОНОВ В. В., ІВАНЕНКО Р. О.

УДК 004.89
JEL: D83; D89; L86; M15

Ящик О. Б., Симонов В. В., Іваненко Р. О. Забезпечення кібербезпеки в еру штучного інтелекту: аналіз технологічних підходів та стратегій для захисту інформації

Технології машинного навчання мають потенціал значно покращити якість життя людей, автоматизуючи повсякденні завдання та надаючи нові можливості для творчості та інновацій. Проте зростання використання штучного інтелекту викликає занепокоєння щодо безпеки особистих даних користувачів та конфіденційних розробок певних компаній. При використанні цього інструменту важливо усвідомлювати потенційні ризики для інформаційної та кібербезпеки. Метою статті є аналіз забезпечення кібербезпеки в еру штучного інтелекту та технологічних підходів і стратегій захисту інформації. Проаналізовано Стратегію кібербезпеки України, схвалену Указом Президента України від 26 серпня 2021 р. Визначено, що штучний інтелект спричиняє як позитивні, так і негативні наслідки в кібербезпеці, оскільки він може або посилити процес кібератак, викликаючи більш швидкі та шкідливі атаки, або навпаки – підвищити кібербезпеку. Основними загрозами штучного інтелекту для кібербезпеки є вразливість, порушення конфіденційності, атаки різного типу. Розповсюдження штучного інтелекту створює загрозу розголошення конфіденційної інформації під час збору та обробки даних, що потребує введення відповідних заходів безпеки на всіх етапах використання технології. Загалом використання штучного інтелекту вимагає не лише інноваційних підходів, але й посилення заходів безпеки для захисту від різноманітних кіберзагроз. Встановлено, що можливості штучного інтелекту можуть бути використані в кібербезпеці, що може сприяти зміцненню захисту для організацій та зменшити навантаження відповідних фахівців. Інструменти, побудовані на основі штучного інтелекту, дозволяють автоматизувати рутинні завдання у сфері безпеки, звільняючи час експертів для вирішення найважливіших завдань. Зроблено висновок, що загалом потенціал штучного інтелекту може бути використаний для зміцнення кібербезпеки, але необхідно впроваджувати нові закони, які регулюватимуть його функціонування.

Ключові слова: *системи штучного інтелекту, інформаційна безпека, кіберзлочини, стратегії захисту, кібербезпека.*
Рис.: *1.* ***Бібл.:*** *11.*

Ящик Олександр Богданович *– кандидат педагогічних наук, доцент, доцент кафедри комп'ютерних технологій, Тернопільський національний педагогічний університет імені Володимира Гнатюка (вул. Максима Кривоноса, 2, Тернопіль, 46027, Україна)*
E-mail: *sanytnpu@gmail.com*
ORCID: *https://orcid.org/0000-0002-8420-3336*
Researcher ID: *https://www.webofscience.com/wos/author/record/I-6291-2018*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57219596072*

Симонов В'ячеслав Володимирович *– магістр, керівник проєктів, Mobios Digital Agency (вул. Середньофонтанська, 19А, Одеса, 65039, Україна)*
E-mail: *viacheslav.digital@gmail.com*
ORCID: *https://orcid.org/0009-0001-4146-5870*

Іваненко Руслан Олександрович *– старший науковий співробітник, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України (вул. Василенка, 3, Київ, 03113, Україна)*
E-mail: *indior@ukr.net*
ORCID: *https://orcid.org/0000-0002-1447-6275*

UDC 004.89
JEL: D83; D89; L86; M15

Yashchyk O. B., Symonov V. V., Ivanenko R. O. Ensuring Cybersecurity in the Era of Artificial Intelligence: Analysis of Technological Approaches and Strategies for Information Protection

