УДК 343.1
DOI https://doi.org/10.32689/2617-9660-2025-2(34)-68-76

Сервецький Іван Васильович,
доктор юридичних наук, доцент, професор кафедри національної безпеки Інституту безпеки ім. Володимира Великого ПрАТ «ВНЗ «Міжрегіональної Академії управління персоналом», вул. Фрометівська, 2, м. Київ, 03039; siv2055@gmail.com; https://orcid.org/0000-0002-5713-8911

Сушко Олександр Володимирович,
аспірант кафедри правоохоронної та антикорупційної діяльності Навчально-наукового інституту права ім. Володимира Великого ПрАТ «ВНЗ «Міжрегіональної Академії управління персоналом», вул. Фрометівська, 2, м. Київ, 03039; eninpoker1917@gmail.com; https://orcid.org/0009-0008-2602-6328

ВИКОРИСТАННЯ ТЕХНІЧНИХ ЗАСОБІВ У РОЗВІДУВАЛЬНІЙ ДІЯЛЬНОСТІ: ПОНЯТТЯ, МЕТОДИ, ІСТОРІЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

Анотація. *У статті здійснено історичний аналіз розвідувальної діяльності в Україні. Розглянуто основні етапи розвитку розвідувальної діяльності, яка має глибокі історичні коріння.*

Основний акцент зроблено використанні технічних можливостях пошуку та фіксації розвідувальній інформації, яку добували розвідники на теренах України так і за її межами.

Очевидно, що ефективність здобуття розвідувальної інформації залежить від методів та якості засобів, які використовує розвідка у своїй роботі.

Сьогодні розвиток та вдосконалення інформаційних технологій, що використовується в розвідувальній діяльності залежить від методів та якості технічних засобів і їх можливостей в добуванні та використанні чутливої для країни інформації.

Технічними засобами розвідки традиційно вважається: апарати, машини та виготовлені з їх основі технічні та технологічні пристрої та обладнання, технічні можливості загального користування та контролю за поверхнею Землі, повітряного (космічного) простору й окремих об'єктів. Усі ці технічні засоби дозволяють отримувати, обробляти будь-яку інформацію, яка є розвідувальною інформацією.

Засобів, які використовує розвідка у своїй роботі стала технічна розвідка, тобто здобуття інформації за допомогою технічних засобів розвідки.

Саме тому розвідувальні органи контролюють, аналізують та використовують усю інформацію, що надходить у всесвіті, а також збирають усю інформацію, фіксується за запомогою спеціальних технічних засобів, які використовують розвідувальні підрозділи.

Глибокий аналіз усієї інформації, яка надходить з відкритих джерел, а також аналіз таємної інформації, яка надходить із розвідувальних джерел дає можливість робити правильні висновки.

Ключові слова: *технічні засоби розвідувальної діяльності, фіксація, розвідувальна інформації, спецтехніка, операції, технічний прогрес, конспірація.*

Servetsky Ivan Vasilyovych,
Doctor of Law, Associate Professor, Professor at the Department of National Security of the Institute of Security Law named after Volodymyr Veliky «Interregional Academy of Personnel Management», 2, Frometivska Str, Kyiv, 03039; siv2055@gmail.com; https://orcid.org/0000-0002-5713-8911

Sushko Oleksandr Volodymyrovych,
Postgraduate Student at the Department of Law Enforcement and Anti-Corruption Activities of the Educational and Scientific Institute of Law named after Volodymyr Veliky «Interregional Academy of Personnel Management», 2, Frometivska Str, Kyiv, 03039; eninpoker1917@gmail.com; https://orcid.org/0009-0008-2602-6328

USE OF TECHNICAL EQUIPMENT IN INTELLIGENCE ACTIVITIES: CONCEPT, METHODS, HISTORY AND DEVELOPMENT PROSPECTS

Abstract. *The article provides a historical analysis of intelligence activities in Ukraine. The main stages of the development of intelligence activities, which have deep historical roots, are considered.*

The main emphasis is placed on the use of technical capabilities for searching and recording intelligence information obtained by intelligence officers in Ukraine and abroad.

It is obvious that the effectiveness of obtaining intelligence information depends on the methods and quality of the means used by intelligence in its work.

