УДК 342.951

ГУРЖІЙ С.В., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-3642-4975.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПИТАННЯХ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *Визначено роль та значення штучного інтелекту у сфері забезпечення кібербезпеки та деталізовано методи його використання. Визначено переваги та пріоритети використання штучного інтелекту у сфері кібербезпеки. Узагальнено недоліки та вади, пов'язані із застосуванням хакерами технологій штучного інтелекту у сфері кібербезпеки. Висвітлено інноваційні здобутки практичного впровадження технологій генеративного штучного інтелекту ChatGPT (Generative Pre-trained Transformer). Окреслено правові засади регулювання штучного інтелекту у сфері кібербезпеки в Україні. Визначено загрозливі тенденції використання технологій штучного інтелекту на підставі звіту Європолу 2023 року. Проведено огляд законодавчих ініціатив ЄС, спрямованих на врегулювання сфери штучного інтелекту, зокрема, й у питаннях забезпечення кібербезпеки. Узагальнено шляхи удосконалення правових засад щодо використання технологій штучного інтелекту у сфері кібербезпеки, особливо в умовах правового режиму воєнного стану в Україні.*

Ключові слова: *штучний інтелект, кібербезпека, кібератака, кіберзагроза, національна безпека, інформаційні технології, машинне навчання.*

Summary*. The role and importance of artificial intelligence in the field of cyber security is determined. The methods of using artificial intelligence in cyber security are detailed. The advantages and priorities of the use of artificial intelligence in the sphere of cyber security are defined. The shortcomings and problematic issues related to the use of artificial intelligence technologies by hackers in the field of cyber security are summarized. The innovative achievements of the practical implementation of generative artificial intelligence technologies ChatGPT (Generative Pre-trained Transformer) are highlighted. The legal principles of the regulation of artificial intelligence in the field of cyber security in Ukraine are outlined. Threatening trends in the use of artificial intelligence technologies have been identified based on the Europol report 2023. A review of the legislative initiatives of the EU aimed at regulating the field of artificial intelligence, in particular in the issue of cyber security, was conducted. The directions of improvement of the legal framework and regulatory requirements regarding the use of artificial intelligence technologies in the field of cyber security are summarized, especially in the conditions of the legal regime of martial law in Ukraine.*

Keywords: *artificial intelligence; cybersecurity; cyberattack; cyberthreat; national security; information technology, machine learning.*

Постановка проблеми. Динамічний розвиток сучасних передових технологій, зростаюча суцільна залежність від Інтернету провокують постійний ризик появи нових кіберзагроз. В сучасних умовах актуалізується проблематика поширення та впровадження у сфери життєдіяльності людства ноу-хау – інноваційних технологій штучного інтелекту(далі – ШІ). ШІ стає однією із важливих технологій, поява яких вже змінила чимало сфер людського життя. У сфері комп'ютерних наук ШІ означає здатність машин виконувати завдання, для яких, зазвичай, вимагається наявність людського інтелекту. Сюди відносяться такі завдання, як розпізнавання мови, вирішення технологічних проблем

та схвалення оперативних рішень. Аналізуючи великі обсяги інформації та даних, алгоритми ШІ можуть розпізнавати закономірності, з'ясування яких дасть їм змогу згодом покращувати свою роботу. Існують різні види ШІ, кожен з яких володіє унікальними властивостями та обмеженнями, які засвідчують його у якості інноваційної технології.

Штучний інтелект – це швидкозростаюча сфера публічного інтересу та інвестицій, яка все активніше використовується для покращення аналізу, прогнозування та захисту від кіберзагроз. Завдяки технологіям ШІ стає можливим відстежувати кіберзагрози, моніторити, прогнозувати й моделювати ситуацію у кіберпросторі, вчасно реагувати на кіберінциденти. На фоні динамічного розвитку інноваційних технологічних рішень, ШІ досить широко застосовується для посилення кібербезпеки, виявлення та ліквідації загроз, посиленого захисту від кібератак, сприяє прийняттю виважених та скоординованих управлінських рішень. У відповідь на зростаючу стурбованість світової спільноти у цій площині, останнім часом, саме технології ШІ відіграють дедалі більш важливішу роль у питаннях посилення захисту цифрового світу, зокрема, персональних даних, забезпечення кібербезпеки. Загальноприйнятою у світі є позиція про те, що ШІ у сфері кібербезпеки стає дедалі більш важливою складовою останньої у міру розвитку глобального цифрового ландшафту. Розширюючи інструментарій та можливості виявлення й запобігання кіберзагрозам, автоматизуючи рутинні завдання та значно скорочуючи час для реагування на кіберінциденти, технології ШІ допомагають захиститися від кібератак, нівелюючи загрозливі тенденції у цьому сегменті. В умовах правового режиму воєнного стану проблематика використання та застосування ШІ у сфері кібербезпеки набуває неабиякої актуальності та потребує окремого розгляду.