Technologies based on machine learning are gradually being introduced as a new means of automation of everyday and routine tasks, providing new opportunities for creativity and innovation. However, the growing use of artificial intelligence raises concerns about the security of personal data of users and the confidential developments of certain companies. When using this tool, it is important to be aware of the potential risks to information and cybersecurity. The purpose of the article was to analyze the issue of ensuring cybersecurity in the era of artificial intelligence and technological approaches and strategies for information protection. The Cybersecurity Strategy of Ukraine, which was approved by the Decree of the President of Ukraine dated August 26, 2021, was analyzed. Artificial intelligence has been identified as having both positive and negative effects in cybersecurity, as it can either enhance the cyber attack process, causing faster and more damaging attacks, or conversely, improve cybersecurity. The main threats of artificial intelligence for cybersecurity are vulnerability, privacy, attacks of various types. The spread of artificial intelligence creates a threat of disclosure of confidential information during data collection and processing, which requires the introduction of appropriate security measures at all stages of technology use. In general, the use of artificial intelligence requires not only innovative approaches, but also increased security measures to protect against various cyber threats. It is found that the capabilities of artificial intelligence can be used in cybersecurity, which can contribute to the strengthening of protection for organizations and reduce the workload of relevant specialists. The tools built on the basis of artificial intelligence allow you to automate routine tasks in the field of security, freeing up the time of experts to solve the most important tasks. In general, the potential of artificial intelligence can be used to strengthen cybersecurity, but it is necessary to implement new laws that will regulate its operation.

Keywords: *artificial intelligence systems, information security, cybercrimes, defense strategies, cybersecurity.*
Fig.: *1.* ***Bibl.:*** *11.*

Yashchyk Oleksandr B. *– PhD (Pedagogy), Associate Professor, Associate Professor, Department of Computer Technologies, Ternopil Volodymyr Hnatyuk National Pedagogical University (2 Maksyma Kryvonosa Str., 46027, Ukraine)*
E-mail: *sanytnpu@gmail.com*
ORCID: *https://orcid.org/0000-0002-8420-3336*
Researcher ID: *https://www.webofscience.com/wos/author/record/I-6291-2018*
Scopus Author ID: *https://www.scopus.com/authid/detail.uri?authorId=57219596072*
Symonov Viacheslav V. *– Master's Degree, Project Manager, Mobios Digital Agency (19A Serednofontanska Str., Odesa, 65039, Ukraine)*
E-mail: *viacheslav.digital@gmail.com*
ORCID: *https://orcid.org/0009-0001-4146-5870*
Ivanenko Ruslan O. *– Senior Research Fellow, Ukrainian Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine (3 Vasylenka Str., Kyiv, 03113, Ukraine)*
E-mail: *indior@ukr.net*
ORCID: *https://orcid.org/0000-0002-1447-6275*

Нині інформаційна безпека вважається ключовим компонентом національної безпеки будь-якої країни. Епоха цифрового інформаційного суспільства привела до значних змін, але вона також внесла свою частку негативних трансформацій. Одним із головних викликів сучасності є загроза кіберінцидентів, які іноді набувають великих масштабів. Наявність кіберзлочинів у системі свідчить про активний розвиток кібератак або вже їх фактичне здійснення. Наслідки кібератак можуть призвести до серйозних порушень інформаційної безпеки, включно з незаконним доступом до даних, їх зміною або знищенням.

Втім, технологія штучного інтелекту стрімко розвивається та має потенціал для значного поліпшення різних аспектів життєдіяльності людей. Штучний інтелект має потенціал для революції в галузі комп'ютерних систем і мереж, але також створює нові виклики у сфері безпеки, на які слід звернути увагу.

Дослідженню кібербезпеки та захисту інформацію присвячені деякі праці вітчизняних науковців. Так, А. Омельченко у своїй праці відзначив, що забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Питома вага кіберзагроз зростає, і ця тенденція за ступенем розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту посилюватиметься [7].

О. Неретін і В. Харченко класифікували можливі типи атак і детально розглянули основні з них. Автори зробили висновок, що існує потреба у формалізації та стандартизації життєвого циклу розроблення та використання безпечних систем штучного інтелекту [6].

