УДК 342.95:351
DOI https://doi.org/10.32782/2521-6473.2024-3.3

А. В. Кумейко, кандидат юридичних наук,
докторант відділу аспірантури і докторантури
Національної академії Служби безпеки України

УДОСКОНАЛЕННЯ СТРАТЕГІЇ І ТАКТИКИ ЗАПОБІГАННЯ ПРАВОПОРУШЕННЯМ, ЩО ПОСЯГАЮТЬ НА ДЕРЖАВНУ БЕЗПЕКУ

У статті досліджено питання удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку. Вказано, що питання удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку, доцільно вирішити шляхом прийняття низки узгоджених законодавчих актів, які містили б як матеріальні, так і процесуальні норми, враховували б інтереси держави, суспільства й окремої особи при застосуванні адміністративного примусу. Констатовано, що одним із правових заходів, який може вплинути на ефективність діяльності органів Служби безпеки України у сфері забезпечення державної безпеки, на підвищення їх авторитету серед населення, розглядається законодавче реформування існуючої структури органу спеціального призначення, яке сприятиме зростанню рівня професіоналізму, підніме престиж цієї Служби, авторитет її працівників, додатково перешкоджатиме залученню представників Служби безпеки України не за компетенцією. Необхідність реформування сектора безпеки зумовлена також і прийняттям Україною міжнародно-правових зобов'язань у сфері забезпечення прав людини і громадянина, прагненням вступу до Європейського Союзу. Зазначено, що виконання покладених на Службу безпеки України завдань, визначених законодавством, є можливим у першу чергу шляхом ефективної організації процесу оперативно-службової діяльності (ОСД). При цьому особливої важливості в роботі Служби безпеки України набули не лише традиційно результативні й високоінтелектуальні складники ОСД, (контррозвідка, захист національної державності тощо), а і напрямок міжнародного співробітництва, який з 2022 року має подекуди вирішальний вплив на процес удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку.

Ключові слова: *стратегії, тактики, запобігання, правопорушення, безпека, державна безпека.*

A. V. Kumeiko. Improving the strategy and tactics of preventing offenses encroaching against the state security

The article examines the issue of improving the strategy and tactics of prevention of offenses that encroach on state security. It is indicated that the issue of improving the strategy and tactics of preventing offenses that encroach on state security should be resolved through the adoption of a number of coordinated legislative acts that would contain both substantive and procedural norms, would take into account the interests of the state, society and the individual in the application of administrative coercion. It is stated that one of the legal measures that can affect the effectiveness of the activities of the Security Service of Ukraine in the field of state security, to increase their authority among the population, is the legislative reform of the existing special-purpose law enforcement structure, which will contribute to the growth of the level of professionalism, raise the prestige of this Service, the authority of its employees, and additionally prevent the involvement of representatives of the Security Service of Ukraine for other purposes. The need to reform the security sector is also due to Ukraine's acceptance of international legal obligations in the field of human and civil rights, the desire for a full-fledged step into the European Union. It is noted that the fulfillment of the tasks assigned to the Security Service of Ukraine, defined by law, is possible, first of all, through the effective organization of the process of operational and service activities (OSD). At the same time, of particular importance in the work of the Security Service of Ukraine are not only the traditionally effective and highly intellectual components of the DSO (counterintelligence, protection of national statehood, etc.), but also the direction of international cooperation, which since 2022 sometimes has a decisive impact on the process of improving the strategy and tactics of preventing offenses that encroach on state security.

Key words: *strategies, tactics, prevention, offenses, security, state security.*

Постановка проблеми. Одним із правових заходів, який може вплинути на ефективність діяльності органів Служби безпеки України у сфері забезпечення державної безпеки, на підвищення їх авторитету серед населення, розглядається законодавче реформування існуючої правоохоронної функції органу спеціального призначення, яке сприятиме зростанню рівня професіоналізму, підніме престиж цієї Служби, авторитет її працівників, додатково перешкоджатиме залученню представників Служби безпеки України не за компетенцією. Необхідність реформування сектора безпеки зумовлена також і прийняттям Україною міжнародно-правових зобов'язань у сфері забезпечення прав людини і громадянина, прагненням повноцінного ступу до Європейського Союзу.