Результати аналізу наукових публікацій. Доцільно вказати, що деякі теоретичні та практичні питання використання ШІ у кібернетичній сфері в Україні та зарубіжних державах раніше вже розглядалися у науковій літературі. Так, наприклад, технічну компоненту та особливості використання систем ШІ в контексті забезпечення кібербезпеки розглядали у своїх наукових працях: О. Неретін та В. Харченко [1], В. Савченко та О. Шаповаленко [2], І. Стьопочкіна та О. Новіков [3]. Перспективні можливості ШІ як важливого механізму автоматизованої та негайної реакції на розвиток та модифікацію кіберзагроз вивчав С. Шаров [4]. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій ШІ у кібербезпеці здійснював С. Цяпа [5]. У зарубіжній науковій літературі роль та значення ШІ у сфері кібербезпеки та подальші шляхи його розвитку досліджували: Т. Сіпола [6], Р. Мостіну [7], Р. Дас та Р. Сандхейн [8].

Проте питання використання ШІ у сфері кібербезпеки недостатньо досліджено на науковому рівні. Особливо це відчувається в умовах появи у листопаді 2022 року феномену генеративного ШІ – ChatGPT та триваючого (протягом останніх 18 місяців) правового режиму воєнного стану, що актуалізує тематику цієї наукової статті.

Метою статті є визначення ролі та значення, переваг і недоліків штучного інтелекту у питаннях посилення стану кібербезпеки, особливостей використання штучного інтелекту у сфері кібербезпеки, регламентації подальших шляхів удосконалення законодавчого забезпечення кібербезпеки.

Виклад основного матеріалу. В сучасних умовах кібербезпека безпосередньо пов'язана із стрімким розвитком Інтернет технологій, сервісів та додатків. Кібербезпека напряму захищає цифрові системи та мережі від несанкціонованого доступу, а ШІ може значно підвищити кібербезпеку, автоматизуючи виявлення загроз та реагуючи на них. За оцінками міжнародних експертів, світовий ринок продуктів кібербезпеки на базі ШІ

сягатиме $133,8 млрд. до 2030 року. ШІ допомагає управляти та попереджувати про небезпеку, своєчасно виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритети серед ймовірних ризиків, знаходити можливості та ресурси для реагування на реальні та потенційні загрози. Це засвідчує великий потенціал ШІ у питаннях покращення стану кібербезпеки. Крім того, технології ШІ можуть використовуватися з метою визначення уразливостей та слабких місць в системах та мережах, що надає змогу упереджено та завчасно ліквідувати їх. У цілому, використання ШІ у кібербезпеці допомагає залишатися на крок попереду від кіберзагроз.

Одним із основних способів використання ШІ у кібербезпеці є розробка передових алгоритмів, які допомагають виявляти та запобігати кібератакам. Ці алгоритми призначені для структурного аналізу великих обсягів даних та виявлення закономірностей, які можуть вказувати на реальну або потенційну загрозу. Обробляючи цю інформацію зі швидкістю та масштабами, які фізично не можливі для людини, системи ШІ можуть швидко виявляти потенційні та реальні кіберзагрози, вчасно реагувати на них, таким чином значно знижуючи ризики здійснення кібератак та її наслідки. Крім того, ШІ може використовуватися з метою автоматизації рутинних завдань кібербезпеки, чим значно спрощує роботу ІТ-спеціалістів на усіх рівнях. Системи на базі технологій ШІ можуть автоматично сканувати мережі на наявність уразливостей, виявляти загрози та навіть схвалювати заходи щодо зниження ризиків, наприклад, виправлення програмного забезпечення або блокування шкідливих IP-адрес. Цей рівень автоматизації не тільки підвищує ефективність, але й допомагає забезпечити послідовне його використання у питаннях забезпечення кібербезпеки.