Є. Криволап наголосив на стратегіях інформаційної кібербезпеки та визначив, що прийняті у 2020–2021 рр. безпекові Стратегії України є логічно взаємопов'язаними документами, реалізація яких ґрунтується на застосуванні механізмів забезпечення відповідної безпеки України [3].

К. Мовчан запропонував комплексний підхід до кібербезпеки роботів, який містить аналіз загроз, розробку методів протидії атакам і впровадження заходів безпеки. Він також зазначив, що для забезпечення цілісності, доступності та конфіденційності рекомендується посилити шифрування, авторизацію/автентифікацію та забезпечити фізичний захист. Це допоможе уникнути перехоплення інформації, несанкціонованого доступу до роботів, а також упровадження шкідливих даних і програм [5].

Метою статті є розгляд і дослідження аспектів забезпечення кібербезпеки в умовах активного поширення штучного інтелекту.

Для дослідження питання забезпечення кібербезпеки та інформаційної безпеки в еру штучного інтелекту були використані стандартні методи наукових досліджень, такі як аналіз, синтез, систематизація, декомпозиція та узагальнення. Метод аналізу дозволив виявити й описати ключові виклики та потенційні загрози, пов'язані з використанням штучного інтелекту в системах інформаційної безпеки. Синтез був використаний для розробки нових методів захисту інформації, які враховують особливості штучного інтелекту. Метод систематизації дозволив розробити нову класифікацію аспектів кібербезпеки в контексті штучного інтелекту. Декомпозиція дозволила розчленувати складні проблеми на окремі, більш зрозумілі та простіші складові, що сприяло їхньому глибшому розумінню. За допомогою методу узагальнення було зроблено висновки про загальні закономірності, які можуть бути використані для подальших досліджень.

Мережа Інтернет за час свого існування пройшла складний шлях розвитку – від початкових

прототипів до сучасної глобальної мережі. Постійні модернізації приводять до поліпшення принципів роботи та алгоритмів побудови самої системи. Сучасна інформаційна система є складною та розгалуженою мережею, яка об'єднує мільярди пристроїв. Вона використовує велику кількість маршрутизаторів і канальних з'єднань, що робить її вразливою до втрати, перехоплення та зміни даних. Ці загрози становлять глобальну проблему, яка потребує постійної уваги та вдосконалення методів її запобігання. Одним із напрямків захисту інформації в інформаційних системах є технічний захист інформації.

Шифрування та дешифрування даних, які використовують криптографічні методи під час їх передачі транспортним каналом, є дієвим засобом запобігання несанкціонованому доступу до інформації. Метод ґрунтується на процесі шифрування на вихідному пристрої, передачі через фізичний канал і розшифрування на приймальному пристрої, і таким чином ускладнює можливість втручання або модифікації даних зловмисниками [4].

Кібербезпека є однією з ключових проблем для будь-якої організації, оскільки існує ризик, що великі обсяги даних і конфіденційна інформація можуть стати об'єктом онлайн-атак з боку хакерів. З розвитком технологій та активізацією глобалізації особиста та фінансова інформація компаній зберігається в хмарних сервісах, і через зростання залежності від цифрових технологій кібератаки стають більш поширеними [1].

До об'єктів кібербезпеки належать:

- конституційні права і свободи людини та громадянина;
- держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;
- суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;
- національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;
- об'єкти критичної інфраструктури [7].

Президент України взаємодіє з Радою національної безпеки та оборони України для координації заходів у сфері кібербезпеки, яка є важливою складовою національної безпеки країни.

Відомо, що стратегія являє собою план дій, спрямований на досягнення конкретної візії або довгострокової мети. У випадку національних стратегій кібербезпеки йдеться про національний план дій, що визначається національною візією з метою досягнення довгострокових цілей у підвищенні рівня безпеки в інформаційній сфері [2].

