DOI: [10.32702/2307-2156-2022.1.2](https://doi.org/10.32702/2307-2156-2022.1.2)

УДК 004.8:354

З. В. Гбур,
д. держ. упр., професор,
професор кафедри управління охороною здоров'я та публічного адміністрування,
Національний університет охорони здоров'я України імені П.Л. Шупика
ORCID ID: 0000-0003-4536-2438

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

Z. Hbur
Doctor of Sciences in Public Administration, Full Professor, Professor of the Department of
Healthcare Management and Public Administration, Shupyk National Healthcare University of
Ukraine Kyiv, Ukraine

USE OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY IN UKRAINE

Статтю присвячено обґрунтуванню використання технологій штучного інтелекту в інформаційній безпеці України в умовах внутрішніх та зовнішніх загроз. Визначено, що інформаційна безпека це захищений інформаційний простір, який здатен забезпечити реалізацію загальнонаціональних інтересів та збереження стійкості держави до внутрішніх та зовнішніх чинників, що становлять загрозу та пов'язані із активним розвитком діджиталізації. В даний час проблеми забезпечення ефективної інформаційної безпеки держави й суспільства, набувають великого значення у вітчизняній національній політиці та державному управлінні. Доведено, що технології штучного інтелекту надають можливість створювати рішення більш високої ефективності, що дозволяють ідентифікувати з високою швидкістю кібератаки, обирати оптимальну відповідь на інциденти безпеки, в автоматичному режимі проводити оцінку актуальності та наслідків інцидентів, в реальному часі виробляти пропорційну відповідь. Визначено, що інтелектуальні системи позбавлені недоліків людського чиннику: вони працюють швидше та помиляються значно рідше за людей. Штучний інтелект дозволяє практично повністю виключити людину з процесу забезпечення захисту інформаційної безпеки та залишає йому допоміжні функції моніторингу та корекції. Розглянуто основні типи технологій штучного інтелекту в системі інформаційної безпеки, що виявляють та нейтралізують кібератаки. Доведено, що розвиток та використання штучного інтелекту на сучасному етапі актуалізує стратегію, яка дозволяє застосовувати комплексні заходи для задоволення інтересів людини, суспільства та держави в інформаційній безпеці для створення найбільш сприятливих мір ефективної протидії зовнішнім та внутрішнім загрозам. В статті доведено, що в сучасному високотехнологічному середовищі державі потрібна надійна інформація для встановлення високих стандартів, покращення протоколів безпеки, а також забезпечення безпеки конфіденційної інформації. Прийняття рішень за допомогою технологій штучного інтелекту допомагає знаходити загрози, попереджувати ризики та виконувати відповідні дії. Більш того, методи штучного інтелекту та машинного навчання відіграють вирішальну роль у покращенні протоколів інформаційної безпеки.

The article is devoted to the substantiation of the use of artificial intelligence technologies in the information security of Ukraine in the conditions of internal and external threats. It is determined that information security is a protected information space that is able to ensure the realization of national interests and maintaining the resilience of the state to internal and external factors that pose a threat and are associated with the active development of digitalization. At present, the problems of ensuring effective information security of the state and society are becoming increasingly important in domestic national policy and public administration. Artificial intelligence technologies have been proven to provide higher efficiency solutions that allow high-speed cyberattacks, select the optimal response to security incidents, automatically assess the relevance and consequences of incidents, and produce a proportional response in real time. It has been determined that intelligent systems are free from the shortcomings of the human factor: they work faster and make mistakes much less often than humans. Artificial intelligence allows almost complete exclusion of a person from the process of information security protection and leaves him the auxiliary functions of monitoring and correction. The main types of artificial intelligence technologies in the information security system that detect and neutralize cyber attacks are considered. It is proved that the development and use of artificial intelligence at the present stage actualizes the strategy that allows to apply comprehensive measures to meet the interests of man, society and the state in information security to create the most favorable measures to effectively combat external and internal threats. The article proves that in today's high-tech environment, the state needs reliable information to set high standards, improve security protocols, and ensure the security of confidential information. Decision-making using artificial intelligence technologies helps to identify threats, prevent risks and take appropriate action. Moreover, artificial intelligence and machine learning techniques play a crucial role in improving information security protocols.

