Напрям 5. Забезпечення державної безпеки
як основоположна передумова для реалізації прав,
свобод і законних інтересів суб'єктів права в Україні.

Дараган Олексій Віталійович
аспірант кафедри конституційного,
адміністративного та фінансового права,
Академія праці, соціальних відносин і туризму (м. Київ)
Науковий керівник – д.ю.н., проф., Діордіца І.В.

МОЖЛИВОСТІ ШТУЧНОГО ІНТЕЛЕКТУ В СФЕРІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

У глобальній безпеці, що невпинно розвивається, штучний інтелект (ШІ) став трансформаційною силою, яка змінила підхід країн до оборони, розвідки та стратегічного планування. Оскільки країни в усьому світі вкладають значні кошти в технології ШІ, наслідки для національної безпеки є глибокими та далекосяжними [1].

Підтвердженням важливості використання ШІ для забезпечення національної безпеки і обороноздатності держав є результати досліджень Науково-технічної організації НАТО, що визначають найбільш суттєві з них для розвитку технологій воєнної сфери на найближчі два десятиліття. Так, згідно з вказаними дослідженнями ключовими технологіями воєнної сфери є: Big Data, ШІ, автономні транспортні засоби, космос, гіперзвукові літальні апарати, квантові технології, біотехнології, нові матеріали ф т. ін. [2].

ШІ активно використовується й в Україні у сфері військових технологій. Зокрема, штучний інтелект допомагає фіксувати переміщення техніки та особового складу окупантів, збивати ворожі ракети, ефективніше наводити БПЛА на цілі, проводити розмінування, навіть працюють вже

системи протиповітряної оборони (ППО), оснащені штучним інтелектом, що визначає траєкторії польотів об’єктів [2].

Вважаю за необхідне виділити переваги та потенційні можливості ШІ у сфері забезпечення національної безпеки.

Переваги ШІ в забезпеченні національної безпеки.

1. Покращений збір і аналіз розвідувальних даних.

Однією з найважливіших переваг ШІ в національній безпеці є його здатність швидко й ефективно обробляти й аналізувати величезні обсяги даних. Розвідувальні служби генерують величезну кількість інформації з різних джерел, включаючи супутникові зображення, перехоплення комунікацій і розвідувальні дані з відкритих джерел. Системи на базі штучного інтелекту можуть аналізувати ці дані, виявляючи закономірності, аномалії та потенційні загрози, які аналітики можуть пропустити. Наприклад, алгоритми машинного навчання можуть аналізувати супутникові зображення, щоб виявити зміни у військових об’єктах або незвичні переміщення військ.

2. Прогностична аналітика та оцінка загроз.

Передбачувані можливості ШІ пропонують цінну підтримку для планування національної безпеки та розробки стратегії. Аналізуючи історичні дані та поточні тенденції, моделі ШІ можуть прогнозувати потенційні ризики безпеці, геополітичні події та нові загрози. Це дозволяє службам безпеки брати участь у більш складному плануванні сценаріїв, передбачаючи можливі атаки чи кризи та готуючи належні відповіді. Наприклад, системи штучного інтелекту можуть моделювати потенційний вплив різних факторів, таких як економічна нестабільність, зміна клімату або політичні заворушення, допомагаючи політикам розробляти більш ефективні довгострокові стратегії безпеки.

3. Кібербезпека та захист мережі.

Оскільки кіберзагрози стають все більш витонченими, ШІ відіграє вирішальну роль у захисті критичної інфраструктури та чутливих мереж.

Алгоритми машинного навчання можуть контролювати мережевий трафік у режимі реального часу, виявляючи аномалії та потенційні вторгнення набагато швидше й точніше, ніж традиційні системи безпеки. Платформи аналізу загроз на основі штучного інтелекту можуть аналізувати глобальні дані про кіберзагрози, щоб передбачати та запобігати майбутнім атакам.

4. Автономні та напівавтономні системи.

ШІ дозволяє розробляти автономні та напівавтономні системи, які можуть працювати в середовищах, надто небезпечних або недоступних для людей. Це включає в себе безпілотні літальні апарати (БПЛА) для розвідки та спостереження, автономні підводні та надводні апарати для морських операцій і роботизовані системи для знешкодження вибухонебезпечних предметів. Ці системи на базі штучного інтелекту можуть посилити військовий потенціал, одночасно зменшуючи ризики для людського персоналу. Вони також можуть працювати тривалий час у суворих умовах, забезпечуючи постійне спостереження та збір розвідданих.