Today, the development and improvement of information technologies used in intelligence activities depends on the methods and quality of technical means and their capabilities in obtaining and using information sensitive to the country.

Technical means of intelligence are traditionally considered to be: devices, machines and technical and technological devices and equipment made on their basis, technical capabilities for general use and control of the Earth's surface, air (space) space and individual objects. All these technical means allow to receive, process any information that is intelligence information.

The means that intelligence uses in its work has become technical intelligence, that is, obtaining information using technical means of intelligence.

That is why intelligence agencies control, analyze and use all information that comes from the universe, and also collect all information, recorded with the help of special technical means used by intelligence units.

Deep analysis of all information that comes from open sources, as well as analysis of secret information that comes from intelligence sources makes it possible to draw the right conclusions.

Key words: *technical means of intelligence activities, recording, intelligence information, special equipment, operations, technical progress, conspiracy.*

Постановка проблеми. Розвідувальної діяльності, яка здійснюється на теренах України є надзвичайно актуальною для нашого часу. Особливо це стосується ситуації, коли на Україну здійснила агресію російська федерація.

Досягнення науково-технічного прогресу дають цінніші ресурси та можливості для здійснення розвідувальної діяльності.

Тому провідні держави докладають великих зусиль для створення оптимальних умов, необхідних для розвитку різноманітних наукових програм і дослідницьких проектів, які направлені на здійснення якості розвідувальної роботи. У цьому контексті науково-технічна розвідка має особливе значення. Вона «проникає» у найновіші наукові таємниці, здатні у перспективі впливати на розвиток людства, чим, по суті, прискорює роботу наукової галузі своєї держави і досягнення важливих науково - технічних проектах.

Водночас робота науково-технічної розвідки допомагає зекономити матеріальні ресурси й уникнути можливих помилок при виконанні вченими тих чи інших досліджень, в першу чергу, в оборонній сфері. Науково-технічна розвідка – це розвідувальна діяльність, об'єктами якої є закордонні науково-технічні розробки і досягнення цивілізацій. Головну увагу приділяють як фундаментальним, так і прикладним дослідженням іноземних вчених. Найбільший інтерес викликають науково-технічні характеристики, можливості і недоліки військових технологій, космічних технологій, ракетобудівництва тощо.

Важливим об'єктом науково-технічної розвідки є наукова інформація і технічні проекти досягнень вчених, які можна таємно скопіювати та передати зацікавленій науковій організації держави.

На початковій стадії загальної наукової і конструкторської розробки ідеї на академічному чи комерційному рівні інформація не є таємною, а отже, до неї легше знайти доступ, ніж після того, як отримані дослідниками результати знайдуть своє підтвердження.

На цьому етапі встановлюються суворі режимні заходи доступу, а тим більше на стадії завершальних випробувань.

Через таємний характер розвідувальної діяльності складно вести розмову про її успіхи у сфері науково-технічного шпіонажу.

В історичному контексті найбільш характерною особливістю розвідки був і залишається науково-технічний шпіонаж у західних державах. На здобування інформації про науково-технічні розробки і досягнення іноземних вчених, можливості й недоліки нових військових технологій, промислові винаходи в оборонній галузі російські спецслужби витрачають великі кошти, особливо під час сьогоднішньої війни: виготовлення та застосування різного типу дронів, ракетних технологій з точного наведення тощо.

Можна без перебільшення сказати, що значення науково-технічної розвідки зростає відповідно до розвитку можливостей сучасної науки і важливості їх осягнути як безпосередньо, так і «опосередковано», тобто за допомогою розвідувальної здатності.

Аналіз останніх досліджень і публікацій. Наукову базу у дослідженні розвідувальної діяльності слали такі праці вчених, як: Я.М. Антонюк, С.І. Білокінь, Л.В. Бородич, Д.В. Вєдєнєєв, О.М. Калюк, В.О. Козенюк, О.Р. Лебедєв, С.М. Мельниченко; В.М. Ніколь-ський, В.Т. Окіпнюк, О.І. Олійник, Е.П. Петровський, В.Г. Пилипчук, В.С. Сідак, О.В. Тимощук, Д.А. Тихоненков, Ю.І. Шаповал та ін.

Метою статті є аналіз та забезпечення успішної розвідувальної діяльності, яка здійснюється за допомогою технічних засобів та спеціальних інформаційних технологій.

