DOI https://doi.org/10.36059/978-966-397-501-6-149

Блик Юрій Олександрович,
аспірант кафедри національного,
міжнародного прав та правоохоронної діяльності
Херсонський державний університет
ORCID ID: 0009-0008-8012-0104
м. Херсон, Україна

ПРАВОВІ АСПЕКТИ ІНТЕЛЕКТУАЛІЗАЦІЯ ПРИКОРДОННОГО КОНТРОЛЮ

Сучасна парадигма забезпечення національної безпеки та недоторканності державних кордонів зазнає докорінної трансформації під впливом четвертої та п'ятої промислових революцій (т.з. Індустрії 4.0. та Індустрії 5.0.), що зумовлює перехід від традиційних лінійних моделей охорони кордону до комплексних, інтелектуалізованих систем управління ризиками.

У межах цієї трансформації прикордонний контроль дедалі більше розглядається не як сукупність ізольованих фізичних заходів, а як багатовимірний інформаційно-аналітичний процес, інтегрований у загальнодержавну систему безпеки. Такий підхід корелює з положеннями Стратегії національної безпеки України, де наголошується на необхідності впровадження цифрових та інноваційних рішень у секторі безпеки і оборони (п. 63 Стратегії визначає одним із напрямів розвитку сектору безпеки і оборони «забезпечити розвиток та удосконалення загальнодержавної системи захисту державного кордону, зокрема імплементацію європейських стандартів прикордонної безпеки, скоординовану діяльність державних органів України та військових формувань для системного розвитку інтегрованого управління державним кордоном України» [1]), а також із Законом України «Про національну безпеку України», який закріплює пріоритет превентивного реагування на загрози (п. 5 ст. 3 Закону визначає, що «Загрози національній безпеці України та відповідні пріоритети державної політики у сферах національної безпеки і оборони визначаються у Стратегії національної безпеки України, Стратегії воєнної безпеки України, Стратегії кібербезпеки України, Стратегії інтегрованого управління державним кордоном України…» [2].

Актуальність впровадження технологій Big Data та AI у сфері прикордонного контролю обумовлена стрімким зростанням обсягів

міжнародного товарообігу та мобільності населення, що в т.ч. сприяє формуванню складних мережевих структур транскордонної злочинності. Традиційний вибірковий прикордонний контроль, заснований на суб'єктивній оцінці або формальних індикаторах ризику, дедалі частіше виявляється неефективним щодо діяльності організованих злочинних груп, які використовують цифрові платформи, шифровані канали зв'язку та фінансові технології для маскування протизаконної діяльності. У цьому контексті інтелектуалізація прикордонного контролю постає як стратегічна необхідність переходу до предиктивної моделі безпеки, де ключовим завданням стає виявлення аномалій у масивах даних ще до моменту фактичного вчинення правопорушення.

Практичне використання великих даних у прикордонній сфері полягає у консолідації різнорідних інформаційних потоків, що надходять із систем біометричного контролю, відеоспостереження, митних та прикордонних інформаційних баз, реєстрів пасажирських перевезень, а також даних дистанційного зондування Землі (наприклад, автоматизоване виявлення несанкціонованих змін інфраструктури або ландшафту в прикордонній зон, використання мультиспектральних та гіперспектральних знімків для виявлення замаскованих об'єктів). Аналогічні підходи вже реалізуються в межах європейських ініціатив, зокрема системи EUROSUR «для обміну інформацією та співпраці між державами-членами та Європейською агенцією прикордонної та берегової охорони» [3] і механізмів попереднього аналізу пасажирських даних Passenger Name Record (інструменту для запобігання та протидії тероризму, інших транскордонних злочинів шляхом виявлення підозрілих схем подорожей, ідентифікації злочинців та ін. [4, с. 5]), що дозволяють оцінювати ризики вчинення транскордонних злочинів ще до фактичного перетину кордону.

