DOI: https://doi.org/10.26565/1992-2337-2024-1-18
УДК 351: 323.2

Лопатченко Іван Сергійович,
аспірант кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: ivan.lopatchenko@gmail.com https://orcid.org/0000-0003-2777-7189

ЗАСТОСУВАННЯ ДОСВІДУ США У ВИКОРИСТАННІ ШТУЧНОГО ІНТЕЛЕКТУ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. Темпи розвитку штучного інтелекту (ШІ) продовжують вражати. Світ вже розділився на два табори: одні закликають зупинити розвиток потужних систем штучного інтелекту, а інші оголошують про інтеграцію чат-ботів на основі ШІ, таких як "ChatGPT", у свої платформи. З поширенням та впливом штучного інтелекту практично на всі сфери людської діяльності в усьому світі виникають нові виклики та значні загрози в реалізації доктрин національної інформаційної безпеки для всіх без винятку країн.

У статті розглядається процес тотальної глобалізації, де національна інформаційна безпека стає провідним чинником забезпечення умов для реалізації національних інтересів і здатності держави долати кризові явища в умовах зовнішньої агресії. Своєчасні та ефективні заходи в управлінні інформаційною безпекою з боку держави здатні пом'якшити загрози соціально-економічному та політичному життю країни. Особлива увага має бути зосереджена на інформаційній безпеці Сполучених Штатів Америки, як основного та стратегічного партнера нашої держави, в тому числі у сфері інформаційної безпеки. З огляду на те, що стрімкий розвиток штучного інтелекту створює нові виклики та можливості для національної інформаційної безпеки, вивчення та запозичення досвіду провідних акторів у цій сфері, зокрема США, є надзвичайно важливим для нашої держави для забезпечення захисту національних інтересів в інформаційній сфері та інформаційного суверенітету.

Ключові слова: національна інформаційна безпека, штучний інтелект, джерела інформації, урядові рішення, безпекові алгоритми, стратегія інформаційної безпеки.

Постановка проблеми. Швидкість розвитку штучного інтелекту (ШІ) продовжує вражати. Світ уже розділився на два табори: одні закликають припинити розробку потужних систем штучного інтелекту, інші анонсують інтеграцію чат-ботів зі штучним інтелектом «ChatGPT» у свої платформи.

Як цитувати: Лопатченко І. С. Застосування досвіду США у використанні штучного інтелекту в забезпеченні національної інформаційної безпеки України. *Державне будівництво.* 2024. № 1 (35). С. 247–257. DOI: https://doi.org/10.26565/1992-2337-2024-1-18

In cites: Lopatchenko, I.S. (2024). Application of the us experience in the USA of artificial intelligence in ensuring the national information security of Ukraine. *State Formation, no. 1 (35), 247–257.* DOI: https://doi.org/10.26565/1992-2337-2024-1-18 [in Ukrainian].

Через тотальне розповсюдження та вплив штучного інтелекту на майже всі сфери діяльності людини у всьому світі, виникають як нові виклики так і суттєві загрози в реалізації доктрин національної інформаційної безпеки усіх без винятку країн.

Розглядаючи процес тотальної глобалізації національна інформаційна безпека є провідним фактором забезпечення умов реалізації національних інтересів, спроможності держави долати кризові явища при наявній зовнішній агресії. Своєчасні ефективні заходи щодо управління інформаційною безпекою з боку держави здатні подолати загрози соціально-економічному та політичному життю країни. Особливо прискіпливо наш погляд має бути прикутим до інформаційної безпеки саме США, як головного та стратегічного партнера нашої держави, у тому числі й у сфері інформаційної безпеки. Враховуючи, що стрімкий розвиток штучного інтелекту створює нові виклики та можливості для національної інформаційної безпеки держави, саме тому дослідження успішних кейсів учасників цієї сфери, й особливо в США, вважаємо надважливим для безпеки країни в сфері інформації та захисту нашого суверенітету.