У новій Стратегії кібербезпеки України, яка була схвалена Указом Президента України від 26 серпня 2021 р., підкреслено, що гарантування кібербезпеки є одним із пріоритетів національної безпеки України. Виконання цього пріоритету передбачає посилення потужностей національної системи кібербезпеки для протистояння кіберзагрозам у сучасному безпековому оточенні [9].

Нині в Україні спостерігається активне впровадження новітніх досягнень комп'ютерних і телекомунікаційних технологій внаслідок вступу у світовий інформаційний простір.

Втім, штучний інтелект являє собою сукупність теоретичних і практичних підходів у галузі інформаційних технологій, спрямованих на створення систем, які можуть операційно діяти та приймати розумні рішення, аналогічно механізму прийняття рішень у мозку людини. З використанням нейромереж і штучного інтелекту машина може навчитися ефективно обробляти та аналізувати великі обсяги інформації в короткі терміни. Основними напрямками використання штучного інтелекту в сучасному світі є такі (*рис. 1*).

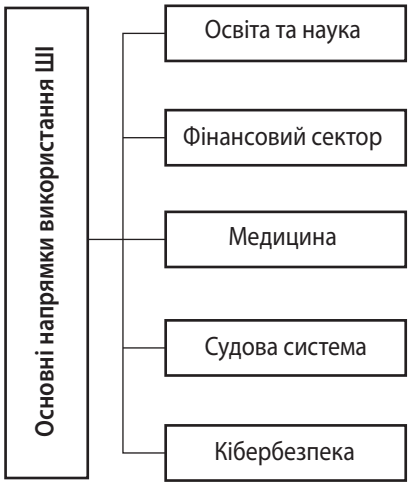

Рис. 1. Основні напрямки використання штучного інтелекту (ШІ)

Джерело: сформовано на основі [10].

Штучний інтелект і робототехніка тісно пов'язані між собою, оскільки робототехніка часто використовує штучний інтелект для управління своїми діями. У міру зростання популярності роботів важливо розуміти їхні вразливості та потенційні загрози, щоб забезпечити безпеку як людей, так і машин. Аналізуючи наявні атаки та ризики для робототехніки, К. Мовчан наголосив на необхідності поліпшення заходів безпеки, таких як автентифікація, авторизація, шифрування та фізичний захист, для пом'якшення несанкціонованого

доступу, маніпулювання даними та встановлення програмного забезпечення. Алгоритми машинного навчання, статистичні методи та техніки розпізнавання образів широко використовуються для виявлення кібератак та аналізу їхніх наслідків [5].

Системи на основі штучного інтелекту є вразливими перед різними загрозами безпеки на всіх етапах свого життєвого циклу, починаючи від збору даних і закінчуючи впровадженням. На етапах збору даних і попередньої обробки вони піддаються атакам на підробку даних і масштабування, а на етапах діагностики та впровадження – вірусним атакам і атакам хакерів. Використання штучного інтелекту, такого як ChatGPT та інші, дозволяє кіберзлочинцям автоматизувати та масштабувати свої атаки, що робить їх ефективнішими.

Штучний інтелект, який все більше використовується в різних сферах, створює нові виклики для безпеки, зокрема загрозу розголошення конфіденційної інформації при зборі та обробці даних. Ключовим аспектом захисту конфіденційності даних є впровадження відповідних заходів безпеки, таких як правила щодо обробки конфіденційної інформації. Згідно з вимогами безпеки фахівці певної компанії повинні використовувати лише програмне забезпечення та інструменти, які є схваленими компанією, а не надані зловмисником, тобто важливим є використання ліцензійного програмного забезпечення. ChatGPT або інші загальнодоступні інструменти штучного інтелекту не мають дозволу на обробку чи вирішення завдань, що стосуються конфіденційної інформації компанії та її клієнтів.

Ці інструменти миттєво генерують текст, що схожий на природну мову, дозволяючи зловмисникам переконливо імітувати стиль комунікації довірених осіб чи організацій і підвищувати ефективність своїх атак. Навіть за наявності певних заходів захисту кіберзлочинці можуть обійти та використовувати штучний інтелект для оптимізації створення шкідливого програмного забезпечення та автоматизації атак.