Таким чином, робота покликана розкрити ролі і місця технічних засобів та інформаційних, які використовуються в розвідувальній діяльності.

Виклад основного матеріалу. Розвідка є важливою складовою забезпечення безпеки держави та захисту її національних інтересів у різних сферах. Ця безпека гарантується шляхом розвідувальної діяльності, яку здійснюють розвідувальні органи держави. У результаті розвідувальної діяльності розвідники отримують інформацію, зокрема:... «усні, зафіксовані на матеріальних носіях (у тому числі в зразках виробів і речовин) чи відображені в електронному вигляді відомості або дані». Ці дані можуть бути добуті як із відкритих джерел, так і нелегальним шляхом, в інтересах національної безпеки й оборони України. Для отримання розвідувальної інформації розвідувальні органи використовують різноманітні сили, засоби та методи [1, с. 26, 29].

Очевидно, що ефективність здобуття розвідувальної інформації залежить від методів та якості засобів, які використовує розвідка у своїй роботі. В сучасну епоху інформаційних технологій надзвичайно важливим методом добування розвідувальної інформації стала технічна розвідка, тобто здобуття інформації за допомогою технічних засобів розвідки.

В Україні, як у державі з розвиненою системою розвідки та відповідними традиціями, значна увага приділяється впровадженню технічних засобів для забезпечення розвідувальної діяльності, а також законодавчому врегулюванню питань, пов'язаних із технічною розвідкою та її засобами.

Згідно з наказом СБУ від 14.01.2021 «Про затвердження Зводу відомостей, що становлять державну таємницю», технічну розвідку слід розуміти як:... «несанкціоноване здобування секретної інформації за допомогою технічних засобів та її аналіз» [2].

У цьому ж наказі визначено, що можна вважати засобами технічної розвідки:...« апарати, машини та виготовлені з їх використанням обладнання або технічні системи, а також інструменти і речовини, призначені для: одержання розвідувальної інформації шляхом контролю поверхні Землі, повітряного (космічного) простору й окремих об'єктів, а також випромінювано акустичної апаратури, добування розвідувальної інформації з каналів електрозв'язку, інформаційних систем та окремих технічних засобів оброблення інформації; подолання технічного і криптографічного захисту розвідувальної інформації; негласного спостереження за об'єктами, що становлять інтерес для розвідувальних органів як джерела розвідувальної інформації; забезпечення передавання розвідувальної інформації» [2].

Багато положень щодо технічних засобів можна знайти в Законі України «Про розвідку». Так, у частині 8 статті 1 визначено, що до сил і засобів розвідки, серед іншого, слід включати технічні засоби розвідки.

У частині 13 цієї ж статті технічні засоби розвідки визначено як:... «технічні засоби, устаткування, апаратуру, прилади, пристрої, препарати та інші вироби, спеціально розроблені, створені, запрограмовані, придбані, модернізовані, пристосовані і призначені для здійснення та забезпечення розвідувальної діяльності».

У статті 9 закону зазначено, що суб'єкти системи воєнної розвідки виключно для виконання покладених на них завдань можуть застосовувати технічні засоби розвідки.

Важливими є положення щодо прав розвідувальних органів на використання технічних засобів розвідки. Так, у частині 10 статті 12 зазначено, що розвідка має право «здійснювати опитування осіб, у тому числі з використанням технічних засобів реєстрації реакцій людини».

У частині 15 цієї ж статті вказується право на вживання заходів щодо «технічного, криптографічного та інших видів захисту інформації, протидії технічним розвідкам».

Для ефективної роботи розвідувальні органи можуть виступати замовниками науково-дослідних, дослідно-конструкторських та інших робіт, зокрема з розроблення і виготовлення технічних засобів розвідки (стаття 19). Також вони мають право створювати, закуповувати, програмувати, модернізувати, пристосовувати і застосовувати технічні засоби розвідки (стаття 20).

У пункті 5 ст. 49 зазначено, що ці технічні засоби розвідки розробляються, створюються,

програмуються, придбаваються, модернізуються та пристосовуються виключно розвідувальними органами або на їх замовлення. Водночас вони залишаються у власності держави та закріплюються на праві оперативного управління за цими органами. Проте в окремих випадках, передбачених законом, розвідувальні органи можуть тимчасово передавати ці засоби іншим суб'єктам.