Аналіз останніх досліджень і публікацій. Окремі проблеми штучного інтелекту були предметом дослідження вчених України та інших країн. Тому роботи присвячені визначенню терміну штучний інтелект та його властивостей досліджували наступні науковці: А. Виловатих, З. Гбур, В. Коцовський, Д. Лубко, С. Шаров. Розгляд терміну національна інформаційна безпека досліджували: О. Климчук, М. Копійка, О. Сорокін. Досліджено використання штучного інтелекту в забезпеченні національної інформаційної безпеки США наступними вченими Б. Преторіус, Б. ван Нікерк, І. Погоріла. Питання застосування штучного інтелекту у національній інформаційній безпеці вивчали С. Барбашин, М. Великанова, Б. Ткач, О. Лісовіченко. Оцінюючи важливість зазначених досліджень, стрімкий розвиток штучного інтелекту створює нові виклики та можливості для національної інформаційної безпеки держави, що вимагає постійних наукових досліджень у цьому напрямку.

Метою роботи є аналіз використання інструментів регулювання, штучного інтелекту у застосуванні в національній інформаційній безпеці держави та виокремлення напрямів можливого використання Україною успішного досвіду Сполучених Штатів Америки в даному напрямку.

Застосована методологія і методи Методологія дослідження поєднує комплекс сучасних філософських, загальнонаукових, спеціально-наукових методів пізнання, включаючи діалектичний, системний, структурно-функціональний, класифікації тощо.

Виклад основного матеріалу. У міжнародній науковій літературі, а також на рівні національного законодавства є достатньо різні варіанти формулювання терміну інформаційна безпека. Основну групу становлять бачення, у рамках яких інформаційну безпеку держави розглядають як стан, можливого розвику, умов життєдіяльності соціуму, його структур, інститутів і

установ, за яких забезпечується збереження їх якісного, вільного, відповідного власній природі та інноваційного функціонування [8].

Інформаційна безпека – це стан захищеності інтересів особи, суспільства і держави в інформаційній сфері, при якому виключається можливість їх пошкодження внаслідок неповноти, застарілості та недостовірності інформації, а також негативних наслідків використання інформаційних технологій. або інформацію, заборонену або обмежену законом.

Інформаційна безпека – стан захищеності об'єкта (особи, компанії, держави) від інформаційних загроз, який визначається рівнем шкоди, яка може бути завдана існуванню, функціонуванню чи діяльності об'єкта в разі реалізації ці загрози через [9]:

– використання неповної, застарілої та недостовірної інформації;

– застосування негативного інформаційного впливу;

– незаконне використання інформаційних технологій;

– несанкціоноване поширення та використання інформації, порушення її цілісності, конфіденційності та доступності.

Розглядаючи термін «забезпечення інформаційної безпеки» вважаємо, що це стосується діяльності, комплексу заходів і в цілому здатності суспільства і держави гарантувати бажаний захищений стан. Забезпечення інформаційної безпеки на думку науковців включає наявність трьох компонентів: діяльності, засобів і суб'єктів (рис. 1).