Штучний інтелект, що використовується в різних сферах діяльності, підвищує ризик розголошення чутливих даних. Тому для захисту конфіденційності даних необхідно впроваджувати комплексні заходи кібербезпеки. Компаніям, які впроваджують ШІ, варто зосередитися на таких заходах кібербезпеки, як:

- безпека кінцевих точок;
- безпечний зв'язок;
- шифрування даних;
- управління вразливостями.

Вразливості систем штучного інтелекту пов'язані з їхньою складністю та відсутністю прозорості, що робить їх легкою мішенню для зловмисників. Прикладом цього є дослідження команди McAfee Advanced Threat Research, яка скористалася недоліками в програмному забезпеченні автопілота «Tesla», змусивши його розганятися до 85 миль на годину замість встановленої швидкості 35 миль на годину [6]. Загалом вразливості систем штучного інтелекту поділяються на дві основні групи:

1) «традиційні» вразливості програмного забезпечення (ПЗ) (атаки на інструментарій);
2) специфічні типи вразливостей, які притаманні тільки складним системам ШІ.

Штучний інтелект охоплює різноманітні суміжні області та технології, такі як:

- машинне навчання;
- глибоке навчання;
- нейронні мережі;
- обробка природних мов та інші.

Беззаперечним є факт, що такі можливості штучного інтелекту можуть бути використані в кібербезпеці. Обсяг даних, які швидко генеруються в сучасному світі, зростає, і ця інформація передається та зберігається в різних формах, використовуючи мережу Інтернет. З розвитком цього процесу кіберпростір стає своєрідним сучасним полігоном для проведення воєнних дій. Виділяється також тенденція до створення кібервійськ, які включають завдання не лише захисту критичної інформаційної інфраструктури від кібератак, але й проведення превентивних операцій у кіберпросторі, таких як виведення з ладу критично важливих об'єктів інфраструктури шляхом руйнування інформаційних систем, що керують такими об'єктами [3].

Застосування штучного інтелекту в кібербезпеці може сприяти укріпленню захисту для організацій та зменшити навантаження відповідних фахівців. Інструменти, побудовані на основі штучного інтелекту, дозволяють автоматизувати рутинні завдання у сфері безпеки, звільняючи час експертів для вирішення найважливіших завдань.

Зростання обсягу інформації, яка генерується та передається в інформаційному просторі, сприяє збільшенню кількості кіберзлочинів. Для забезпечення інформаційної та кібербезпеки використовується штучний інтелект, оскільки він може автоматизовано та негайно реагувати на розвиток та модифікацію кіберзагроз. Використання штучного інтелекту для підвищення рівня інформаційної безпеки має різноманітні напрямки. Якщо йдеться про захист програмного забезпечення, ефективним методом виявлення шкідливого програмного

коду є використання алгоритмів машинного навчання [10].

У рішеннях з кібербезпеки застосовуються різноманітні види програм, які використовують технології штучного інтелекту. Серед них – системи SIEM, різноманітні фільтри спаму, інструменти захищеної автентифікації користувачів та засоби прогнозування інцидентів злому. Ці програми навчаються за допомогою бази даних попередньої поведінки та можуть ідентифікувати кожну окрему поведінку як шкідливу чи безпечну [11].

Нині для забезпечення безпечного та ефективного використання штучного інтелекту необхідно впроваджувати нові закони, які регулюватимуть його функціонування. Також важливо створити передові системи моніторингу, які будуть передбачати ризики, пов'язані із взаємодією людей зі штучним інтелектом.

ВИСНОВКИ

Розвиток технологій штучного інтелекту є важливим трендом сучасності, на який звертають увагу провідні компанії та держави. Проте не менш важливим є питання забезпечення кібербезпеки та захисту інформації. Питома вага кіберзагроз збільшується, і ця тенденція буде зміцнюватися в найближчому десятилітті, оскільки розвиток інформаційних технологій та їх інтеграція з технологіями штучного інтелекту формують нову безпекову ситуацію для функціонування як національних, так і транснаціональних структур країни.