Ще одна сфера, де ШІ значно впливає на кібербезпеку – структуризація інтелектуальної та оперативної інформації про кіберзагрози. Використовуючи методи машинного навчання, системи ШІ можуть оперативно аналізувати великі обсяги даних з різноманітних джерел, таких як: месенджери, соціальні мережі, е-публікації, телеграм-канали, дарк веб-форуми з метою виявлення загрозливих тенденцій та уразливостей. Цей аналіз у режимі реального часу надає змогу залишатися на крок попереду та розробляти й адаптувати стратегії кібербезпеки з метою прогнозування ситуацій та ризиків. Також з метою виявлення та запобігання кіберзагрозам, ШІ досить широко використовується для розширення можливостей реагування на кіберінциденти. За наслідками кібератак важливим є стримання та недопущення масштабування збитків і попередження подальших порушень штатного режиму роботи комп’ютерної техніки та систем. Саме завдяки технологіям ШІ можливо проаналізувати характер та властивості кібератаки, визначити ступінь уразливості системи та окреслити оптимальний перелік заходів оперативного реагування з метою локалізації та вирішення проблеми. Це надає сприятливі можливості, які дозволяють значно зменшити негативний вплив від кібератак та їх наслідків на штатний режим роботи інформаційно-комунікаційних систем, діяльність та репутацію державних органів, установ й організацій приватного сектору.

Однією із вагомих переваг використання ШІ є його здатність швидко та оперативно аналізувати великі обсяги даних. ШІ може швидко проаналізувати масиви даних, які би людина не змогла опрацювати за короткий проміжок часу. Це надає можливість завчасно виявляти загрози та оперативно схвалювати рішення з метою їхнього попередження та недопущення. Використання ШІ також допомагає автоматизувати процеси виявлення та реагування на кібератаки. ШІ може безперервно у режимі 24/7 моніторити мережу та виявляти аномальну поведінку, яка у свою чергу, може свідчити

про кібератаку. Крім того, ШІ може автоматично реагувати на загрози, блокуючи доступ хакерів до систем та запобігати витоку конфіденційних даних.

Ще одним важливим аспектом використання ШІ у кібербезпеці є його здатність до машинного навчання на підставі набутого досвіду. ШІ може використовувати дані про попередні кібератаки з метою покращення своїх алгоритмів та забезпечення більш точного виявлення ризиків та загроз у майбутньому. ШІ дозволяє гарантувати ефективний захист від автоматичних або скерованих кібератак. Цілком логічно розуміти той факт, що ШІ є важливим та ефективним інструментом для боротьби із кіберзагрозами, проте він, на наше переконання, повністю не може замінити людський фактор. Хоча деякі науковці помилково стверджують, що інтелектуальні системи позбавлені недоліків людського фактора: вони працюють швидше і помиляються значно рідше людей, що дозволяє практично повністю виключити людей з процесів забезпечення захисту і залишає їм допоміжні функції моніторингу та корекції [9, с. 66]. Дійсно, ШІ може допомогти автоматизувати процеси виявлення та реагування на кіберзагрози, проте вважаємо, що схвалення остаточного рішення про безпеку та гарантії її дотримання все ж належить виключно людині. Тобто ШІ у питаннях кібербезпеки значно допомагає, проте не здатний бути альтернативою та абсолютно замінити людський фактор. ШІ надає змогу розширювати масштаби та швидкість кібербезпеки, створюючи ефективний захист від кібератак та кіберзагроз.

Алгоритми ШІ можуть стати революційним підходом щодо виявлення нових кібератак, сприяти посиленню захисту систем, прогнозувати ситуації навколо поширення нових уразливостей, розробляти нові більш складні методи захисту від шкідливих програм тощо. Таким чином, за допомогою ШІ управляти мережевою безпекою стає значно простіше, упереджено мінімізуючи помилки та уразливості. Тобто, ШІ стає потужним інструментом під час захисту від кібератак. ШІ допомагає командам реагування на кіберінциденти (CERT) створювати потужні сервіси та спільні людсько-машинні проекти, які розширяють знання, навички та вміння, сприяючи посиленню кібербезпеки, запроваджуючи новий рівень кіберзахисту. Завдяки ШІ стає можливим упереджувати загрози та отримувати оперативну інформацію у режимі реального часу про кіберінциденти.