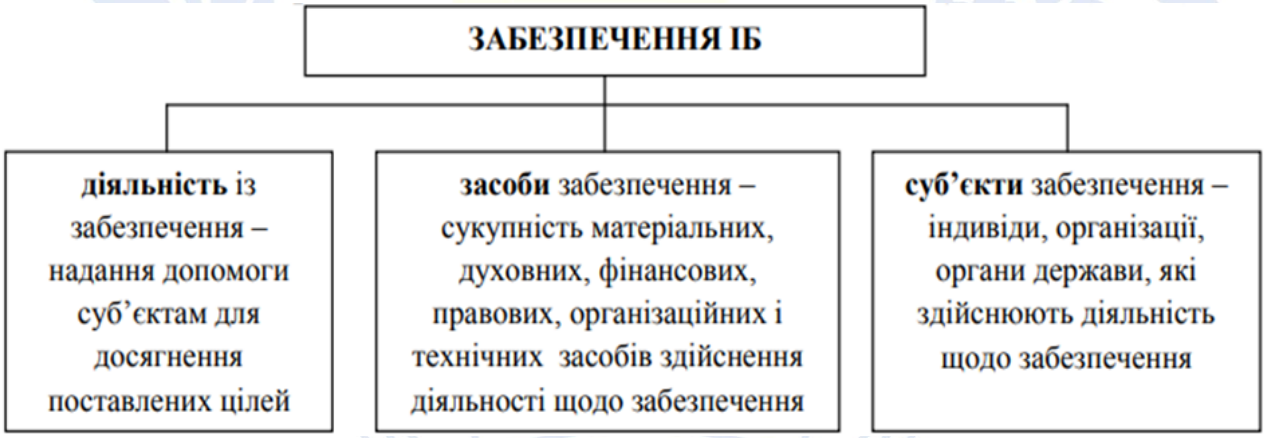

Рисунок 1 – Структура забезпечення інформаційної безпеки

Figure 1 – The structure of information security

Цікавим є визначенням зарубіжних фахівців, у якому зроблено акцент на необхідності проактивної позиції держави, суспільства й особистості в умовах прискореного розвитку та впровадження інформаційно-телекомунікаційних технологій у всі сфери життєдіяльності суспільства, виникнення нових видів загроз та потреби вироблення інноваційних форм поведінки для забезпечення інформаційної безпеки [9].

Якщо говорити про національну інформаційну безпеку України, то указом Президента України від 28 грудня 2021 року введено в дію «Стратегію інформаційної безпеки» [10].

Стратегія інформаційної безпеки (далі – Стратегія) визначає актуальні виклики та загрози національної безпеки України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію цим загрозам та захист прав громадян. для захисту інформації та персональних даних.

Метою Стратегії є зміцнення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, забезпечення інформаційними ресурсами та заходів соціально-політичної стабільності, захисту держави, захисту державного суверенітету, територіальної цілісності України, демократичних і політичних стабільності, захисту держави, охорони здоров'я та безпеки держави. конституційний лад, що забезпечує права і свободи кожного громадянина [10].

Штучний інтелект (ШІ) готовий повністю змінити життя людини. Такі зміни відбуваються з розвитком і поширенням Інтернету з початку цього століття й призвело до серйозних змін у структурах економіки, суспільстві, політиці та звичайному житті. Хоча штучний інтелект ще не став широко поширеним і явним, у всьому світі точаться дебати щодо того, як зробити керованим вплив ШІ на нашу роботу, здоров’я, освіту, розваги та багато інших аспектів нашого життя. Варто зазначити, що обговорення ШІ не стосується часу чи інтенсивності цих змін, проте має безпосереднє відношення до моментів, коли ШІ буде здатний змінювати суть біологічного існування життя, а також вплив цих нюансів на загальний світовий уклад. ШІ особливо не передбачає трансформації в тому сенсі, яким чином ми виконуємо нашу діяльність: господарську, соціальну, державну. Йде мова про те, що ШІ впливає на те, як досягається кінцевий продукт, оскільки він виконує дії шляхом заміни людського фактору.

Стурбованість щодо динамічного розвитку цієї технології призвела до збільшення кількості досліджень правових наслідків роботи систем ШІ. Однак більшість з цих аналізів зосереджуються на правових наслідках застосування ШІ в приватному секторі і як це впливає на окремих осіб та їх права. Але також надцікавим є ризики, котрі створюються ШІ в момент його застосування у державному управлінні, зокрема в урядових функціях, і як це впливає на здійснення публічної влади, інформаційну безпеку держави та на безпосередні права громадян [4].