Ключові слова: *штучний інтелект; інформаційна безпека; національна безпека; кібератаки.*

Key words: *artificial intelligence; information security; national security; cyber attacks.*

Постановка проблеми. На даний час в світі суспільний розвиток характеризується формуванням інформаційного суспільства. Україна активно приймає участь у формуванні єдиного світового ринку інформації та в процесах глобальної інформатизації. Саме інформаційний чинник відіграє значну роль у відстоюванні державних інтересів у державотворчому процесі та на міжнародній арені. Ключовою складовою процесу управління процесами та інститутами стає широкий та оперативний доступ до підвищення ефективності інформації. Масове впровадження новітніх систем обробки інформації та телекомунікацій супроводжує інформатизацію сучасного суспільства.

Одним з чинників, що сприяє забезпеченню інформаційної безпеки є застосування технологій штучного інтелекту. Адже штучний інтелект є одним з трендових напрямів, яким охоплені всі розвинуті країни світу. У випадку відсутності необхідної уваги зі сторони держави до проблем штучного інтелекту Україна ризикує втратити можливість технологічного прориву. Глобальний ринок технологічних рішень на основі штучного інтелекту буде розділений між країнами-конкурентами, що ускладнить розвиток держави в стратегічно важливих галузях економіки та уповільнить її розвиток.

Під штучним інтелектом розуміється комплекс технологічних рішень, що дозволяє імітувати когнітивні функції людини та отримувати при виконанні конкретних завдань результати, що дорівнюють результатам інтелектуальної діяльності людини.

Активний розвиток інформаційних технологій обумовлює актуальність вивчення проблем інформаційної безпеки, а саме:

- загроз для інформаційних ресурсів, різних засобів та заходів захисту;
- бар'єрів для проникнення;
- вразливих місць в системі захисту інформації.

В загальному під інформаційною безпекою необхідно розуміти сукупність засобів, методів та процесів (процедур), які забезпечують захист інформаційних активів та, як наслідок, гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і відомостей, які в таких системах зберігаються та обробляються.

Особливого значення та актуальності в спектрі суспільних відносин набуває використання штучного інтелекту в системі забезпечення інформаційної безпеки, оцінка та аналіз інформаційних загроз та практичне застосування штучного інтелекту в контексті інформаційного опору з метою захисту територіальної цілісності України та суверенітету, що належить до концептуальних основ діяльності суспільства.

Аналіз останніх досліджень і публікацій. Дослідженню питань щодо впровадження технологій штучного інтелекту та проблем інформаційної безпеки присвячені чисельні роботи як вітчизняних, так і закордонних науковців, зокрема, О. В. Адамчука, О. А. Баранова, О. В. Глазова, Т. Г. Каткова, М. В. Карчевського, К. О. Хернес, С. Ю. Петраєва, О. Е. Радутного, Ю. М. Сидорчук, В. М. Фурашева, О. О. Ястреб, Є. О. Харитоновна, О. І. Харитонівна та інших. Проте, враховуючи думки зазначених авторів, доводиться констатувати, що в умовах постійного впливу зовнішніх та внутрішніх чинників необхідно приділити більше уваги дослідженню проблем штучного інтелекту в інформаційній безпеці як пріоритетній складовій національної безпеки України.

Метою статті є обґрунтування використання штучного інтелекту в інформаційній безпеці держави в умовах зовнішніх та внутрішніх загроз.

Виклад основного матеріалу. В даний час світ швидко змінюється під впливом сучасних інформаційних технологій, які зближують людей. Інформація для кожної держави стає вкрай важливим стратегічним ресурсом, який впливає на безпеку країни та перспективи формування демократичного суспільства.

Важливою невід'ємною складовою національної безпеки є інформаційна безпека держави, на яку впливають внутрішні та зовнішні чинники, зокрема, загальний рівень економічного, соціального й інформаційного розвитку країни та політична ситуація в країні та в цілому в світі. Зацікавленими у розвитку даного сектора є не тільки бізнес-структури, що активно застосовують нововведення у даній сфері, а й державні установи, для яких найголовнішим є питання національної безпеки [4, с. 20].