Проте, на нашу думку, удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку, доцільно пов'язати із законодавчим запровадженням порядку й підстав використання нових видів заходів адміністративного запобігання і припинення, потреба в застосуванні яких залежить від становлення й розвитку нових суспільних відносин, науково-технічного прогресу, зокрема зумовленого появою штучного інтелекту.

Аналіз останніх досліджень та публікацій. Діяльність Служби безпеки України, зокрема її організаційно-функціональний аспект завжди перебував у центрі уваги науковців: М.І. Ануфрієва, А.М. Благодарного, О.К. Жарого, А.В. Іщенка, І.М. Копотуна, І.М. Коропатніка, О.В. Кривенка, І.В. Кубарєва, Ю.Б. Курилюка, О.М. Литвинова, В.Г. Пилипчука, М.П. Стрельбицького. Між тим, їх увага завжди була сконцентрована на окремих сферах і напрямах діяльності Служби безпеки України. Питання удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку у спеціальній літературі досліджувалося фрагментарно, що актуалізує пропоноване дослідження.

Мета статті. Дослідити питання удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку.

Виклад основного матеріалу. Варто вказати, що у швидко змінному ландшафті глобальної безпеки штучний інтелект (ШІ) стає тією трансформаційною силою, що змінює стратегії і тактики підходу країн до запобігання правопорушенням, що посягають на державну безпеку, та й безпеки в цілому, розвідки та стратегічного планування. Оскільки країни по всьому світу постійно інвестують у технології штучного інтелекту, наслідки для національної безпеки є глибокими та далекосяжними.

Варто вказати, що 1 серпня 2024 року набрав чинності Європейський закон про штучний інтелект (Artificial Intelligence Act) [1], проте більшість положень закону почнуть застосовувати 2 серпня 2026 року. Закон визначає, що пріоритетом є забезпечення того, що системи штучного інтелекту будуть безпечними, прозорими, можуть бути відслідковуваними, не дискримінаторними та екологічно безпечними. Зокрема, він встановлює: гармонізовані правила щодо введення на ринок, введення в експлуатацію та використання систем штучного інтелекту; заборони деяких практик у сфері штучного інтелекту; конкретні вимоги до систем штучного інтелекту високого ризику та обов'язки операторів таких систем; гармонізовані правила щодо прозорості для певних систем штучного інтелекту; правила моніторингу ринку, управління моніторингом ринку та забезпечення виконання; заходи щодо підтримки інновацій, включаючи стартапи [2]. Отже, розвиток та впровадження в життя нових технологій є тенденцією часу, яка вже має незворотній ефект.

Варто вказати, що однією з найважливіших переваг штучного інтелекту в національній безпеці є його здатність швидко та ефективно обробляти та аналізувати величезні обсяги даних. Зокрема, Служба безпеки України та всі правоохоронні та розвідувальні органи генерують величезну кількість інформації з різних джерел, включаючи супутникову візуалізацію, перехоплення комунікацій та розвідку з відкритим кодом. Системи, що працюють на основі штучного інтелекту, можуть переглядати ці дані, виявляючи закономірності, аномалії та потенційні загрози, які можуть пропустити людські аналітики.

Особливо це є вкрай важливим під час дії правового режиму воєнного стану, оскільки, штучний інтелект може аналізувати супутникові зображення для виявлення змін у військових установках або незвичайних переміщень військ. Моделі обробки природної мови (NLP) можуть сканувати мільйони публікацій у соціальних мережах, щоб виявити нові загрози безпеці або відстежувати поширення дезінформаційних кампаній. Ця розширена аналітична здатність дозволить Службі безпеки України приймати більш обґрунтовані рішення та швидше реагувати на потенційні загрози в процесі запобігання правопорушенням, що посягають на державну безпеку.

Експерти підтверджують, що можливості ШІ пропонують цінну підтримку для планування національної безпеки та розробки стратегії [3]. Аналізуючи історичні дані та поточні тенденції, моделі штучного інтелекту можуть прогнозувати потенційні ризики безпеки, геополітичні події та нові загрози. Це дозволить Службі безпеки України брати участь у більш складному плануванні сценаріїв, передбачаючи можливі напади або кризи та готуючи відповідні відповіді.

Наприклад, системи штучного інтелекту могли б моделювати потенційний вплив різних факторів – таких як економічна нестабільність, зміна клімату або політичні заворушення – на регіональну безпеку, допомагаючи політикам розробляти більш ефективні довгострокові стратегії безпеки [4].