На думку американського дослідника штучного інтелекту Хосе Фернандеса, поточна актуальність штучного інтелекту пояснюється, з одного боку, його величезним технологічним розвитком за останні роки, а з іншого боку, надзвичайними можливостями. Стосовно технологічного розвитку штучного інтелекту слід зазначити, що ця технологія існує з середини минулого століття, але лише в останнє десятиліття відбувся справжній поштовх для розвитку та застосування штучного інтелекту в цілому. Це пов’язано з трьома

взаємопов’язаними факторами: по-перше, прогресом у глибокому навчанні, що дозволяє вирішувати нові проблеми; по-друге, обробка великих об’ємів даних, яка завдяки хмарним обчисленням дає змогу отримувати, зберігати, обмінюватися та керувати великими обсягами високоякісних даних; і в кінці, постійне зростання обчислювальної потужності, що дозволяє ШІ вирішувати завдання за більш короткий час [4].

Дослідники ШІ зазначають, що стосовно трансформаційної здатності є загальна думка щодо того, що штучний інтелект постійно перебуває на передньому краї проривної діяльності технологій через його величезну неконтрольовану здатність у всьому – промисловості, сільському господарстві, охороні здоров'я й безперечно у оборонній сфері, яка відображається у впливі на національну інформаційну безпеку.

Існує серйозне занепокоєння щодо розширення використання ШІ, яке має

призвести до розробки численних нормативних актів і інструментів впливу, щоб забезпечити безпеку національній інформаційній системі, як у США, так і в ЄС. Ці унікальні проблеми виникають особливо часто, коли ШІ використовується в прийнятті урядових рішень, що передбачають використання влади та вплив на права громадськості, такі як нормотворчість (наприклад, нормативний аналіз), судове рішення (наприклад, гранти, допомога) або примусове виконання (перевірка). З іншого боку, управління внутрішніх процесів, робота з громадськістю (чат-боти), процеси моніторингу, а також надання послуг від держави є завданнями, які за своєю природою подібні до використання ШІ в державному секторі. Проте, важливо адекватно застосовувати ці новітні можливості й гармонізувати вигоду й ризики від їх використання без заподіяння шкоди, в першу чергу саме інформаційній безпеці держави, як найбільш дотичній сфері до ШІ [4].

Що стосується застосування ШІ у прийнятті важливих державних рішень, які передбачають використання алгоритму механізмів безпеки, то перше на що варто звертати увагу, здатність ШІ замінити працівників публічної влади або публічних адміністрацій в процесах прийняття рішень, або він буде використовуватися як інструмент, який допомагає таким процесам, так як такі моменти прийняття рішень можуть бути критичним ризиком для національної безпеки держави, зокрема й інформаційної.

Щодо основних ризиків впливу ШІ на національну інформаційну безпеку, то важливо уточнити роль системи ШІ - чи може вона припускати та встановлювати правило, яке вказує, в якому випадку система може діяти незалежно від людей, оскільки це може мати серйозний вплив на подальший розвиток подій. Також існує проблема в узгодженні зобов’язань в царині публічного права перед громадськістю та пояснення причин саме таких дій, оскільки бракує прозорості, а також необхідність заздалегідь пояснити громадськості дій системи штучного інтелекту в разі, наприклад, початку ядерної війни, або надпотужних природних чи космічних катаклізмів [4].

На наш погляд, прозорість є основним принципом використання ШІ в державному управлінні загалом, й в системі інформаційної безпеки зокрема. Це має ширший масштаб, ніж прозорість ШІ в приватному секторі, оскільки це йде від розробки загальнодоступного алгоритму до прийняття та спостереження за алгоритмічним прийняттям рішень. З одного боку, державне використання штучного інтелекту має включати громадську участь у розробці алгоритму так само, як загально прийняті процеси ухвалення рішень за участі громади у місцевому самоврядуванні.

Згідно з деякими думками дослідників, алгоритми ШІ слід вважати правилами і вони мають бути передані на політичне узгодження та нормотворчі процеси. З іншого боку, прозорість включає демонстрування важливих інформаційних даних щодо елементів розробки, а також алгоритмічну потужність. Це розкриття потребує, відстежування процесів й має включати можливість дізнатися повну інформацію, це допоможе стати доступним та зрозумілим громадянам [6].