В сучасних умовах глобалізації інформаційна безпека виступає одним з найголовніших чинників забезпечення умов реалізації національних інтересів, спроможності держави долати кризові явища при зовнішній агресії. Своєчасні ефективні заходи щодо управління інформаційною безпекою з боку держави, як основного суб'єкта забезпечення інформаційної безпеки, здатні подолати загрози соціально-економічному та політичному життю країни. Сфера оборони та безпеки в світі – це галузь номер один і вона зазнає серйозних змін від впровадження технологій штучного інтелекту, що змінює баланс сил між державами [2, с. 16].

Штучний інтелект представляє собою результат людської діяльності здатний до логічного мислення, управління своїми діями, обґрунтовування своїх рішень, які не може коректувати в разі зміни умов.

Штучний інтелект – це високий результат досягнень техногенної цивілізації, складна система взаємозв'язків та підґрунтя для створення інформаційних системних утворень. У найближчій перспективі активне застосування технологій штучного інтелекту, нанобіотехнологій може дозволити переформатувати поведінку людини, змінити суспільні відносини та вплинути на екзистенційні характеристики особистості.

Штучний інтелект – це, насамперед, технології. Саме технології, які застосовуються для розробки систем та продуктів. До таких технологій відноситься:

- машинне навчання;
- комп'ютерний зір;
- когнітивістика;
- NLP (Natural Language Processing);
- глибоке навчання та інші.

Сучасні технології штучного інтелекту реалізуються за наступними напрямками:

- розпізнавання та синтез мови;
- інтелектуальні системи підтримки прийняття рішень;
- перспективні методи штучного інтелекту.

У сфері інформаційної безпеки застосування штучного інтелекту почалось з достатньо простих речей (на початку 2000-х років) – побудови систем, що полегшують роботу спеціалістів певного профілю, зокрема, вірусних аналітиків. До певного часу кількість зразків шкідливих файлів стала такою великою, що ручним або простим автоматизованим аналізом вже було не обійтися. Це були системи, які виявляють паттерни в шкідливому коді та дозволяють проводити хоча б мінімальну атрибуцію. Тобто вони представляли певну інформацію реверс-спеціалістам та вірусним аналітикам, яка дозволяла те чи інше програмне забезпечення віднести до певної групи чи класу.

Використання штучного інтелекту в інформаційній безпеці обумовлено насамперед двома чинниками:

- необхідністю оперативного реагування під час настання кіберінциденту;
- нестачею кваліфікованих спеціалістів з кіберзахисту [11, с.10].

На даний час застосування штучного інтелекту в інформаційній безпеці значно ширше. Є глобальні компанії, які аналізують в мережі великий обсяг інформації, що може вказувати на нові загрози або, наприклад, передбачити атаки нульового дня. В цих компаніях є системи, які збирають масиви даних, аналізують їх за допомогою технологій класу штучного інтелекту, виявляють закономірності, проводять кластеризацію даних та прогнозують загрози. Без таких технологій обробляти подібний обсяг інформації практично неможливо. Тут широко використовуються нейронні мережі та кластеризація.

Штучний інтелект активно застосовується у відслідковуванні загроз, де з його допомогою на основі інформації, яка зібрана з відкритих та закритих джерел, прогнозуються загрози інформаційній безпеці. Таким чином масштаб завдань та обсяг застосування штучного інтелекту в сфері інформаційної безпеки за останні двадцять років значно збільшився. Штучний інтелект є ефективним помічником у захисті від кіберзагроз.

Останнім часом спостерігаються три чинники, що сприяють ескалації ризиків інформаційної безпеки для державних органів всіх країн світу. По-перше, це розширення поверхні атаки. Частково це пов'язано зі зростанням кількості Інтернет приладів, яке в 2020 році оцінювалось в 30,73 млрд дол США. По-друге,

кіберзлочинці навчились оминати брандмауери та програмне забезпечення безпеки, яке в минулому ефективно працювало. По-третє, фрагментація рішень кібербезпеки залишає прогалини, через які дані стають вразливими [6].

Кращою стратегією інформаційної безпеки є випереджальний комплексний підхід, який охоплює п'ять ключових галузей:

- виявлення та аналітика загроз;
- безпека даних та додатків;
- управління ідентифікацією;
- безпека мережі та систем.