Важливим пріоритетом використання ШІ у сфері кібербезпеки є його здатність прогнозувати кібератаки ще навіть до їхнього повноцінного здійснення, що надає змогу своєчасно посилити засоби захисту. Іншою його перевагою є значне скорочення людського фактору – тобто ШІ не схильний до різних психологічних впливів або втоми. Реагування безпеки на кіберзагрози, автоматизоване за допомогою ШІ вимагає менше часу та знижує ризик людської помилки. Так, ШІ допомагає управляти та попереджувати про небезпеку, своєчасно виявляти загрози та реагувати на них у режимі реального часу, визначати пріоритети серед ймовірних ризиків та знаходити можливості та ресурси для реагування на реальні та потенційні загрози. Це засвідчує великий потенціал ШІ у питаннях покращення стану кібербезпеки.

Крім того, технології ШІ можуть використовуватися з метою визначення уразливостей в системах та мережах, що надає змогу ліквідувати їх завчасно. У цілому, використання ШІ у кібербезпеці допомагає залишатися на крок попереду від кіберзагроз. За таких умов ШІ зданий революціонізувати підхід до вирішення складних проблем у сфері кібербезпеки та стає її невід'ємною частиною. Системи ШІ навіть можуть навчити розпізнавати аномалії поведінки та попереджувати про небезпеку, виявляти нові штами шкідливого програмного забезпечення та захищати критично важливі дані.

Транформації та динамічний розвиток передових технологій змінюють цифровий світ, зокрема й інструменти та тактики забезпечення кібербезпеки. Важливою подією сучасності стало відкриття у листопаді 2022 року нового генеративного інструменту ШІ, такого як ChatGPT (Generative Pre-trained Transformer). Це чат-бот зі ШІ, розроблений компанією OpenAI – дослідницькою установою, яка вивчає та опановує ШІ та зробила революційний крок у питаннях його розвитку. Він може генерувати тексти на задані теми та відповідати на питання зрозумілою мовою. Запуск чат боту ChatGPT став революційним кроком у сфері технологій і дав поштовх до активної розробки продуктів зі ШІ. Водночас зростає ризик дезінформації, а особисті дані користувачів можуть опинитися в небезпеці. Сучасна технологія генеративного ШІ, яка може створювати прозу з текстових підказок, захопила громадськість після того, як чат бот ChatGPT був запущений трохи більше півроку потому, і став додатком, котрий глобально розвивається швидкими темпами. На цьому фоні ШІ став предметом занепокоєння через його здатність створювати підроблені зображення та іншу дезінформацію. У січні 2023-го ChatGPT досяг 100 млн. активних користувачів. Спочатку цей чат-бот був доступний безоплатно, згодом компанія заявила про запуск підписки на ChatGPT у США вартістю $20. Розробник чат-бота заборонив деяким окремим країнам користуватися своїми сервісами відповідно накладених санкцій, тож в рф він поки що недоступний. 18 лютого 2023 року міністр цифрової трансформації України М. Федоров повідомив, що ChatGPT став доступний в Україні, проте ця програма не працюватиме на тимчасово окупованих рф територіях України для того, щоб нею не скористалися військові держави-агресора [12].

Таким чином, ШІ може успішно допомагати захищатися від кібератак шляхом: автоматизованого пошуку загроз із використанням алгоритмів машинного навчання та за наслідками виявлення проблем у роботі систем, що може свідчити про порушення безпеки; того, що машинне навчання використовується з метою аналізу великих обсягів даних та прогнозування розвитку ситуації на підставі виявлених уразливостей та закономірностей, що надає змогу навчати системи ШІ розпізнаванню невідомих або непередбачуваних атак; предикативної аналітики, яка надає можливість прогнозувати майбутні загрози, наприклад, які облікові дані співробітників з найбільшою вірогідністю можуть бути зламані та які типи атак можуть відбутися у той чи інший день, у зв’язку з чим такий аналіз допомагає визначити, де знаходяться ймовірні проблеми в системі, щоб упереджено виявити та блокувати їх заздалегідь; виявлення аномалій у мережевому трафіку або у інших потоках даних, аналізуючи шаблони на предмет тотожності або відмінності між ними. Такий тип моніторингу допомагає виявити аномальну поведінку до того, як вона трансформується у майбутню шкідливу діяльність; автоматизації безпеки та впровадження нових політик й протоколів безпеки, що захищає від таких кібератак, як загрози спуфінгу або фішингу тощо. Автоматизація безпеки надає змогу запровадити економію часу та витрат; суттєвого зменшення помилок, пов`язаних із людським фактором, надання економічно ефективних рішень з 100 % точністю.