Важливими у наш час є положення ст. 27, а саме пункту 1, згідно з цим пунктом, суб'єкти системи воєнної розвідки мають право застосовувати технічні засоби розвідки без дотримання вимог статті 15 цього Закону. Це означає, що на відміну від звичайного режиму, коли проведення розвідувальних заходів стосовно особи, місця або речі, що перебувають на території України, потребує рішення суду, під час воєнного стану та бойових дій такі заходи можуть здійснюватися без відповідного судового дозволу з використанням технічних та інших засобів розвідки. А в 3 частині цієї статті вказано, що: «... в умовах, передбачених частиною першою цієї статті, на тимчасово окупованій території або території, де органи державної влади тимчасово не здійснюють свої повноваження, у районах бойових дій та зонах безпеки, прилеглих до цих районів, для виконання розвідувальних завдань та під оперативним контролем розвідувальних органів особи, залучені до конфіденційного співробітництва, можуть зберігати та застосовувати технічні та інші засоби розвідки» [3].

Тепер, коли ми розібралися із законодавчими положеннями щодо технічної розвідки та технічних засобів розвідки, можна перейти до історії їхнього використання українськими розвідувальними органами.

Перший випадок застосування технічних засобів розвідки українськими спецслужбами зафіксовано під час Української революції 1917–1921 років.

Так, у 1918 році на будівлі Першого генерал – квартирмейстерства, у будівлі якої розташовувався розвідувальний відділ, була встановлена потужна радіостанція, що працювала на прийом і передачу сигналу. За часів правління гетьмана Павла Скоропадського цю радіостанцію обслуговували й використовували фахівці з Миколаївської спеціальної школи, яка за часів царату готувала персонал для станцій радіоперехоплення російської армії [4, 5, арк. 35].

Відомо, що за часів Директорії при Агентурному відділі розвідувальної управи отримували інформацію про дислокацію та загальний стан військ Червоної армії, збройних формувань генерала Врангеля та отамана Нестора Махна. Джерелами даних були агентурні повідомлення, польова розвідка, радіоперехоплення та матеріали преси [4].

Після відступу Директорії до Польщі та створення Повстансько –партизанського штабу УНР при ньому було організовано ІІ-й (розвідувальний) відділ. Його агенти проходили спеціальні курси підготовки старшин-керівників технічних секцій при ІІ відділі (зокрема, навчалися роботі з фотографією, радіорозвідкою тощо) [6, с. 657–658].

Крім того, технічні засоби розвідки використовували й інші борці за незалежність України. Зокрема, підрозділи ОУН-УПА застосовували примітивні технічні засоби для перехоплення радіотелефонних переговорів ворогів [7, с. 256].

В часи незалежної України технічною розвідкою займалися вже національні розвідувальні органи. Після розпаду Радянського Союзу на території України залишилося два об'єкти стратегічної радіорозвідки Спеціальної служби КДБ СРСР (16 управління): 8-й окремий радіовузол та 9-й окремий радіовузол.

У 1992 році ці частини радіоперехоплення були введені до структури Служби безпеки України, а їхній особовий склад прийняв присягу. Також у структуру СБУ влився підрозділ Спеціальної служби ГРУ Генерального штабу Збройних Сил СРСР, а саме 85-й Головний центр, який займався обробкою матеріалів шифролистування [8, с. 295–297].

Того ж 1992 року голова СБУ підписав наказ про створення **У**правління «Р» у складі Головного управління контррозвідки СБУ. Цей підрозділ спеціалізувався на радіоелектронній розвідці та контррозвідці [8, с. 297].

Хоча новостворені підрозділи на перших порах існували в надзвичайно скрутних умовах, вони все ж не поступалися аналогічним структурам інших держав. Наприклад, вже у 1993 році Управління «Р» забезпечувало майже 50% усіх інформаційних матеріалів, що надходили до СБУ [8, с. 300].

Уже в грудні 1993 року управління стало самостійним підрозділом СБУ, однак лише у вересні 1999 року отримало статус Головного управління. Саме з цього моменту розпочалася планомірна побудова єдиного технологічного комплексу радіоелектронної розвідки, який охоплював такі види технічної розвідки: радіоперехоплення, технічний аналіз та дешифрування.