В Україні важливою складовою реформування оборонно-промислового комплексу є впровадження інноваційних технологій штучного інтелекту. Адже провідні країни світу вивчають та використовують можливості штучного інтелекту в галузі оборони [6]. Так, сучасна міжнародна група Thales Group3 [10], що функціонує в сфері цифрової ідентифікації безпеки створює й випускає інформаційні системи для авіакосмічної та військової галузей, що є потужною основою для швидкого ефективного захисту різних секторів критичної інфраструктури (енергетика, хімічна промисловість, транспорт, екологія та ін.). Дана група сприяє в забезпеченні інформаційної безпеки державним органам, приватним компаніям та власникам об'єктів критичної інфраструктури.

В 2019 році Швейцарією підписано угоду з Thales Group3, якою передбачено поставку елементів центру обробки зображень IMINT4. Ця система дозволить збирати та аналізувати всі типи цифрових інформаційних зображень, а також включатиме провідні технології штучного інтелекту, що дасть змогу Збройним Силам Швейцарії ідентифікувати загрози та застосовувати адекватні моделі захисту [10].

Сенсорні інструменти Thales на основі штучного інтелекту Cybels забезпечують інноваційний захист від кібератак у критично важливих секторах інфраструктури. Cybels Sensor шляхом встановлення штучного інтелекту безперервно спостерігає за різними джерелами атаки. Експертами лабораторії Thales зафіксовано нові види шкідливих програм. Під час виявлення загроз система Cybels Sensor маскує дану сигнатуру, щоб кіберзлочинці не дізнались про це і не змогли обійти захист. Також дана технологія здатна аналізувати кожен файл, що проходить крізь мережу, досліджуючи і виявляючи можливі загрози, шкідливі програми та інші аномалії [10].

2 грудня 2020 року в Україні Розпорядженням Кабінету Міністрів України №1556-р було схвалено Концепцію розвитку штучного інтелекту в Україні [3], яка передбачає визначення основних напрямів та пріоритетних завдань розвитку технологій штучного інтелекту з метою забезпечення конкурентоспроможності національної економіки та захисту технологічних інформаційно-комунікаційних систем. Завдяки застосуванню технологій штучного інтелекту відбуватиметься моніторинг соціальних мереж та інтернет-ресурсів, що дасть можливість аналізувати аудиторію, виявляти та попереджати певні проблеми. Відповідно до головної мети Концепції – забезпечення інформаційної безпеки було визначено основні напрями її забезпечення (рис. 1).

Рис. 1. Основні напрями забезпечення інформаційної безпеки

Джерело: [3]

На перший погляд впровадження штучного інтелекту здається дорогим та неперевіреним рішенням, яке приймається тільки інноваційними компаніями з великим бюджетом. Однак його використання в управлінні інформаційною безпекою гостро необхідно для всіх компаній, незалежно від їх масштабів та сфери діяльності.

На даний час кількість атак зростає, а ландшафт загроз змінюється з блискавичною швидкістю. Наприклад, продукти Kaspersky попереджають більше 700 млн онлайн-атак на квартал по всьому світу, а Cisco блокує 20 млрд мережових атак в день. Беззаперечно, при такому обсязі злочинної діяльності зловмисники активно застосовують засоби автоматизації кібератак, в тому числі використовують технології штучного інтелекту для їх вдосконалення та трансформації, а також для обходу відомих засобів захисту.

Так, наприклад, ефективним прототипом є відомий троян Emotet з основним каналом для його розповсюдження спам-фішингом, та групування, що стоїть за створенням Emotet, могло б без особливих труднощів використовувати штучний інтелект для посилення атаки.

Іншою можливою сферою шкідливого застосування штучного інтелекту є ефективніший підбір паролів або обхід двохфакторної аутентифікації. В 2017 році дослідники створили бота, який був здатен обходити перевірки CAPTCHA з ефективністю 90% за допомогою технологій штучного інтелекту. Використовуючи велику кількість різних джерел даних в даркнеті з метою формування бази знань штучного інтелекту, зловмисники можуть створити атаки, тому виробники систем захисту починають активно впроваджувати технології штучного інтелекту та машинного навчання з метою виявлення, прогнозування кіберзагроз, реагування на них в режимі реального часу. В цілому, за даними Webroot, біля 85% професіоналів з інформаційної безпеки вірять у те, що зловмисники використовують технології штучного інтелекту в своїх цілях [5].