Застосування технологій ШІ у кібервійні є досить важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення національної безпеки України. На фоні окресленого позитивного досвіду використання технологій ШІ у питаннях забезпечення кібербезпеки та наявності його беззаперечних переваг, ця технологія не позбавлена своїх проблем й недоліків.

Однією із основних проблем є можливість використання технології ШІ кіберзлочинцями та хакерами з метою розробки більш складних та цілеспрямованих атак. Тобто продумані кібератаки з використанням технологій ШІ – глобальна загроза сучасності. Тобто хакери та кіберзлочинці можуть також використовувати ці технології для скоєння потужних та інноваційних кібератак. Наприклад, шкідливе програмне забезпечення на базі ШІ може навчатися та адаптуватися, щоб уникнути виявлення за допомогою традиційних інструментів мережевої безпеки. Кіберзлочинці можуть використати ШІ для виявлення закономірностей у комп'ютерних мережах, які визначають слабкі місця у програмному забезпеченні, що надає змогу хакерам виявляти та використовувати ці уразливості на власний розсуд. Постійно змінюючись, сигнатури шкідливих програм можуть допомогти зловмисникам обійти статичні засоби захисту, такі як брандмауери та системи виявлення за периметром. Аналогічним способом, шкідливе програмне забезпечення зі ШІ може перебувати усередині системи, збираючи дані та спостерігаючи за поведінкою користувача, доки не буде готове розпочати нову фазу атаки. Враховуючи економіку кібератак, зазвичай, простіше та дешевше організувати атаки, аніж будувати ефективний захист, про що впевнено знають й зловмисники. Більш того, ШІ є інноваційною технологією, яка призводить до появи нових кіберзагроз.

Так, за допомогою ШІ, а саме нейтронних мереж став можливим синтез високоякісних зображень, відео, аудіо матеріалів, створених з метою введення в оману пересічних користувачів, вимушеного впливу на системи розпізнавання обличчя. Ця технологія підробки зображень, в основі якої перебуває ШІ, отримала назву "deepfake" та вона вже була успішно використана на практиці з метою реалізації шахрайських схем та інших протиправних дій. Завдяки цій зловмисній програмі кібершахраї можуть видавати себе за іншу людину: скопіювати зовнішність, міміку, голос. Так, наприклад, був зафіксований резонансний випадок, коли керівнику підрозділу компанії зателефонувала стороння людина та голосом генерального директора попросила про переказ коштів у розмірі 220 тис. Євро, у зв'язку з чим вказані грошові кошти були переведені шахраю. Спеціалісти з кібербезпеки компанії "Check Point Research" з'ясували, що хакери розробили спосіб використання чат бот ChatGPT з метою розробки шкідливих програми та фішингових електронних листів. Раніше кіберспеціалісти "Check Point Research" з'ясували, що за допомогою ChatGPT можливо розробити скрипт для створення даркнет-маркетплейсу, на якому можна було придбати скомпрометовані облікові дані, інформацію про платіжні картки, шкідливі програми, інші незаконні товари тощо.

Тобто хакери можуть використовувати ШІ з метою обходу систем захисту та створення більш складних та удосконалених кібератак. У зв'язку з цим доцільно забезпечити захист даних та алгоритмів безпеки ШІ від кібератак та взломів. Хакери вірогідно можуть використовувати шкідливі алгоритми з метою впровадження їх в систему ШІ щоб обійти системи захисту. Тому необхідно посилити заходи захисту систем, які працюють на базі ШІ, проводити регулярні перевірки на наявність уразливостей. Також необхідно навчати ШІ різним видам кібератак та кіберзагроз, використовувати при цьому актуальні дані про нові типи та види. За таких умов важливо, щоб індустрія кібербезпеки випередила ці події та постійно впроваджувала інновації для протидії новим загрозам. Тобто завдання щодо посилення кіберзахисту є актуальним на перманентій основі, виходячи із нового формату динамічно розроблених нових сучасних технологій, які продикують появу нових загроз. На сьогодні не існує жодних надійних та універсальних методів захисту від кібератак на системи ШІ. Тому будь-яке використання технологій ШІ може надавати користь та одночасно формувати нові потужні загрози та виклики.