5. Підтримка прийняття рішень у кризових ситуаціях.

Під час кризи чи конфлікту ШІ може забезпечити швидкий аналіз ситуації, що розвивається, допомагаючи військовим і політичним лідерам приймати обґрунтовані рішення під тиском. Алгоритми машинного навчання можуть обробляти дані в режимі реального часу з багатьох джерел, надаючи повну картину поля бою або кризової зони. Це може призвести до більш ефективних тактичних рішень і потенційно зменшити втрати.

Майбутні перспективи ШІ в забезпеченні національної безпеки.

1. Квантовий ШІ та криптографія.

У міру розвитку квантових обчислювальних технологій вони можуть значно розширити можливості штучного інтелекту в національній безпеці. Квантові системи штучного інтелекту можуть зламати поточні методи шифрування, що потребує розробки нової квантово-стійкої криптографії. І навпаки, квантовий штучний інтелект також може забезпечувати незламні

методи шифрування, революціонізуючи захищений зв’язок для розвідки та військових операцій.

2. Військові ігри та симулятори з розширеним штучним інтелектом.

Передові системи штучного інтелекту можуть змінити військове планування та навчання за допомогою стратегічних можливостей бойових ігор та симуляції. Ці системи можуть моделювати складні геополітичні сценарії, дозволяючи військовим стратегам тестувати різні підходи та краще готуватися до широкого спектру потенційних конфліктів або криз.

3. Когнітивна електронна війна.

ШІ, ймовірно, відіграватиме дедалі важливішу роль у радіоелектронній війні. Системи на базі штучного інтелекту можуть аналізувати спектр у реальному часі, швидко ідентифікуючи та протидіючи комунікаційним і радарним системам противника. Це може призвести до нової ери когнітивної електронної війни, де системи ШІ беруть участь у складних динамічних електромагнітних битвах.

4. Ройовий інтелект і скоординовані автономні системи.

Майбутні військові операції можуть включати великі зграї автономних дронів або роботів, координованих системами ШІ. Ці зграї зможуть (чи, можливо, вже можуть) виконувати такі складні завдання, як розвідка, закриття території або навіть скоординовані атаки, створюючи нові виклики та відкриваючи нові можливості для військових стратегів.

5. Прогнозування та запобігання загрозам на основі ШІ.

Оскільки системи штучного інтелекту стають все більш складними, вони можуть передбачати потенційні загрози безпеці з безпрецедентною точністю. Аналізуючи величезні обсяги даних із різноманітних джерел, штучний інтелект може виявити ознаки раннього попередження про терористичну діяльність, кібератаки чи геополітичні кризи, дозволяючи вживати більш активні заходи безпеки.

6. Об’єднання людини та ШІ.

Майбутнє національної безпеки, ймовірно, передбачатиме тісну співпрацю між людьми-операторами та системами ШІ. Це може включати вдосконалені ШІ системи підтримки прийняття рішень для командирів, ШІ-пілотів винищувачів або помічників ШІ для аналітиків розвідки. Розробка ефективних протоколів та інтерфейсів для об'єднання людини та штучного інтелекту буде ключовою сферою уваги.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Adam Kilsby (2024). Artificial intelligence: threats and opportunities in national security. *Zaizi.* URL: https://www.zaizi.com/blog/artificial-intelligence-threats-and-opportunities-in-national-security/

2. Застосування штучного інтелекту у сфері національної безпеки та обороноздатності держави (2024). *Сідкон.* URL: https://sidcon.com.ua/tpost/7vuygong71-zastosuvannya-shtuchnogo-ntelektu-u-sfer

Діордіца Ігор Володимирович,
д.ю.н., професор, професор кафедри приватного та публічного права,
Київський національний університет технологій та дизайну (м. Київ)

НОРМАТИВНО-ПРАВОВИЙ АНАЛІЗ ПРОБЛЕМАТИКИ ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ БЕЗПЕКИ УКРАЇНИ ЗА ДОПОМОГОЮ ШТУЧНОГО ІНТЕЛЕКТУ З УРАХУВАННЯМ ДОСВІДУ ОЛІМПІЙСЬКИХ ІГОР В ПАРИЖІ 2024 РОКУ

На початку 2024 року, із метою гарантування безпеки під час проведення Олімпійських ігор в Парижі, французький уряд уклав контракти з чотирма компаніями – Videtics, Orange Business, ChapsVision та Wintics, які активно використовують можливості штучного інтелекту (ШІ).