Науковці припускають - прозорість буде надавати можливість інвесторам обирати правильну технологію, щоб вона передбачала і контролювала рішення, засновані на адміністративному алгоритмі, і при цьому враховувати потенційні рішення уряду, а це вже може призвести до негативних наслідків в інформаційній безпеці держави. Цей побічний ефект прозорості можна визнати в деяких випадках (наприклад приклад рішення щодо пільг), тому слід скласти алгоритм, який мав би виключити занепокоєння громадськості. В інших випадках (наприклад, податкова перевірка), алгоритм має бути прихованим, щоб уникнути передачі переваги для дій держави [3].

Крім того, якщо системи ШІ без командування людьми, вступають у судовий конфлікт й не можуть пояснити свої рішення, суди не зможуть забезпечити судовий перегляд відповідно до традиційних моделей. Обмеження судів щодо забезпечення повного судового розгляду призводить до розробки нових альтернатив державному нагляду за системами ШІ за межею компетенції судів. Це фактично й є одним з найнерозв'язуваніших питань щодо забезпечення гарантованої інформаційної безпеки держави [7].

У законодавстві та політиці щодо ШІ США сформувалася федеральна політика щодо використання штучного інтелекту. Незважаючи на численні регіональні та державні закони про штучний інтелект також набули чинності протягом багатьох років, федеральні закони та політика щодо штучного інтелекту мають підвищене значення для розуміння унікальної національної стратегії країни щодо штучного інтелекту. Дійсно, основа стратегії федерального уряду щодо штучного інтелекту вже закладена і дає уявлення про те, як будуть вирішуватися юридичні та політичні питання, викликані цією новою технологією, найближчим часом.

Три роки тому було підготовлено Національну стратегію Сполучених Штатів Америки зі штучного інтелекту, в ній йдеться про наступні моменти: Підтримувати потребу в освітніх програмах штучного інтелекту; підтримувати

потребу в міждисциплінарних дослідженнях штучного інтелекту; залучати інвестиції в розвиток систем штучного інтелекту; Національна стратегія штучного інтелекту США не має обов'язкової сили. У той же час стрімкий розвиток штучного інтелекту привертає все більше уваги, і попит на його нагляд також зростає [2].

У жовтні 2022 року Управління з питань наукової та технологічної політики Білого дому оприлюднило проект Білля про права на штучний інтелект. Вважається, що законопроект має стати певними правилами відповідального використання штучного інтелекту. Він визначає 5 основних принципів, яких слід дотримуватися при розробці та впровадженні автоматизованих систем ШІ:

– безпечні та ефективні системи. Людство має бути захищене від небезпечних або неефективних технологій. При розробці штучного інтелекту необхідно консультуватися з різними спільнотами, зацікавленими сторонами та експертами у відповідних галузях. Цей «мозковий штурм» допоможе визначити проблеми, ризики та потенційні наслідки впровадження технології;

– алгоритмічний захист від дискримінації. Програми, що використовують штучний інтелект, не повинні бути дискримінаційними. Розробникам автоматизованих систем при навчанні штучного інтелекту слід враховувати, що вихідний матеріал для навчання штучного інтелекту має представляти максимальну кількість груп і спільнот;

– зберігайте інформацію конфіденційною. Використовуючи програми ШІ, люди повинні вірити, що їхні особисті дані захищені та що вони можуть контролювати їх використання. Тому розробники повинні надати інструмент, який дозволяє користувачам отримувати дозвіл на збір, використання, доступ, передачу та видалення своїх даних. Запити на згоду мають бути короткими, чіткими та написаними простою та зрозумілою мовою;

– поясніть мету використання. Люди повинні знати про це щоразу, коли мова йде про використання програм штучного інтелекту. Крім того, необхідно надати інформацію про те, для чого використовується штучний інтелект, яких результатів потрібно досягти та як це може вплинути на користувачів;

– людські альтернативи та резервні варіанти. Для людей, які не хочуть використовувати програми штучного інтелекту, має бути можливість відмовитися від автоматизованих систем і замість цього використовувати людські альтернативи. Якщо певні процеси автоматизовані, наприклад доступ до певних соціальних послуг, чи повинні бути альтернативи? Через нього людина зможе реалізувати свої права[1].