Отже, світова спільнота активно переймається проблематикою поширення та впровадження технологій ШІ у сферу кібербезпеки та його унормування, у зв`язку з чим навколо світу набуває обертів та триває обговорення необхідності здійснення правового врегулювання ШІ, особливо у питаннях забезпечення кібербезпеки. Оскільки відсутні міжнародні правила та правові засади використання ШІ, то це питання залишається відкритим. Також доцільно враховувати організаційні та правові питання використання ШІ у кібербезпеці, оскільки схвалення рішень на основі ШІ може призвести до порушення прав людини на приватність. Оскільки провідні держави світу моделюють свої політики, включаючи ШІ у різні сфери та галузі, існує нагальна потреба розробки та затвердження етичних правил і правових стандартів, які мають врегулювати сферу використання ШІ у питаннях забезпечення кібербезпеки. Так, зокрема, перед країнами-членами "Великої сімки" на порядку денному стоїть питання щодо обговорення розробки та удосконалення законодавства, яке має регулювати використання та застосування технологій, пов'язаних зі ШІ. Очікується, що ШІ несе певні ризики для безпеки, оскільки він може продукувати фейкові новини та руйнівні рішення для суспільства, якщо дані, на яких він базується, є несправжніми. Тому доцільним є врегулювання сфери ШІ на законодавчому рівні, що водночас має зберегти відкрите та сприятливе середовище для розвитку його технологій, а також ґрунтуватися на демократичних цінностях та засадах.

Україна не відстає у питаннях регулювання ШІ від світових тенденцій сучасності. У 2020 році була схвалена Концепція розвитку сфери штучного інтелекту. Нормативно задекларовано, що основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі ШІ є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об'єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян. Задекларовано, що комплексне розв'язання проблем кібербезпеки вимагає виконання таких завдань: удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик ШІ у сфері кібербезпеки і кіберзахисту; розроблення інноваційних систем кібербезпеки, які широко застосовують технології ШІ для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчення питання ліцензування іноземних розробок ШІ у сфері кібербезпеки, особливо у державному секторі; створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління; оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, з урахуванням європейських та міжнародних стандартів, зокрема стандартів ISO 27001, ISO/IEC 27032, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень тощо [10].

12 травня 2021 року Кабінет Міністрів України затвердив План заходів щодо реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки [11]. Цим стратегічним документом регламентовані питання впровадження технологій ШІ в національну систему кібербезпеки для проведення аналізу і класифікації загроз та вибору стратегії їх стримування і запобігання їх виникненню. У рамках стратегічного планування наприкінці 2021 року за сприяння РНБО України на державному рівні мали бути затвердженими заходи протидії кіберзагрозам з використанням технологій ШІ. Проте, на

жаль, нормативно ці заходи ще й досі не визначені, що актуалізує діяльність державних органів за цим напрямком, особливо в умовах правового режиму військового стану.

Занепокоєння щодо негативних наслідків та загрозливих тенденцій використання ШІ знайшли своє відображення у звіті Європолу, який було оприлюднено у березні 2023 року [13]. Так, на підставі аналізу здобутих результатів роботи Європейського поліцейського офісу з'ясовано, що чат-бот ChatGPT та інші генеративні системи ШІ можуть бути використані для онлайн-шахрайства та скоєння інших видів злочинів. Попри позитивні приклади та користь, яку можуть принести звичайним людям генеративні моделі ШІ, серед яких чат-бот ChatGPT, поширення таких інструментів може вірогідно призвести до нових проблем, з якими стикнуться правоохоронні органи. Експерти Європолу підкреслюють, що правила модерації ChatGPT можна обійти за допомогою т.зв. "оперативного проектування", тобто практики надання вхідних даних у модель ШІ саме для отримання певного результату. Оскільки чат-бот ChatGPT є відносно новою сучасною технологією, незважаючи на його постійне оновлення, у цьому інструменті постійно виявляються прогалини. Наприклад, існують команди, завдяки яким ШІ може використовуватися у злочинній діяльності, хоча, якщо такі команди надати чат-боту ChatGPT у звичайному форматі, він обов'язково попередить, що його роботу не можна застосовувати у протиправній діяльності та злочинним умислом. Якщо ж змінити окремі слова запиту чи контекст, він може стати дієвим інструментом для реалізації своїх цілей кіберзлочинцями. Експерти підкреслюють, що обхідні шляхи, якими вдається позбавити модель від будь-яких обмежень, постійно розвиваються та стають все складнішими.

