***Ханькевич Андрій Миколайович,***
кандидат юридичних наук, професор,
старший викладач кафедри досудового
розслідування Національного
юридичного університету
імені Ярослава Мудрого

## ПРЕДИКТИВНА АНАЛІТИКА В КОНТРРОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Стрімкий розвиток цифрових технологій та методів обробки великих даних відкриває принципово нові можливості для підвищення ефективності контррозвідувальної діяльності (далі – КРД). Традиційні підходи до організації роботи Служби безпеки України (далі – СБУ) потребують суттєвого переосмислення з урахуванням викликів сучасності та наявних технологічних можливостей.

За останні роки значно розширились можливості збору та аналізу різноманітних даних, що становлять інтерес у КРД СБУ. Водночас традиційні методи аналітичної роботи вже не здатні у потрібному обсязі забезпечити своєчасну та якісну обробку постійно зростаючих масивів інформації, що актуалізує питання впровадження предиктивної аналітики як сучасного інструментарію прогнозування та виявлення загроз державній безпеці України.

Сьогодні існують різні підходи до визначення поняття предиктивної (прогнозної) аналітики. Як зазначає О. Заєць, це є «вид аналітики даних, спрямованої на прогнозування майбутніх результатів, яка базується на отриманих історичних даних і методах аналітики, зокрема, таких як статистичне моделювання та машинне навчання» [1, с. 49].

Метою предиктивної аналітики є здійснення прогнозів щодо майбутніх подій та використання цих прогнозів для покращення процесу ухвалення рішень. При цьому важливо, що такі процедури можуть забезпечити достатній для практики рівень точності прогнозування [1, с. 50].

Аналіз положень Закону України «Про контррозвідувальну діяльність» дозволяє встановити безпосередній зв’язок між законодавчо визначеними завданнями контррозвідувальної діяльності та потенціалом предиктивної аналітики.

Ключовою метою контррозвідувальної діяльності, відповідно до статті 2 Закону, є «попередження, своєчасне

виявлення і запобігання зовнішнім та внутрішнім загрозам безпеці України, припинення розвідувальних, терористичних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що їм сприяють, та причин їх виникнення» [2]. Саме превентивний характер цієї мети зумовлює необхідність використання методів предиктивної аналітики, спрямованих на прогнозування майбутніх подій та загроз.

Серед основних завдань контррозвідувальної діяльності законодавець визначає «добування, аналітичну обробку та використання інформації, що містить ознаки або факти розвідувальної, терористичної та іншої діяльності спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на шкоду державній безпеці України» (ст. 2 Закону) [2], що безпосередньо співвідноситься з можливостями предиктивної аналітики щодо опрацювання великих масивів даних та виявлення прихованих закономірностей.

Важливо зазначити, що зазначений Закон передбачає широкий спектр джерел отримання інформації для контррозвідувальної діяльності, а саме «заяви і повідомлення громадян, осіб, залучених до конфіденційного співробітництва, посадових та службових осіб, громадських організацій, медіа; матеріали органів досудового розслідування та суду; запити, інформації та матеріали спеціальних служб і правоохоронних органів іноземних держав, міжнародних установ і організацій» (ст. 6) [2], що створює значний масив різнорідних даних, ефективне опрацювання яких можливе саме із застосуванням інструментів предиктивної аналітики.

«Комплексне застосування правових, профілактичних та організаційних заходів», визначене як один з основних принципів контррозвідувальної діяльності» (ст. 4 Закону) [2], також потребує використання сучасних аналітичних інструментів для оцінки ефективності та прогнозування результатів таких заходів.

Особливу увагу варто приділити й принципу «адекватності заходів щодо захисту державної безпеки реальним і потенційним загрозам» (ст. 4 Закону України «Про контррозвідувальну діяльність»), оскільки саме предиктивна аналітика надає можливість об’єктивної оцінки потенційних загроз та вибору найбільш адекватних методів реагування через своєчасне виявлення прихованих закономірностей у масивах різнорідних даних.

Практика застосування предиктивної аналітики спеціальними службами низки країн світу демонструє високу ефективність у сфері забезпечення національної безпеки. Зокрема, впровадження аналітичних методів прогнозування в діяльність спеціальних служб дозволило суттєво підвищити результативність превентивних заходів.