Особливе значення у протидії транскордонній злочинності має аналіз поведінкових патернів та побудова графів соціальних і логістичних зв'язків. Наприклад, алгоритми штучного інтелекту ідентифікують так звані «ланцюгові перельоти», коли особа використовує складні маршрути з багатьма пересадками, що економічно не виправдані, або придбаває квитки за готівку в останній момент перед вильотом. Поєднання цих ознак із даними про попередні правопорушення або зв'язки з особами, що перебувають під наглядом, створює складний індикатор ризику, який дозволяє виявити канали незаконної міграції або торгівлі людьми ще на етапі реєстрації на рейс. Подібні індикатори активно застосовуються в ризик-орієнтованих моделях митного та прикордонного контролю, що відповідає стандартам Всесвітньої митної організації та рекомендаціям

Європейської Агенції з прикордонної та берегової охорони (FRONTEX). Водночас автоматизовані системи розпізнавання облич і біометричних даних дозволяють у режимі реального часу співставляти інформацію з національними та міжнародними базами розшуку, не підміняючи при цьому дискреційні повноваження посадової особи.

Запровадження концепції Індустрії 5.0 суттєво змінює філософію використання штучного інтелекту в прикордонній сфері, доповнюючи технологічну ефективність людиноцентричним та етичним виміром. Якщо Індустрія 4.0 була зосереджена на автоматизації та швидкості обробки інформації, то Індустрія 5.0 акцентує на синергії між людиною і машиною, де алгоритми підтримують прийняття рішень, але не усувають відповідальність інспектора. Такий підхід узгоджується з міжнародними стандартами захисту прав людини, зокрема положеннями Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних [5] та Загального регламенту про захист даних [6], принципи яких імплементуються і в українське законодавство.

Водночас інтеграція Big Data та AI у прикордонну безпеку породжує складні правові та етичні виклики, пов'язані із захистом персональних даних, недопущенням дискримінації та забезпеченням прозорості алгоритмічних рішень. Відповідно до Закону України «Про захист персональних даних», використання таких технологій повинно супроводжуватися чітким визначенням мети обробки інформації, пропорційністю втручання та ефективними механізмами контролю [7]. Додатковим викликом є ризик використання злочинними угрупованнями власних інтелектуальних систем для обходу державних механізмів контролю, що фактично формує умови для технологічної конкуренції у сфері безпеки державних кордонів.

Узагальнюючи зауважимо, що інтелектуалізація прикордонного контролю, підсилена ціннісними орієнтирами Індустрії 5.0 та належним нормативно-правовим забезпеченням, постає безальтернативним напрямом розвитку сучасної держави. Поєднання аналітичного потенціалу великих даних, адаптивності штучного інтелекту та професійного досвіду персоналу дозволяє перейти від реактивного реагування до системного прогнозування загроз. В умовах триваючої збройної агресії та гібридних впливів з боку росії розбудова інтелектуального кордону стає ключовим елементом загальнонаціональної стійкості, забезпечуючи ефективне блокування транскордонних каналів дестабілізації при збереженні балансу між безпекою, правами людини та відкритістю для легальної мобільності.

Література:

1. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14 вересня 2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#top (дата звернення: 04.04.2025)

2. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 07.04.2025)

3. Регламент Європейського Парламенту і Ради (ЄС) № 2019/1896 від 13 листопада 2019 року про Європейську прикордонну і берегову охорону та скасування Регламенту (ЄС) № 1052/2013 та Регламенту (ЄС) № 2016/1624: Європарламент, Рада ЄС; Регламент, Міжнародний документ, Правила від 13.11.2019 № 2019/1896. URL: https://zakon.rada.gov.ua/laws/show/984_016-19/ed20191113#n161 (дата звернення: 12.04.2025)

4. Міжнародний досвід та кращі практикм у сфері попередньої інформації про пасажирів (API) записі пасажирів (PNR) / Ендрю Прістлі, Марк Бове, 2021. 52 с. URL: https://www.osce.org/sites/default/files/f/documents/a/6/510620.pdf (дата звернення: 09.04.2025)

5. Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Рада Європи від 28 січня 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 11.04.2025)

6. Регламент європейського парламенту і ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 14.04.2025)

7. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 11.04.2025)