Розуміючи ризики та загрози, які несе суцільне використання ШІ, зокрема у питаннях кібербезпеки, 14 червня 2023 року Європарламент схвалив проект закону, який регулюватиме правила у сфері ШІ на території країн ЄС [14]. Цей законопроект висвітлюватиме питання поширення та використання ШІ відповідно до рівня ризику: чим він вищий для прав чи свобод людей, тим більше зобов'язань. Особливі нормативні вимоги висуватимуться до генеративних систем, таких як ChatGPT, що здатні створювати текст, зображення, аудіо та медіафайли. Законодавчо встановлюється вимога щодо інформування користувачів про те, що контент був створений машиною, а не людиною. Прийнятий нещодавно законопроект про регулювання ШІ в ЄС стане першим у світі документом, в якому закладені основи використання цієї технології та враховані обмеження й застереження щодо її негативного впливу. Хоча документ передбачає велику кількість різноманітних обмежень, його основною ідеєю є мінімізація впливу ШІ на базові права людини. Цей законопроект декларує доволі жорстку обрану тактику стосовно використання ШІ загалом та чатботів в бізнесі та інших галузях життєдіяльності європейського співтовариства зокрема. Перспективне схвалення цього законопроекту, яке планується у 2026 році, має стати важливим та актуальним кроком у питаннях правової регламентації розвитку ШІ на теренах ЄС.

Очікується, що цей закон допоможе забезпечити більшу безпеку та відповідальність при використанні ШІ та захистити права та свободи користувачів. Законопроект може бути застосовано відносно різних галузей, включаючи кібербезпеку, банківську, медичну та страхову. В ньому регламентовані вимоги щодо збору та зберігання даних, але найголовніше – правила використання алгоритмів, зокрема чат-ботів, у різноманітних взаємодіях з клієнтами. Головна вимога закону – інструменти ШІ можуть бути використані лише тоді, коли вони гарантуватимуть неупередженість й безпеку та здатність до відновлення у разі збою. Окремою вимогою є забезпечення прозорості використання ШІ. Досить жорстким рішенням є встановлення відповідальності за будь-

які помилки, що можуть виникнути при використанні чатботів в медичній галузі. Іншими сферами, які регулюватимуться цим законом, є судова система та правоохоронні органи. Одночасно європейський "AI Act" встановлює загальні принципи та вимоги до використання ШІ в будь-якій галузі, зокрема у кібербезпеці. Очікувано, цей модельний закон може стати прикладом для інших країн та підгрунтям для розробки міжнародних стандартів використання ШІ. Зокрема, його може бути покладено в основу ініціатив з боку ООН та інших світових організацій щодо створення міжнародного законодавства в цій сфері.

Висновки.

Роль та значення ШІ у питаннях забезпечення кібербезпеки без перебільшення не можна недооцінювати. ШІ стає невід`ємною частиною архітектури сучасної кібербезпеки. У зв'язку із динамічним та перспективним розвитком передових технологій, ШІ досить широко використовуєтсья для виявлення кіберзагроз, формування дієвих механізмів захисту від кібератак та схвалення оперативних управлінських рішень. Можливості ШІ сприяють удосконаленню процесів моніторингу змін ландшафту загроз на кіберфронті, виявленню кібератак, надають змогу покращити стан забезпечення кібербезпеки в цілому. Технології ШІ дають змогу, на постійній основі, автоматизувати процеси сканування мереж з метою виявлення та реагування на кібератаки. Однозначно не можна повністю виключати людський фактор під час використання ШІ у сфері кібербезпеки, оскільки остаточне рішення за наслідками використання ШІ належить саме людині. Тобто ШІ допомагає людині, проте не замінює її.

Беззаперечно, ШІ відіграє подвійну роль у питаннях забезпечення кібербезпеки. На фоні позитивного аспекту, з одного боку, можна констатувати, що за його допомогою, хакери та кіберзлочинці можуть планувати та здійснювати потужні й руйнівні кібератаки. Загрози, реалізовані за допомогою ШІ, є особливо небезпечними. Позитивним здобутком сучасності стала поява генеративної системи ШІ зокрема чат-боту ChatGPT. Проте, на підставі досвіду, який склався за останні півроку його активного використання, фахівці засвідчили та підтвердили можливість його реалізації хакерами у злочинних цілях: викрадати конфіденційні дані, створювати шкідливе програмне забезпечення тощо. Тобто вірогідно чат-бот ChatGPT може використовуватися для поширення комп'ютерних вірусів, надавати зловмисникам та хакерам неабияку підтримку під час використання ними цих технологій для проведення кібератак, поширення шкідливого програмного забезпечення.