Штучний інтелект чинить як позитивні, так і негативні впливи на кібербезпеку. Це може привести як до посилення процесів кібератак, зумовлюючи швидкі та шкідливі атаки, так і до підвищення рівня кібербезпеки. Використання штучного інтелекту вимагає не лише новаторських підходів, але й усіх можливих заходів безпеки для протидії різноманітним кіберзагрозам. Проте можливості штучного інтелекту можуть бути використані для поліпшення кібербезпеки, сприяючи укріпленню захисту організацій та зменшенню труднощів для відповідних фахівців.

Перспективами подальших досліджень може бути аналіз можливих слабкостей і вразливостей алгоритмів машинного навчання для розробки вдосконалених методів захисту. ■

БІБЛІОГРАФІЯ

1. Кісь А. А. Безпека комп'ютерних систем при використанні технологій штучного інтелекту. *Proceedings of the 14th International Scientific and Practical Conference «Scientific Research in XXI Century»* (July 16–18, 2023). Ottawa, Canada. 2023. No. 162. С. 246–248. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/4066/4103
2. Котух Є. В. Національні стратегії кібербезпеки: порівняльний аналіз. *Актуальні проблеми державного управління*. 2021. № 1. С. 32-42. DOI: https://doi.org/10.34213/ap.21.01.04
3. Криволап Є. В. Вплив Стратегій інформаційної та кібербезпеки на інші безпекові стратегії України // Матеріали VI Міжнародного молодіжного наукового юридичного форуму (м. Київ, 18 травня 2023 р.). Київ, 2023. С. 120–122. URL: https://er.nau.edu.ua/handle/NAU/59616
4. Кушнарьов В. В. Національна система кібербезпеки України: виклики та кіберзагрози // Інформація, комунікація та управління знаннями в глобалізованому світі : збірник матеріалів П'ятої міжнар. наук. конф. (м. Київ, 23–24 червня 2022 р.). Київ, 2022. С. 29–33. URL: https://knukim.edu.ua/wp-content/uploads/2022/06/28.06.22-_Zbirnyk-materialiv_-2022-1.pdf#page=29
5. Мовчан К. О. Ризики кібербезпеки в епоху робототехніки. *Вчені записки ТНУ імені В. І. Вернадського. Серія «Технічні науки»*. 2023. Т. 34. № 4. С. 79–83. DOI: https://doi.org/10.32782/2663-5941/2023.4/13
6. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. *Вісник Національного університету «Львівська політехніка»*. 2022. Вип. 12. С. 7–22. DOI: https://doi.org/10.23939/sisn2022.12.007
7. Омельченко А. В. Організаційно-правові засади забезпечення кібербезпеки України. *Київський часопис права*. 2022. № 3. С. 140–145. DOI: https://doi.org/10.32782/klj/2021.3.22
8. Солдатова М. О., Вітюк А. Є., Мартинюк А. С., Чернобородюк В. Д. Перспективи використання штучного інтелекту в кібербезпеці. *The 9th International scientific and practical conference «Innovations and prospects of world science»* (April 28–30, 2022). Perfect Publishing, Vancouver, Canada, 2022. P. 256–259. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/40786/1/INNOVATIONS-AND-PROSPECTS-OF-WORLD-SCIENCE-28-30.04.22.pdf#page=256
9. Указ Президента України «Про рішення Ради національної безпеки та оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
10. Шаров С. В. Сучасний стан розвитку штучного інтелекту та напрямки його використання. *Українські студії в європейському контексті*. 2023. № 6. С. 136–144. URL: http://obrii.org.ua/usec/storage/conference/zb_vol6_2023.pdf#page=137
11. Yushko A., Shevchuk R., Łopaciński K. et al. Shielding Web Application against Cyber-Attacks using SIEM. *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*. Wrocław, Poland, 21–23 September 2023. DOI:https://doi.org/10.1109/acit58437.2023.10275630