Крім того, доцільно підкреслити, що останнім часом все більш витонченими стають кіберзагрози, у зв'язку з чим ШІ відіграє вирішальну роль у захисті критичної інфраструктури. ШІ контролює мережевий трафік у режимі реального часу, виявляючи аномалії та потенційні вторгнення набагато швидше та точніше, ніж традиційні системи безпеки. Наприклад AI-powered Threat Intelligence платформи можуть аналізувати глобальні дані про кіберзагрози, щоб передбачити та запобігти майбутнім атакам [5].

Крім того, ШІ може автоматизувати багато аспектів кібербезпеки, таких як управління патчами та оцінка вразливості, зменшуючи навантаження на співробітників Служби безпеки України та дозволяючи їм зосередитися на більш складних проблемах щодо запобігання правопорушенням, що посягають на державну безпеку.

ШІ забезпечує розробку автономних і напівавтономних систем, які можуть працювати в середовищах, занадто небезпечних або недоступних для людей. Сюди входять безпілотні повітряні апарати (UAVs) для розвідки та спостереження, автономні підводні транспортні засоби для морських операцій та роботизовані системи для утилізації вибухонебезпечних боєприпасів [6].

Ці системи на основі штучного інтелекту можуть удосконалити стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку, одночасно зменшуючи ризики для співробітників Служби

безпеки України. Разом з тим вони можуть працювати протягом тривалого періоду у суворих умовах, забезпечуючи постійні можливості спостереження та збору розвідданих.

Проте звісно, фахівці вказують й на окремі недоліки та ризики використання штучного інтелекту. Так, хоча системи штучного інтелекту можуть покращити кібербезпеку, вони також вразливі до складних атак. Потенційно може відбуватися маніпулювання вхідними даними або використовуватися слабкі місця в алгоритмах ШІ, щоб обійти ці системи. Наприклад, тонкі зміни зображень можуть обійти системи спостереження на основі штучного інтелекту, або ретельно створений текст може обійти фільтри вмісту штучного інтелекту. Ця вразливість може призвести до серйозних порушень безпеки або дезінформації, що звісно негативним чином може сказатися на забезпечення безпеки та процесі запобігання правопорушенням, що посягають на державну безпеку [4].

Крім того існує ризик того, що співробітники Служби безпеки України можуть стати надмірно залежні від цих технологій, оскільки його використання зумовлює потенційно зменшення використання критичного мислення, інтуїції та здатності розуміти складні контексти, що на сьогодні залишається унікальними людськими навичками, які є вирішальними при прийнятті рішень у сфері запобігання правопорушенням, що посягають на державну безпеку.

Надмірна залежність від ШІ може призвести до помилкового відчуття безпеки при оцінці загрози, якщо системи ШІ не зможуть врахувати нові або безпрецедентні форми правопорушень, що посягають на державну безпеку.

Використання ШІ в сфері національної безпеки часто передбачає обробку величезної кількості даних, включаючи інформацію про громадян, що викликає питання щодо конфіденційності даних та правомірності використання персональних даних.

Балансування потреб національної безпеки з індивідуальними правами на конфіденційність є постійною проблемою, оскільки технології штучного інтелекту стають більш поширеними. Саме тому Рада Європи прийняла перший в історії міжнародний юридично обов'язковий договір, спрямований на забезпечення дотримання прав людини, верховенства права та правових стандартів демократії при використанні систем штучного інтелекту. Відповідно нашій державі необхідно адаптувати новітнє європейське законодавство з національним, що є суттєвим бар'єром в процесі удосконалити стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку.

Звісно не слід забувати, й про те, що швидкий розвиток ШІ у сфері національної безпеки порушує існуючі етичні та правові аспекти. Для України загрозою приватній безпеці особи є непідконтрольність діяльності спецслужб та абсолютизація державного й суспільного інтересу. Поява й поширення нових технологій, які в декілька разів збільшують можливості для спостереження, збирання інформації, стеження, а також посилення закріплення заходів захисту публічної безпеки як одного з пріоритетів державної політики й розширення повноважень органів сектора безпеки дозволяють визнати такі посягання з боку правоохоронних органів і спецслужб головною й найсерйознішою загрозою праву на недоторканість приватного житла в Україні [7].