Закон, що визначає національну ініціативу відносно штучного інтелекту зосереджений на розширенні наукового впливу та розвитку досліджень щодо ШІ та подальшій координації науково-дослідної діяльності в галузі штучного інтелекту між оборонними/розвідувальними спільнотами та цивільними федеральними агентствами. Закон також законодавчо закріпив створення Національного офісу ініціатив зі штучного інтелекту, який входить до складу

Білого дому і якому доручено «наглядати та впроваджувати національну стратегію США щодо штучного інтелекту» [2].

Наприкінці травня 2023 року, Білий дім зробив кілька додаткових кроків для подальшого окреслення свого підходу до управління штучним інтелектом. У результаті було опубліковано переглянутий Національний стратегічний план досліджень і розвитку штучного інтелекту, щоб «координувати та зосередити федеральні інвестиції в дослідження та розробки штучного інтелекту». План включає кілька стратегічних тез:

– робити довгострокові інвестиції у фундаментальні та відповідальні дослідження штучного інтелекту. Надати пріоритет інвестиціям у наступне покоління штучного інтелекту для стимулювання відповідальних інновацій, які служать суспільним інтересам і зберігають Сполучені Штати світовим лідером у цій галузі;

– розробка ефективних методів співпраці людини та штучного інтелекту. Поглибити розуміння того, як створювати системи штучного інтелекту, які ефективно доповнюють і покращують людські можливості;

– визначення та вирішення етичних, правових і соціальних наслідків використання штучного інтелекту;

– забезпечити безпеку систем штучного інтелекту. Це включає визначення можливостей тестування для перевірки функціональності та точності систем ШІ та захисту систем ШІ від кіберзагроз і вразливості даних.

– розробити спільні публічні бази даних і технології навчання;

– використовувати стандарти для вимірювання та оцінки систем ШІ;

– визначення національних потреб у робочій силі для досліджень штучного інтелекту;

– розвиток державно-приватного партнерства для прискорення розвитку штучного інтелекту та створення можливостей для продовження інвестицій у відповідальні дослідження та розробки штучного інтелекту [3].

Хоча системи штучного інтелекту обіцяють підвищення продуктивності в багатьох сферах державного управління, їх зростаюча складність, технологічна база, що швидко розвивається, і великі вимоги до даних можуть призвести до збільшення ризиків, пов’язаних з їх розробкою. У результаті люди все більше уваги приділяють національній інформаційній безпеці, особливо безпеці систем штучного інтелекту. З цією метою рекомендується провести національне дослідження для вирішення фундаментального питання про те, наскільки рівень тестування систем штучного інтелекту достатній для забезпечення безпеки використання штучного інтелекту в національній інформаційній безпеці США.

Останніми роками в нашій державі маємо змогу спостерігати тенденцію до стрімкого розвитку світового досвіду використання штучного інтелекту в усіх важливих сферах життя, промисловості, медицини, а особливо в ОПК та національній інформаційній безпеці. Прецедент у США та великих європейських країнах із використанням штучного інтелекту та чат-ботів дав комітету цифрової трансформації нашої держави певну кількість інформації для

аналізу та розуміння. Використовуючи досвід Сполучених Штатів 2020 року було створено Концепцію розвитку штучного інтелекту в Україні, там законодавчо визначаються терміни, мета, а також завдання щодо розвитку ШІ в нашій країні. Відповідно до концепції штучного інтелекту – це група організованих інформаційних технологій, які можуть виконувати складні та комплексні завдання, використовуючи наукові методи дослідження та алгоритмічні системи для обробки інформації, отриманої на роботі або створеної самостійно [4].