В 2019 році світовий ринок технологій штучного інтелекту в інформаційній безпеці оцінювався експертами (MarketsandMarkets, Zion Market Research) в 8,8 млрд дол США, з досягненням до 38,2 млрд дол США в 2026 році та щорічним зростанням на 23% (рис.1) [7].

Основними чинниками зростання даного ринку є:

- зростаюча кількість користувачів мережі Інтернет та збільшення кількості підключених пристроїв;
- збільшення випадків кіберзагроз;
- зростання вразливості мережі Wi-fi до загроз безпеці.

Рис. 2. Прогноз об'єму світового ринку штучного інтелекту в інформаційній безпеці на 2019-2026 рр., млрд дол США
Джерело: [8]

Крім того, основні можливості штучного інтелекту на ринку інформаційної безпеки включають зростання потреби в хмарних рішеннях безпеки серед малих та середніх підприємств та збільшення використання соціальних мереж для виконання бізнес-функцій.

Організації, які впроваджують технології штучного інтелекту для поведінкового аналізу та продуктивної аналітики, отримують суттєві результати у вигляді підвищення ефективності виявлення атак, скорочення часу реагування та витрат на організацію безпеки. За даними Capgemini Research Institute, 64% організацій, річна виручка яких складає більше 1 млрд дол США, заявляють про те, що технології штучного інтелекту скорочують витрати на виявлення та реагування на загрози безпеці, та біля 75% заявляють про скорочення часу реагування (до 12%) [1, с. 188].

Класифікувати продукти організацій, що застосовують технології поведінкового аналізу та предикативної аналітики, можна за двома напрямками: за функціональним та технологічним типом та за сценаріями використання.

Рис. 3. Розподіл продуктів із застосуванням технологій штучного інтелекту за сценаріями використання
Джерело: [5]

Технології штучного інтелекту відкривають нові перспективи для розвитку сучасних засобів захисту інформації. Внаслідок останніх тенденцій в галузі діджиталізації аналітики інформаційної безпеки відзначають неухильне зростання як обсягу, так і складності даних, які генеруються в інформаційному просторі [9, с. 3]. Крім того, кіберзлочинці серйозно трансформували свої методи та техніки проведення атак. Більшість сучасних DDoS-атак побудовані за принципом «розумних» ботнетов, які, не маючи централізованого управління, здатні самоорганізуватися та вирішувати складні розрахункові завдання. Істотно вдосконалились й методи соціальної інженерії: зловмисники навчилися автоматизувати розсилки різними каналами, де інформація виглядає дуже правдиво для користувачів. У зв'язку з цим більшість компаній зіткнулись з тим, що традиційні технології забезпечення інформаційної безпеки стають малоефективними або зовсім неефективними та збитковими.

Основними типами технологій штучного інтелекту в системі інформаційної безпеки є:

1. EDR (Endpoint Detection and Response) – платформи виявлення атак на робочих станціях, серверах, будь-яких комп'ютерних пристроях (кінцевих точках) та оперативне реагування на них. За допомогою технологій штучного інтелекту продукти даної категорії можуть виявляти невідомі шкідливі програми, автоматично класифікувати загрози та самостійно реагувати на них, передаючи дані в центр управління. Штучний інтелект приймає рішення на основі загальної бази знань, накопиченої шляхом збору даних з безлічі пристроїв. Деякі продукти даного типу використовують технології штучного інтелекту для розмітки даних на кінцевих точках та подальший контроль їх переміщення, щоб виявляти внутрішні загрози [5].

2. NDR (Network Detection and Response) – пристрої та аналітичні платформи, які виявляють атаки на мережевому рівні та дозволяють оперативно на них реагувати. Використовуючи накопичену статистику та базу знань про загрози, продукти даного типу виявляють за допомогою технологій штучного інтелекту загрози в мережевому трафіку та можуть автоматично реагувати на них відповідним чином, змінюючи конфігурацію мережевих пристроїв та шлюзів. Частина продуктів даного типу спеціалізується на захисті хмарних провайдерів та їх інфраструктури. Додатковий сценарій використання штучного інтелекту в мережевому захисті – це аналіз поштового трафіку на предмет фішингу.