REFERENCES

Kis, A. A. "Bezpeka kompiuternykh system pry vykorystanni tekhnolohii shtuchnoho intelektu" [Security of Computer Systems When Using Artificial Intelligence Technologies]. *Scientific Research in XXI Century*, no. 162 (2023): 246-248. https://archive.interconf.center/index.php/conference-proceeding/article/view/4066/4103

Kotukh, Ye. V. "Natsionalni stratehii kiberbezpeky: porivnialnyi analiz" [National Cybersecurity Strategies: Comparative Analysis]. *Aktualni problemy derzhavnoho upravlinnia*, no. 1 (2021): 32-42. DOI: https://doi.org/10.34213/ap.21.01.04

Kryvolap, Ye. V. "Vplyv Stratehii informatsiinoi ta kiberbezpeky na inshi bezpekovi stratehii Ukrainy" [Impact of Information and Cyber Security Strategies on Other Security Strategies of Ukraine]. *Materialy VI Mizhnarodnoho molodizhnoho naukovoho yurydychnoho forumu* (2023): 120-122. https://er.nau.edu.ua/handle/NAU/59616

Kushnaryov, V. V. "Natsionalna systema kiberbezpeky Ukrainy: vyklyky ta kiberzahrozy" [National Cyber Security System of Ukraine: Challenges and Cyber Threats]. *Informatsiia, komunikatsiia ta upravlinnia znanniamy v hlobalizovanomu sviti* (2022): 29-33. https://knukim.edu.ua/wp-content/uploads/2022/06/28.06.22-_Zbirnyk-materialiv_-2022-1.pdf#page=29

[Legal Act of Ukraine] (2021). https://zakon.rada.gov.ua/laws/show/447/2021#Text

Movchan, K. O. "Ryzyky kiberbezpeky v epokhu robototekhniky" [Cybersecurity Risks in the Age of Robotics]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia «Tekhnichni nauky»*, vol. 34, no. 4 (2023): 79-83. DOI: https://doi.org/10.32782/2663-5941/2023.4/13

Neretin, O., and Kharchenko, V. "Zabezpechennia kiberbezpeky system shtuchnoho intelektu: analiz vrazlyvostei, atak i kontrzakhodiv" [Ensurance of Artificial Intelligence Systems Cyber Security: Analysis of Vulnerabilities, Attacks and Countermeasures]. *Visnyk Natsionalnoho universytetu «Lvivska politekhnika»*, no. 12 (2022): 7-22. DOI: https://doi.org/10.23939/sisn2022.12.007

Omelchenko, A. V. "Orhanizatsiino-pravovi zasady zabezpechennia kiberbezpeky Ukrainy" [Organizational and Legal Bases of Cybersecurity of Ukraine]. *Kyivskyi chasopys prava*, no. 3 (2022): 140-145. DOI: https://doi.org/10.32782/klj/2021.3.22

Sharov, S. V. "Suchasnyi stan rozvytku shtuchnoho intelektu ta napriamky yoho vykorystannia" [The Current State of Artificial Intelligence Development and Directions of Its Use]. *Ukrainski studii v yevropeiskomu konteksti*, no. 6 (2023): 136-144. http://obrii.org.ua/usec/storage/conference/zb_vol6_2023.pdf#page=137

Soldatova, M. O. et al. "Perspektyvy vykorystannia shtuchnoho intelektu v kiberbezpetsi" [Prospects for the Use of Artificial Intelligence in Cyber Security]. *Innovations and prospects of world science* (2022): 256-259. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/40786/1/INNOVATIONS-AND-PROSPECTS-OF-WORLD-SCIENCE-28-30.04.22.pdf#page=256

Yushko, A. "Shielding Web Application against Cyber-Attacks using SIEM". *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*. Wroclaw, Poland, 2023. DOI:https://doi.org/10.1109/acit58437.2023.10275630