Національний інститут національної безпеки і протидії тероризму представив українським колегам у Раді національної безпеки і оборони України дослідження під назвою «Національна безпека та регулювання штучного інтелекту», в якому розглядаються різні аспекти загрози штучного інтелекту та відповіді на законодавство. і проблеми кіберстійкості країни. Українські колеги зазначили, що для ефективного реагування на загрози Україна співпрацює з міжнародними партнерами для обміну інформацією та досвідом для забезпечення відповідального використання штучного інтелекту. Однак наразі це дослідження не є відкритим для громадськості через конфіденційність інгредієнтів [5].

У 2020 році була затверджена Концепція розвитку штучного інтелекту в Україні. Це вказує на необхідність нарешті вирішити питання норм суспільних відносин у сфері розвитку штучного інтелекту. Нещодавно відновив роботу Комітет з питань розвитку сфери штучного інтелекту при Міністерстві цифрової трансформації України. Звісно, у процесі формування регламенту буде враховано й питання використання штучного інтелекту для створення та поширення неправдивої інформації.

Проаналізувавши процеси використання ШІ національною інформаційної безпекою США маємо можливість надати варіанти застосування даної технології в Україні:

– дослідити, проаналізувати процеси технології ШІ, а також надати на розгляд певний документ, який описує, чого компаніям і суспільству слід очікувати в найближчому майбутньому стосовно використання ШІ, він має висвітлювати підхід країни до регулювання штучного інтелекту та описувати кінцеві результати, яких країна планує досягти використовуючи технологію;

– розробити законодавство для регулювання та розвитку штучного інтелекту;

– вести діалогову взаємодію з громадянським суспільством та бізнесом, стосовно можливих меж використання інструментів ШІ в усіх сферах діяльності;

– використовуючи медіа-комунікативні технології, проводити роз’яснювальну роботу у суспільстві щодо дезінформаційних процесів, які можуть бути створювані та поширені з використанням штучного інтелекту;

– в умовах воєнних дій, особливо обережно використовувати технологію ШІ в стратегічно важливих сферах діяльності держави через можливість витоку або отримання важливої інформації іншими особами, до поки не буде сформовано зрозумілі для використання алгоритми дій ШІ.

Висновки з даного дослідження та перспективи подальших досліджень. Застосування нашою державою досвіду Сполучених Штатів в процесі використання технології ШІ у національній інформаційній безпеці спрямована на покращення системи національної інформаційної безпеки в Україні, зокрема, на узгоджене використання штучного інтелекту для виявлення, аналізу та запобігання потенційним загрозам для країни. Вона дозволяє Україні використовувати передовий досвід США для підвищення рівня безпеки в інформаційному просторі та захисту важливих національних інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Artificial Intelligence (AI). U.S. Department of State. URL: https://www.state.gov/artificial-intelligence/#nav__primary-nav
2. Artificial Intelligence and Democracy, URL: https://il.boell.org/en/2022/01/06/artificial-intelligence-and-democracy
3. Artificial intelligence and foreign policy decision-making. URL: https://calhoun.nps.edu/handle/10945/7993
4. Artificial Intelligence and Politics. URL: https://vocal.media/futurism/artificial-intelligence-and-politics
5. Eric Schmidt // National Security Commission on Artificial Intelligence. URL: https://www.nscai.gov/about/commissioners/schmidt
6. Pretorius B., van Niekerk B. Cyber-Security for ICS/SCADA. Int. J. Cyber Warf. *Terror.* 2016. Vol. 6. P. 1–16.
7. The Future of AI: How Artificial Intelligence Will Change the World. URL: https://builtin.com/artificial-intelligence/artificial-intelligence-future
8. Гбур З. В. Основи інформаційної безпеки держави в умовах війни. Russian-Ukrainian war (2014-2022): historical, political, cultural-educational, religious, economic and legal aspects: a scientific monograph. Riga, Latvia: "Baltija Publishing", 2022. С. 868-872. URL: http://baltijapublishing.lv/omp/index.php/bp/catalog/view/237/6325/13361-1
9. Дезінформація та штучний інтелект: (не)видима загроза сучасності. URL: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/
10. Правове регулювання Штучного Інтелекту. Голос України. URL: http://www.golos.com.ua/article/372783