У США, Великій Британії, Німеччині, Нідерландах та Китаї розроблені та успішно використовуються спеціальні програмні комплекси, що дозволяють здійснювати прогнозування загроз національній безпеці. Такі системи спираються на аналіз трьох основних змінних: вид загрози, час та місце потенційного інциденту. Важливо, що ці аналітичні інструменти не потребують персональних даних для ефективного функціонування.

Показовим є досвід поліції Німеччини, де система «Precobs» використовує алгоритми та знання про минулі події для прогнозування можливих рецидивів [3, с. 1044]. Система генерує прогнози на основі найактуальніших даних, які можуть використовуватися службами як в оперативних, так і в профілактичних цілях.

Експериментальні дослідження, проведені в США, показали, що алгоритмічні методи прогнозування здатні передбачати загрози з удвічі вищою точністю порівняно з традиційним експертним аналізом. При цьому важливо розуміти, що предиктивна аналітика не замінює традиційних методів роботи спеціальних служб, а посилює їх шляхом застосування передових статистичних моделей та алгоритмів.

У сфері забезпечення національної безпеки досвід провідних держав світу демонструє активне впровадження систем стратегічного моніторингу інформації як різновиду предиктивної аналітики.

Показовим є досвід Німеччини, де застосування системи стратегічного моніторингу регулюється законом G10 [4], законність функціонування якої визнана Європейським судом з прав людини (Case of Weber and Saravia v. Germany, Application № 54934/00, ECHR, 2006) [5]. Система здійснює збір та аналіз інформації для попередження загроз, зокрема: міжнародного тероризму, незаконної зовнішньої торгівлі, міжнародних кібератак на критичну інфраструктуру.

У Великій Британії діє система Tempora (Big brother watch v. The United Kingdom, Applications no. 58170/13, 62322/14, 24960/15, ECHR, 2018), що дозволяє здійснювати аналіз даних

для забезпечення національної безпеки. Подібна система працює і в Швеції, де її функціонування також визнано правомірним (Case of Centrum för rättvisa v. Sweden, Application № 35252/08, ECHR, 2018) [5].

Ключовими особливостями таких систем є:

– автоматизована фільтрація інформації в режимі реального часу;

– застосування складних критеріїв пошуку;

– комплексна аналітична обробка даних;

– чітка регламентація процедур використання отриманої інформації.

Упровадження подібних систем предиктивної аналітики у КРД створює потужний інструментарій для раннього виявлення та запобігання загрозам національній безпеці через автоматизований аналіз значних масивів різнорідної інформації в режимі реального часу.

На основі аналізу практичних аспектів застосування предиктивної аналітики можна виділити ключові напрями її використання у сфері КРД.

Як зазначає А. Фергюсон, основними напрямами застосування є виявлення прихованих зв'язків та мереж (аналіз великих даних дозволяє з високою ймовірністю виявляти структури та зв'язки між особами, що становлять інтерес), комплексний моніторинг активності (системи здатні обробляти візуальні дані, активність в інтернеті, цифрові сліди) та прогнозування загроз через алгоритми машинного навчання [6, с. 272].

За даними компанії Mashable, сьогодні у світовій практиці сформувались два основні підходи до організації систем предиктивної аналітики:

– неперсоніфіковані системи, що працюють виключно зі статистичними даними;

– персоніфіковані системи, що здійснюють комплексний аналіз широкого спектру даних про конкретних осіб [7].

У контексті КРД особливо важливою є здатність таких систем виявляти приховані закономірності та аномалії в поведінці об'єктів спостереження на ранніх стадіях формування загроз, що створює можливості для превентивного реагування.

Важливим елементом предиктивної аналітики є предиктор – фізична або юридична особа, яка призначена для прогнозування можливої майбутньої поведінки. Множина предикторів становить модель предиктивної аналітики, що

дозволяє прогнозувати певні події в майбутньому з визначеним ступенем ймовірності. Безумовним є те, що предиктивну аналітику найефективніше використовувати за наявності широкого спектру максимально повних та очищених пакетів даних. Точність результатів аналізу прямо залежить від обсягу доступних даних з різних сфер [1, с. 51-52].