Розробка комплексних рекомендацій щодо відповідального використання ШІ в оборонних та розвідувальних операціях є складним завданням. Виникають питання щодо відповідного рівня людського контролю над системами штучного інтелекту, підзвітності рішень, керованих штучним інтелектом, та потенційних наслідків операцій з безпеки на основі штучного інтелекту щодо прав людини, національного та міжнародного права.

Уряди держав світу, зокрема США, Великої Британії та держав-членів ЄС, уже розробляють власні стратегії розвитку та регуляції ШІ. Україна теж рухається в цьому напрямку: у жовтні 2023 року Міністерство цифрової трансформації презентувало дорожню карту з регулювання ШІ [8]; окремі ініціативи з розвитку та застосування ШІ з'являються і на місцевому рівні. Проте звісно розробка внутрішніх документів Службою безпеки України щодо використання штучного інтелекту в процесі удосконалити стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку є надзвичайно актуальним та своєчасним питанням.

Ефективність систем штучного інтелекту в процесі удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку, значною мірою залежить від якості та репрезентативності даних, на яких вони засновані. Упереджені або неповні дані можуть призвести до помилкового аналізу та потенційно дискримінаційних результатів. Забезпечення того, щоб системи ШІ мали доступ до високоякісних, різноманітних та неупереджених наборів даних, є значним викликом, особливо враховуючи обмежений (закритий/секретний) характер великої кількості інформації про правопорушення, що посягають на державну безпеку.

Оскільки різні агентства та союзні країни розробляють власні системи штучного інтелекту для цілей безпеки, забезпечення сумісності між цими системами стає вирішальним. Встановлення загальних стандартів та протоколів для ШІ в національних додатках безпеки вимагатиме великої міжнародної співпраці та переговорів.

Більше того, варто пам'ятати, що інтеграція штучного інтелекту в національні охоронні операції вимагає співробітників Служби безпеки України, які б мали нові набори навичок. Наприклад, які могли розробляти, розгортати та інтерпретувати системи штучного інтелекту, а також розуміти більш широкі стратегічні та операційні контексти, що звісно є теж значним викликом для процесу удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку.

Більше того, оскільки майже всі держави на сучасному етапі, інвестують у штучний інтелект для національної безпеки, це створює новий вимір конкуренції у сфері запобігання правопорушенням, що посягають на державну безпеку.

ШІ, ймовірно, відіграватиме все більш важливу роль в інформаційній війні. Системи, що працюють на штучному інтелекті, можуть брати участь у аналізі спектру в режимі реального часу, швидко виявляючи та протидіючи ворожим комунікацій та радіолокаційним системам. Це може призвести до нової ери когнітивної інформаційної війни, де системи штучного інтелекту беруть активну участь.

Крім того, складні завдання, такі як розвідка, можуть бути керовані штучним інтелектом, що може сприяти ранній попереджувальній діяльності співробітників Служби безпеки України, що призведе до ефективного удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку.

Думається, що у зв'язку з тим, що ШІ стає все більш активним суб'єктом життєдіяльності людства для національної безпеки, ми можемо передбачити появу нових міжнародних організацій та угод, орієнтованих на управління ШІ у сфері безпеки та розвідки. Це може слугувати відправною крапкою для створення окремого структурного підрозділу Служби безпеки України.

Інтеграція штучного інтелекту в національну безпеку та процес удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку, тісно пов'язані та представляють складний ландшафт можливостей і викликів. Хоча ШІ пропонує значні переваги з точки зору аналізу даних, прогнозних можливостей в процесі запобігання правопорушенням, що посягають на державну безпеку, він також викликає питання з етикою, конфіденційністю тощо.

Важливим чинником майбутнього успішного використання ШІ Службою безпеки України є необхідність розробки етичних рекомендацій, нормативних рамок, з залученням найкращих практик використання ШІ у світовій практиці [9]. Метою використання ШІ в процесі запобігання правопорушенням, що посягають на державну безпеку, має бути підвищення безпеки та стабільності при одночасному пом'якшенні ризиків та збереженні прав людини, національного та міжнародного права.

Проте використання ШІ в процесі запобігання правопорушенням, що посягають на державну безпеку – це наше можливе майбутнє, тоді як використання технічних засобів, якими можна було б оперувати в діяльності по захисту державної безпеки, можна назвати різноманітні засоби негласного отримання інформації, спеціальні засоби для автоматичного фіксування порушень у сфері державної безпеки тощо.