Стаття надійшла до редакції 03.04.2024 р.
Стаття рекомендована до друку 15.05.2024 р.

Lopatchenko I. S.,
postgraduate student of the Department of Public Policy,
Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University,
4 Svobody Sq., Kharkiv, 61022, Ukraine
e-mail: kiev1112@gmail.com https://orcid.org/0000-0003-2777-7189

APPLICATION OF THE US EXPERIENCE IN THE USA OF ARTIFICIAL INTELLIGENCE IN ENSURING THE NATIONAL INFORMATION SECURITY OF UKRAINE

Annotation. The pace of artificial intelligence (AI) development continues to astound. Already, the world has divided into two camps: some calling for a halt to the advancement of

powerful AI systems, while others announce integrations of AI-powered chatbots like "ChatGPT" into their platforms. With AI's pervasive spread and influence across nearly all spheres of human activity worldwide, new challenges and significant threats arise in implementing doctrines of national information security for all countries without exception.

The article discusses the process of total globalization, where national information security becomes a leading factor in ensuring conditions for the realization of national interests and a state's ability to overcome crises in the face of external aggression. Timely and effective measures in managing information security by the state can mitigate threats to the socio-economic and political life of the country. Our focus should particularly be on information security in the United States, as our state's main and strategic partner, including in the realm of information security. Considering that the rapid development of artificial intelligence creates new challenges and opportunities for national information security, studying and borrowing the experience of leading actors in this field, including the United States, is extremely important for our state to ensure the protection of its national interests in the information sphere and information sovereignty.

Keywords: National information security, artificial intelligence, sources of information, government decisions, security algorithms, information security strategy.

REFERENCES

1. Artificial Intelligence (AI). U.S. Department of State. URL: https://www.state.gov/artificial-intelligence/#nav__primary-nav
2. Artificial Intelligence and Democracy, URL: https://il.boell.org/en/2022/01/06/artificial-intelligence-and-democracy
3. Artificial intelligence and foreign policy decision-making. URL: https://calhoun.nps.edu/handle/10945/7993
4. Artificial Intelligence and Politics. URL: https://vocal.media/futurism/artificial-intelligence-and-politics
5. Eric Schmidt // National Security Commission on Artificial Intelligence. URL: https://www.nscai.gov/about/commissioners/schmidt
6. Pretorius B., van Niekerk B. (2016). Cyber-Security for ICS/SCADA. Int. J. Cyber Warf. *Terror, 6, 1–16.*
7. The Future of AI: How Artificial Intelligence Will Change the World. URL: https://builtin.com/artificial-intelligence/artificial-intelligence-future
8. Gbur, Z.V. (2022). Fundamentals of information security of the state in the conditions of war. Russian-Ukrainian war (2014-2022): historical, political, cultural-educational, religious, economic and legal aspects, *868–872*. DOI: https://doi.org/10.30525/978-9934-26-223-4-106 [in Ukrainian].
9. Disinformation and Artificial Intelligence: (In)visible Threat of Modernity. URL: https://cedem.org.ua/analytics/dezinformatsiya-shtuchnyi-intelekt/ [in Ukrainian].
10. Legal regulation of Artificial Intelligence. Voice of Ukraine. URL: http://www.golos.com.ua/article/372783 [in Ukrainian].

The article was received by the editors 03.04.2024.
The article is recommended for printing 15.05.2024.