Також було намічено курс на розмежування розвідувальних та правоохоронних функцій у сфері перехоплення телекомунікацій. У зв'язку з цим від стратегічної зовнішньої розвідки було відокремлено такі підрозділи, як радіоконтррозвідка та моніторинг внутрішніх телекомунікацій [8, с. 301].

На початку 2000-х років управління продовжило активно розвивати методи та технології технічної розвідки, зробивши значні прориви у сферах криптоаналізу та дешифрування. Саме в цей період намітилися тенденції до розвитку нових напрямів технологічної розвідки, зокрема комп'ютерної та видової космічної.

Тому, коли 14 жовтня 2004 року було підписано Указ Президента України «Про Службу зовнішньої розвідки України», підрозділ технічної розвідки зайняв своє почесне місце серед інших підрозділів СЗР [8, с. 302, 303, 308].

Сучасний етап розвитку технологічної розвідки розпочався після подій 2014 року, коли українські розвідувальні органи виявили повну безпорадність перед діями Росії. Зрозуміло, що за таких умов було намічено курс на зміну особового складу розвідувальних органів, а також постало питання про реформування СЗР відповідно до стандартів НАТО, які після розриву відносин із Росією стали головними союзниками України.

У липні 2018 року Президентом України було затверджено Концепцію реформування Служби зовнішньої розвідки України відповідно до стандартів НАТО. У рамках цієї концепції було проведено кластеризацію та виокремлення окремих організаційно-практичних блоків, серед яких блок технічної розвідки [8, с. 315, 323].

Окрім змін у особовому складі та структурі, зазнали трансформацій і методи ведення розвідки. Українські розвідники мали адаптуватися до реалій гібридної війни з Росією, що зумовило зростання ролі розвідки за відкритими джерелами (OSINT) та геопросторової розвідки (GEOINT).

Під поняттям геопросторова розвідка можна розуміти безперервний процес збору, обробки та аналізу геопросторової інформації, який використовується для опису, оцінки, візуального відображення об'єктів, процесів і явищ, а також для прогнозування їх змін. Основна мета геопросторової розвідки – забезпечення національної безпеки та оборони й забезпечення керівництво країни актуальною інформацією. Такий спосіб розвідки з використання технічних засобів дозволяє здобувати такі дані: супутникові та аерофотознімки (панхроматичні, інфрачервоні, гіперспектральні, радіолокаційні знімки територій), розташування джерел випромінювання (аналітика щодо місць радіочастотної активності), динаміку руху об'єктів (переміщення техніки, кораблів, військових підрозділів тощо), тривимірні моделі об'єктів (реконструкція місцевості, будівель, військових баз) [9, с. 54–55].

В Україні з 2014 року активно приділяється увага збору інформації за допомогою геопросторової розвідки. Про важливість цього напряму та перспективи використання краудсорсингових систем писали фахівці ВІКНУ ще у 2016 році. Зокрема, вони пропонували передати на краудсорсинг виявлення конкретних однакових ознак у певному місці, що гарантувало б, що виявлена інформація є цінною для розвідки [10, с. 161].

Вже під час повномасштабної війни українська влада та армія на постійній основі почали співпрацювати із західними партнерами для ведення геопросторової розвідки. Так, на комерційній основі Україна отримувала супутникові знімки зі супутників SAR-LUPE, які перебувають у власності німецької компанії Kayser-Threde GmbH. Ця компанія є структурним підрозділом OHB-System AG, а замовником на створення системи SAR-LUPE виступило космічне агентство Німеччини (DLR) [11, с. 200].

У 2022 році Міністерство оборони України почало співпрацювати із супутниковим оператором SAR ICEYE. У серпні 2022 року компанія уклала контракт із Благодійним фондом Сергія Притули, надавши Україні доступ до супутникових знімків. Крім того, ICEYE дозволила Збройним Силам України використовувати свою мережу супутників для збору критично важливих даних. У липні 2024 року компанія підписала новий договір із Міністерством оборони України, спрямований на посилення космічної оборони країни. А у вересні того ж року німецький оборонний концерн Rheinmetall розпочав співпрацю із SAR ICEYE, щоб підтримати Україну в рамках оборонних ініціатив [12].