Звісно, що впровадження новітніх технологій в діяльність Служби безпеки України потребує змін та доповнень до чинного законодавства, особливо в частині захисту права особи на приватне життя, зокрема доцільним вбачається:

1) внесення змін і доповнень до законодавства, створення й закріплення додаткових інститутів і механізмів захисту права особи на приватне життя;

2) створення сприятливих умов для дотримання прав громадян на приватність;

3) заборону й регулювання існуючих обмежень приватності, а також закріплення додаткових гарантій від зловживань у випадках обмеження останнього.

Правові колізії і протиріччя в національному законодавстві (щодо питань адміністративного затримання, ідентифікації особи, доставлення правопорушника і його приводу, складання протоколів, питання про порядок застосування адміністративного затримання у вихідні і святкові дні, врегулювання порядку особистого огляду й огляду речей тощо), призводять до того, що у співробітників Служби безпеки України виникають різні погляди на те, як їм діяти в тій чи іншій ситуації, як застосовувати ті чи інші заходи запобігання правопорушенням, що посягають на державну безпеку.

Висновки. Вважаємо, що врахування й вирішення зазначених правових проблем створить необхідні законодавчі передумови для діяльності співробітників Служби безпеки України по ефективному й координованому застосуванню заходів запобігання правопорушенням, що посягають на державну безпеку, сприятиме зміцненню правопорядку й міжнародного співробітництва.

Крім того, виконання покладених на Службу безпеки України завдань, визначених законодавством, є можливим у першу чергу шляхом ефективної організації процесу оперативно-службової діяльності (ОСД). При цьому особливої важливості в роботі Служби безпеки України набули не лише традиційно результативні й високоінтелектуальні складники ОСД, (контррозвідка, захист національної державності тощо), а і напрямок міжнародного співробітництва, який з 2022 року має подекуди вирішальний вплив на процес удосконалення стратегії і тактики запобігання правопорушенням, що посягають на державну безпеку.

Початок повномасштабного вторгнення країни-агресора зумовив від СБ України невідкладного вжиття системи заходів, спрямованих на започаткування, підтримання та розвиток партнерських відносин зі спецслужбами і правоохоронними органами країн світу.

Наразі центр міжнародного співробітництва (ЦМС) є головним підрозділом Служби безпеки України, відповідальним за міжнародну співпрацю, який забезпечує партнерські контакти з понад 100 спецслужбами і правоохоронними органами близько 60 країн. Це є найвищим показником за час функціонування української спецслужби, адже створено передумови для подальшого розширення числа зарубіжних партнерів, що дозволяє Службі безпеки України оперативно співпрацювати з потужними міжнародними організаціями для запобігання правопорушенням, що посягають на державну безпеку.

Список використаних джерел:

1. Artificial Intelligence Act. URL: https://artificialintelligenceact.eu/the-act/
2. EU AI Act: first regulation on artificial intelligence URL: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence
3. Пилипчук В.Г, Гиляка О.С. Проблема правового регулювання у сфері штучного інтелекту в контексті розвитку законодавства Європейського Союзу. URL: https://visnyk.kh.ua/web/uploads/journals_pdf/Вісник%20НАПрНУ_Том%2029(2)_2022.pdf#page=35
4. Banata A. Artificial Intelligence and National Security. URL: https://www.linkedin.com/pulse/artificial-intelligence-national-security-prof-ahmed-banafa-lg71c
5. AI-powered Threat Intelligence. URL: https://www.silobreaker.com/glossary/ai-in-threat-intelligence/
6. Unmanned aerial vehicle. https://www.britannica.com/technology/military-aircraft/Unmanned-aerial-vehicles-UAVs
7. Жарий О.К. Адміністративно-запобіжні заходи в діяльності Служби безпеки України. URL: https://nrat.ukrintei.ua/searchdoc/0417U000129/
8. Дорожня карта з регулювання штучного інтелекту в Україні. URL: https://cms.thedigital.gov.ua/storage/uploads/files/page/community/docs/Дорожня_карта_з_регулювання_ШІ_в_Україні_compressed.pdf
9. Lakhno V., Akhmetov B., Korchenko A., Alimseitova Z., Grebenuk V. Development of a decision support system based on expert evaluation for the situation center of transport cybersecurity. URL: https://www.elibrary.ru/item.asp?id=35719279