3. UEBA (User and Entity Behavior Analytics) – системи поведінкового аналізу користувачів та інформаційних сутностей. Вони виявляють випадки незвичної поведінки та використовують їх для детектування внутрішніх та зовнішніх загроз. Основний сценарій застосування технологій штучного інтелекту

в продуктах типу UEBA – це автоматичне виявлення аномалій в поведінкових моделях (відхилення від норми або невідповідність шаблону) для користувачів та різних інформаційних систем. Виявлені аномалії класифікують за допомогою штучного інтелекту як різні загрози та ризики для держави. Аномальна поведінка може виявитися з метою моніторингу та управління доступом, виявлення шахрайства, захист конфіденційних даних, перевірка дотримання тих чи інших регламентів та нормативних актів.

4. TIP (Threat Intelligence Platform) – платформи попереднього детектування загроз та реагування на них, що діють на основі великої кількості різних даних (Data Lake) та індикаторів компрометації (IoC). Застосування штучного інтелекту дозволяє підвищити ефективність виявлення невідомих загроз на ранніх етапах; сценарій дуже схожий з роботою SIEM-систем, але націлений на зовнішні джерела даних та зовнішні загрози [5].

5. SIEM (Security Information and Event Management) – рішення, які здійснюють моніторинг інформаційних систем в режимі реального часу аналізують події безпеки, що поступають від мережевих пристроїв, засобів захисту інформації, IT-сервісів, інфраструктури систем та додатків, та допомагають виявити інциденти інформаційної безпеки. В системах такого класу накопичується велика кількість даних з різних джерел, а застосування технологій штучного інтелекту дає можливість виявити евристичними методами аномалії та скоротити хибні спрацьовування під час зміни моделей даних.

6. SOAR (Security Orchestration and Automated Response) – системи, що дозволяють виявляти загрози інформаційній безпеці та автоматизувати реагування на інциденти. В рішеннях даного типу, на відміну від SIEM-систем, штучний інтелект допомагає не тільки проводити аналіз. Але й автоматично реагувати відповідним чином на виявлені загрози.

7. Засоби захисту додатків (Application Security) – системи, що дозволяють визначати загрози безпеці прикладних додатків, управляти подальшим циклом моніторингу та нейтралізації таких загроз. Основний сценарій застосування технологій штучного інтелекту в системах захисту прикладних додатків – автоматичний збір інформації про вразливі місця, атаки та зараження, яка доступна в відкритих джерелах, та заснована на його результатах автоматизація захисних дій: сканування на вразливість, зміна правил захисту для веб-додатків, виявлення загроз та зміна ризикової моделі.

8. Антифрод (Antifraud) – системи, які дозволяють виявляти загрози в бізнес-процесах та попереджати шахрайські операції в режимі реального часу. В системах захисту від шахрайства технології штучного інтелекту застосовуються для визначення відхилень від встановлених бізнес-процесів, тим самим допомагаючи швидко реагувати на можливий фінансовий злочин [5].

Отже, в сучасному високотехнологічному середовищі державі потрібна надійна інформація для встановлення високих стандартів, покращення протоколів безпеки, а також забезпечення безпеки конфіденційної інформації. Прийняття рішень за допомогою технологій штучного інтелекту допомагає знаходити загрози, попереджувати ризики та виконувати відповідні дії. Більш того, методи штучного інтелекту та машинного навчання відіграють вирішальну роль у покращенні протоколів інформаційної безпеки.

Висновки. На даний час в усьому світі структури знаходяться в стані переломного моменту, обумовленого застосуванням з метою інформаційної протидії більш сучасного обладнання та програмного забезпечення. Зарубіжні фахівці з інформаційної безпеки очікують, що інформаційно-технічний та інформаційно-психологічний вплив має значний потенціал в умовах стрімкого розвитку технологій штучного інтелекту.