Отже проведене дослідження дозволяє сформулювати такі висновки щодо ролі та місця предиктивної аналітики в контррозвідувальній діяльності:

1. У сучасних умовах предиктивна аналітика виступає потужним інструментом КРД, що через використання методів статистичного моделювання, машинного навчання та штучного інтелекту забезпечуватиме якісно новий рівень прогнозування та виявлення загроз державній безпеці України. Застосування комплексу аналітичних методів – від поведінкового аналізу до виявлення аномалій та кластерного аналізу, створює можливості для раннього виявлення ознак підготовки ворожих операцій та спроб проникнення у критичну інфраструктуру.

2. Практичний досвід провідних держав світу демонструє, що впровадження систем предиктивної аналітики дозволяє перейти від реактивної до проактивної моделі забезпечення державної безпеки, що підвищить ефективність контррозвідувальних заходів через автоматизацію процесів виявлення загроз та оптимізацію використання наявних ресурсів.

3. Водночас ефективне використання можливостей предиктивної аналітики вимагатиме комплексного підходу до модернізації організаційно-технічної складової КРД, зокрема високого рівню автоматизації процесів та розширення технологічних можливостей моніторингу.

За таких умов впровадження предиктивної аналітики стає не просто технологічною інновацією, а необхідною передумовою забезпечення спроможності контррозвідки ефективно протидіяти сучасним викликам та загрозам національній безпеці України.

***Список використаних джерел***

1. Заєць О. Prediction Analytics (прогнозна аналітика): визначення, типи моделей і використання. *Актуальні питання та перспективи розвитку кримінального аналізу в правоохоронній системі України* : матеріали науково-практ. конф., м. Київ, 17 листоп. 2023 р. Київ, 2023. С. 49–55. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/6a681285-7ff9-4718-9451-dd907f56ba6f/content.

2. Про контррозвідувальну діяльність : Закон України від 26.12.2002 № 374-IV : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/374-15#Text.

3. Assessing the Generalizability of the Near Repeat Phenomenon / T. J. Youstin et al. *Criminal Justice and Behavior*. 2011. Vol. 38, no. 10. P. 1042–1063. URL: https://doi.org/10.1177/0093854811417551.

4. G 10 - Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. *Gesetze im Internet*. URL: https://www.gesetze-im-internet.de/g10_2001/BJNR125410001.html.

5. HUDOC - European Court of Human Rights. *HUDOC - European Court of Human Rights*. URL: https://hudoc.echr.coe.int/fre#%7B»sort»:[«kpdate%20Descending»], «itemid»:[«001-76586»]%7D.

6. Ferguson A. G. Chapter: «Blue Data» (Excerpt from «The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement»). *SSRN Electronic Journal*. 2017. URL: https://doi.org/10.2139/ssrn.3959202.

7. China is using AI to predict who will commit crime next. *Mashable*. URL: https://mashable.com/article/china-ai-crime-minority-report?test_uuid=01iI2GpryXngy77uIpA3Y4B&test_variant=b.

***Худенко Дмитро Миколайович,***
ветеран Національної поліції України,
керівник Департаменту кримінального аналізу у 2021–2023 роках

## РОЛЬ КРИМІНАЛЬНОГО АНАЛІЗУ В РОЗСЛІДУВАННЯХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ДЕ ПРЕДМЕТОМ АБО ЗАСОБОМ ВЧИНЕННЯ Є ШТУЧНИЙ ІНТЕЛЕКТ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ З ПІДГОТОВКИ ФАХІВЦІВ

Глобальна дискусія щодо використання штучного інтелекту вплинула і на сферу кримінального аналізу, де активно почала набирати обертів з 20 років нашого століття. Втім, одною із перших, хто приєднався до неї виявилась ще 2018 року харківська школа кримінального аналізу [1]. Зокрема, Д.Ю. Узловим штучний інтелект було розглянуто, як метод та технологію. Поступово науковим товариством вказано на потребу зміни підходів за допомогою штучного інтелекту [2], його значний технологічний потенціал [3, 4, робились спроби вивчення відповідного закордонного досвіду [5], а сам штучний