Застосування технологій ШІ у кібервійні є важливим. Зокрема, моніторинг соціальних мереж та Інтернет-ресурсів електронних медіа засобами ШІ надає можливість виявляти дезінформацію, приховану російську пропаганду, системні тренди і проблематику та діяти на випередження. В умовах кібервійни Україна має нарощувати потенційні зусилля в просуванні своїх національних інтересів, використовуючи сучасні інформаційні технології та алгоритми ШІ в інтересах забезпечення національної безпеки України. Навіть попри деякі негативні тенденції, пов'язані із можливостями використання ШІ, його застосування з метою проведення потужних кібератак може стати найнебезпечнішим атрибутом**.** Здатність зламувати кібермережі супротивника матиме вирішальне значення, оскільки військові продовжують проводити бойові операції, логістику, націлювання, розвідку і всі інші аспекти сучасної кібервійни, в основі яких перебуває мережа Інтернет.

Важливим та перспективним напрямком залишається розробка нормативних вимог та подальша їх уніфікація щодо використання технологій ШІ у сфері кібербезпеки, особливо в умовах правового режиму воєнного стану в Україні. Також необхідним є

унормування правової регламентації як на державному, так і міжнародному рівнях, використання технологій ШІ у сфері кібербезпеки з метою недопущення порушень прав людини на приватність.

Використанна література

1. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. *Information Systems And Networks.* 2022. № 12. С. 7-20.

2. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації.* 2020. № 4 (44). С. 6-11.

3. Стьопочкіна І.В., Новіков О.М. Методи штучного інтелекту в кібербезпеці: навч. посіб. для здобувачів спец. 125 "Кібербезпека". Київ: КПІ ім. Ігоря Сікорського, 2022. 82 с.

4. Шаров С.В. Сучасний стан розвитку штучного інтелекту та напрямки його використання*:* зб. наук. пр. *Інноваційні обрії України*. 2023. № 6. С.136-144. – (Громадська організація Українські студії в європейському контексті).

5. Цяпа С.М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. *Інформація і право.* № 2(37)/2021. С. 51-59.

6. Tuomo Sipola, Tero Kokknen, Mika Karjalainen Artificial Intelligence and Cybersecurity: Theory and Applications. JAMK University of Applied Sciences. Publisher: Springer; 1st ed. 2023 edition (December 8, 2022). 311 p. DOI 10.1007/978-3-031-15030-2

7. Narcisa Roxana Mosteanu. Artifical Inelligence and cyber security – face to face with cyber attack – a maltese case of risk management approach. *Ecoforum journal.* 2020. Vol 9. № 2. URL: http://www.ecoforumjournal.ro/index.php/eco/article/view/1059

8. Rammanohar Das, Raghav Sandhane. Artificial Intelligence in Cyber Security. ICACSE 2020. IOP Publishing. Journal of Physics: Conference Series 1964 (2021). P.1-10 doi:10.1088/1742-6596/1964/4/042072. URL: https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf

9. Гладка Ю.А., Назаренко Є.О. Аналіз застосування технологій штучного інтелекту в кібербезпеці: наукові праці третьої Міжнар. наук.-практ. конф. *Сучасні тенденції розвитку інформаційних систем і телекомунікаційних технологій*, м. Київ, 25 – 26 січня 2021 р. Київ: НУХТ, 2021. С. 64-66.

10. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.20 р. № 1556 URL: https://zakon.rada.gov.ua/laws/show/1556-2020-р#Text

11. Про затвердження Плану заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021 – 2024 роки: Розпорядження Кабінету Міністрів України від 12.05.21 р. № 438 URL: https://zakon.rada.gov.ua/laws/show/438-2021-р#Text

12. Федоров: в Україні став доступний чат-бот зі штучним інтелектом ChatGPT. – (Українські національні новини від 18.02.23 р.). URL: https://www.unn.com.ua/uk/news/2016033-fedorov-v-ukrayini-stav-dostupniy-chat-bot-zi-shtuchnim-intelektom-chatgpt

13. ChatGPT. The impact of Large Language Models on Law Enforcement. Europol Public Information. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20Enforcement.pdf

14. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~