В контексті інформаційної безпеки штучний інтелект – програмне забезпечення, яке здатне інтерпретувати стан середовища, розпізнати певні події та самостійно прийняти необхідні заходи. Технології штучного інтелекту ефективно справляються з розшифруванням закономірностей та аномалій, тому можуть бути інструментом моніторингу загроз. Надійна стратегія інформаційної безпеки також допомагає захистити персональні дані населення та державні дані та алгоритми, що стає важливішим у міру розгортання нових моделей штучного інтелекту.

Література.

1. Виловатых А.В. На пути к теории глобальной безопасности в условиях становления цифровой эпохи. *Свободная мысль*. 2020. № 4. С. 188–193.
2. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. № 4. С. 16–26.
3. Концепція розвитку штучного інтелекту в Україні [Електронний ресурс]: Розпорядження Кабінету міністрів України № 1556-р від 02.12.2020. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 07.12.2021).
4. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.
5. Применение технологий искусственного интеллекта в информационной безопасности. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security (дата звернення: 07.12.2021).
6. Укроборонпром хоче використовувати штучний інтелект в «оборонці». URL: <https://www.epravda.com.ua/news/2021/08/26/677230> (дата звернення: 07.12.2021).
7. Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research. URL: <https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In->

Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html (дата звернення: 07.12.2021).

8. Artificial Intelligence in Cybersecurity Market by Offering. URL: <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html> (дата звернення: 07.12.2021).

9. Jeschke S. et al. Industrial Internet of Things and Cyber Manufacturing Systems. *Cham: Springer International Publishing Switzerland*. 2017. Vol. 3, pp. 3–19.

10. Leveraging artificial intelligence to maximize critical infrastructure cybersecurity. URL: <https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure> (дата звернення: 07.12.2021).

11. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA. *Int. J. Cyber Warf. Terror*. 2016. Vol. 6, pp. 1–16.

References.

1. Vilovatyyh, A.V. (2020), “Towards a theory of global security in the emerging digital age”, *Svobodnaya mysl*, vol. 4, pp. 188–193.

2. Gurzhij, T. (2018), “Information law: the challenges of hybrid warfare”, *Zovnishnya torgivlya: ekonomika, finansi, parvo*, vol. 4, pp. 16–26.

3. The Verkhovna Rada of Ukraine (2020), The Order of Ukraine “The concept of artificial intelligence development in Ukraine”, available at: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (Accessed 7 December 2021).

4. Nishimenko, O. A. (2016), “Information security of Ukraine at the present stage of development of the state and society”, *Nashe pravo*, vol. 1, pp. 17–23.

5. Anti-Malware (2020), “Application of artificial intelligence technologies in information security”, available at: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security (Accessed 7 December 2021).

6. Economic truth (2021), “Ukrainian defense wants to use artificial intelligence in “defense”, available at: <https://www.epravda.com.ua/news/2021/08/26/677230> (Accessed 7 December 2021).

7. GlobeNewswire (2019), “Artificial Intelligence (AI) In Cyber Security Market Will Reach to USD 30.9 Billion By 2025: Zion Market Research”, available at: <https://www.globenewswire.com/news-release/2019/08/28/1907655/0/en/Artificial-Intelligence-AI-In-Cyber-Security-Market-Will-Reach-to-USD-30-9-Billion-By-2025-Zion-Market-Research.html> (Accessed 7 December 2021).

8. Markets and Market (2019), “Artificial Intelligence in Cybersecurity Market by Offering”, available at: <https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-security-market-220634996.html> (Accessed 7 December 2021).

9. Jeschke, S. (2017), “Industrial Internet of Things and Cyber Manufacturing Systems”, *Cham: Springer International Publishing Switzerland*, vol.3, pp. 3–19.

10. Thales (2019), “Leveraging artificial intelligence to maximize critical infrastructure cybersecurity”, available at: <https://www.thalesgroup.com/en/worldwide/security/magazine/leveraging-artificial-intelligence-maximize-critical-infrastructure> (Accessed 7 December 2021).

11. Pretorius, B. and van Niekerk, B. (2016), “Cyber-Security for ICS/SCADA”, *Int. J. Cyber Warf. Terror*, vol. 6, pp. 1–16.

Стаття надійшла до редакції 20.01.2022 р.