Шевчук Т. А.,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і кримінології ННІ № 1,
Харківський національний університет внутрішніх справ
(м. Харків, Україна)

Божук К. О.,
курсант 4 курсу ННІ № 1,
Харківський національний університет внутрішніх справ
(м. Харків, Україна)

ЗАГРОЗИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ОБОРОНОЗДАТНОСТІ ДЕРЖАВИ

Стрімкий розвиток інформаційних технологій та цифрових платформ призвів до змін технологічного ландшафту, що мало суттєвий вплив на всі сфери суспільного життя. Не є виключенням і сфера правоохоронної діяльності, яка спрямована на захист прав і свобод громадян, забезпечення законності та правопорядку, що є ключовими аспектами стабільного функціонування будь-якого суспільства. На сьогоднішній день впровадження цифрових технологій у роботу правоохоронних органів відкриває нові можливості для запобігання злочинності. Серед інноваційних рішень особливе місце займають технології штучного інтелекту (далі – ШІ), застосування яких у роботі органів кримінальної юстиції щодо аналізу та прогнозування злочинності, виявлення, розслідування та запобігання кримінальним правопорушенням дає можливість оптимізувати відповідні процеси та досягти кращих результатів за коротші терміни.

Штучний інтелект є невід'ємним елементом захисту національної безпеки та підвищення рівня обороноздатності держави. Використання комп'ютерних моделей і алгоритмів для виконання завдань у військових операціях, кібербезпеці, розвідці та аналітиці даних відкриває нові можливості для підвищення ефективності управлінських і бойових рішень.

Стрімким поштовхом запровадження технологій штучного інтелекту в сферу національної безпеки та обороноздатності України, як прикро б не було, стало повномасштабне вторгнення у 2022 році. За останні три роки можливості використання ШІ стали вражаючими, особливо у військовій сфері. Зокрема, технології штучного інтелекту сприяють моніторингу та відстеженню переміщень ворожої техніки й особового складу, підвищенню ефективності перехоплення ракетних загроз, покращенню наведення БПЛА на цілі та автоматизації розмінувальних робіт. Вже впроваджуються системи протиповітряної оборони, оснащені алгоритмами ШІ, які здатні аналізувати

траєкторії польоту об’єктів та приймати швидші й точніші рішення у режимі реального часу [1].

Однак необхідно бути свідомими щодо ризиків та загроз, які існують у цій галузі, зокрема у зв’язку із війною, в тому числі в інформаційному просторі, коли ворог використовує ШІ як один із інструментів ведення війни, засіб проведення інформаційно-психологічних операцій з метою ефективного впливу на громадську думку (діпфейк, частковий діпфейк, ШІ-контент для підсилення емоційного ефекту повідомлень, тощо).

Крім того, держава-агесор може використовувати ШІ для вчинення так званих «воєнно-контекстуальних кіберзлочинів», метою яких є підрив обороноздатності держави, зокрема диверсій (ст. 113 КК України), перешкоджання законній діяльності Збройних Сил України та інших військових формувань (ст. 114-1 КК України), несанкціонованого поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (ст. 114-2 КК України), терористичних актів (ст. 258 КК України), воєнних злочинів (ст. 438 КК України).

Попри значний потенціал і широкі можливості технологій штучного інтелекту, останнім часом спостерігається тенденція їх активного використання правопорушниками, які знаходять нові форми злочинної діяльності, засновані на цифрових технологіях. Можна констатувати, що використання штучного інтелекту супроводжується низкою проблем, вирішення яких має стати одним із пріоритетних завдань для наукової спільноти та державних інституцій. Під час розроблення й упровадження систем штучного інтелекту особливу увагу слід приділяти питанням безпеки, надійності, прозорості, справедливості, етичності та недискримінаційності, а також забезпеченню дотримання основних прав людини. Оскільки передбачити всі наслідки застосування новітніх технологій не завжди можливо, з поширенням ШІ у повсякденне життя дедалі більшої актуальності набуває проблема захисту прав і свобод людини та громадянина [2, с. 19].

Додаткову проблему становить відсутність чіткого розмежування відповідальності за рішення, прийняті за участю або під впливом ШІ, що викликає серйозні правові та етичні запитання. У зв’язку з цим вкрай важливо забезпечити постійний людський контроль над військовими системами, які використовують штучний інтелект, та розробити національні і міжнародні механізми регулювання їх застосування.

Оскільки штучний інтелект у військових системах залишається вразливим до спеціалізованих кібератак, які використовують внутрішні обмеження алгоритмів. Навіть незначна, але цілеспрямована зміна вхідних даних може призвести до критичних помилок у роботі ШІ, попри його ефективність у нормальних умовах. Тому загрозою його використання є повна залежність від алгоритмів, що в разі його пошкодження може призвести до нерозуміння як протидіяти небезпечним факторам [1].

Використання технологій штучного інтелекту для гарантування національної безпеки та обороноздатності України має комплексний характер, що охоплює міжвідомчу та міжнародну взаємодію. Це передбачає реалізацію заходів як на національному, так і на міжнародному рівнях. Визначення стратегічних пріоритетів, глибоке розуміння загроз у сфері безпеки й оборони, пошук ефективних рішень, а також тісна співпраця між правоохоронними органами, спеціалізованими структурами сектору безпеки України та іноземними партнерами сприятимуть формуванню ефективної системи протидії сучасним викликам. Очевидно, що лише завдяки міжнародній співпраці та скоординованим міжвідомчим діям як усередині країни, так і на міжнародній арені можливо ефективно вирішувати актуальні завдання у сфері національної безпеки в умовах сучасних глобальних викликів [3, с. 360].

Попри значний потенціал ШІ у зміцненні обороноздатності та забезпеченні національної безпеки, його застосування супроводжується низкою серйозних ризиків. Варто розуміти що ШІ виступає одночасно як потужний інструмент зміцнення національної безпеки, так і потенційне джерело нових загроз. Він фактично є технологією подвійного призначення, яка, залежно від способу застосування, може діяти як союзник, так і становити реальну загрозу безпеці держави. Це вимагає виваженого, комплексного та етично відповідального підходу до його впровадження у сферу національної безпеки та оборони. У зв'язку з цим критично важливим є формування цілісної, несуперечливої нормативно-правової бази у сфері кібербезпеки, гармонізація національного законодавства із законодавством ЄС у питаннях використання ШІ, забезпечення етичного контролю та збереження людського фактора в системах управління безпеки й оборони.

Список використаних джерел:

1. Застосування штучного інтелекту у сфері національної безпеки та обороноздатності держави URL: https://sidcon.com.ua/tpost/7vuygong71-zastosuvannya-shtuchnogo-ntelektu-u-sfer
2. Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. 2022. Випуск 4 (29). С.12–46
3. Шевчук В.М Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. *Юридичний науковий електронний журнал.* № 2024. № 6. С. 356–361