Щодо розвідки за відкритими джерелами, то вона стала доволі актуальною з 2014 року у зв'язку з характером гібридної війни та розвитком інформаційних технологій.

Загалом, розвідка за відкритими джерелами, або OSINT (від англійського open-source intelligence), є методом пошуку, збору, відбору та аналізу інформації, яка становить оперативний інтерес, з відкритих джерел. У сучасних

умовах методи збору інформації за відкритими джерелами базуються на використанні технічних засобів, здебільшого комп'ютерів, хоча можуть застосовуватися також телефони чи інші електронні пристрої з доступом до Інтернету, а також засоби для перехоплення незашифрованих радіохвиль і мобільного зв'язку.

Цей вид розвідки зазвичай використовується у конкурентній розвідці, коли компанії намагаються дізнатися більше про своїх конкурентів або партнерів. Однак у сучасному світі, де більшість інформації можна отримати легальним або відносно легальним шляхом через Інтернет, OSINT стала потужним інструментом у руках розвідувальних органів. Наприклад, американські розвідувальні служби отримують із відкритих джерел від 35% до 95% розвідувальних даних [13, с. 761–762].

Зараз російська розвідка використовує методи розвідки за відкритими джерелами для збору інформації про розташування українських військ та результати своїх обстрілів. Для цього їхні спецслужби активно моніторять соціальні мережі, групи у месенджерах та різні інтернет-ресурси з метою виявлення необхідної інформації. Їхні співробітники можуть навіть за допомогою діалогу в чаті спонукати громадян України до ненавмисного розголошення важливих даних ворогу.

Однак українські спецслужби також активно використовують методи OSINT. Взагалі, історія використання таких методів у вітчизняній розвідці сягає 20-х років минулого століття. Відомо, що розвідники часів Української революції 1917–1921 років часто отримували інформацію з відкритих джерел, таких як газети, журнали, спеціалізована періодична література тощо [4].

Також відомо, що розвідкою за відкритими джерелами з використанням технічних засобів займалися українські націоналісти. Так, на VI конференції ЗЧ ОУН(б) у травні 1953 року було визначено основне коло розвідувальних завдань, серед яких можна виділити збір інформації про Україну шляхом обробки радіоповідомлень, радянської та зарубіжної преси [14, с. 140].

З 2014 року українські розвідувальні органи активно використовують методи OSINT для збору інформації про російські війська, які брали участь у боях у зоні АТО на стороні сепаратистів. Завдяки моніторингу інтернет-ресурсів розвідка отримувала особисту інформацію про бойовиків та їхніх командирів, що допомагало у ідентифікації підрозділів і частин РФ, що воюють проти України на Донбасі. До речі цю інформацію на основі даних OSINT-розвідки представили волонтери команди InformNapalm [15, с. 83].

Треба зазначити, що використання підрядників для ведення розвідки за відкритими джерелами є доволі поширеною та перспективною практикою. Наприклад, у 2009 році розвідувальні органи США витрачали понад 70% бюджету на оплату роботи «підрядників», а ЦРУ – близько 30%. Такі приватні розвідувальні компанії є більш мобільними та ефективними, особливо у питанні збору легальної інформації за допомогою технічних засобів.

Одним із прикладів такої компанії є приватна розвідувальна компанія Terrogence, яка вже майже 20 років займається пошуком і аналізом критично важливої розвідувальної інформації. Вона використовує передові технологічні рішення, зокрема власну систему Web-Intelligence, яка здатна отримувати глибокі дані з онлайн-мереж і форумів. Особливу увагу компанія приділяє тим цифровим просторам, де можуть виникати та розвиватися потенційні загрози. Основними клієнтами Terrogence є державні установи, правоохоронні органи та служби національної безпеки різних країн, а також великі міжнародні корпорації, фінансові інститути та компанії, що працюють у сфері критичної інфраструктури [16, с. 178–180].

В Україні вже діють десятки організацій та ресурсів, які займаються збором інформації та протидією ворожій пропаганді. Серед них можна виділити кілька важливих проєктів: *InformNapalm*, які описаного вище, також змогли довести невідповідність статистики втрат ЗС РФ станом на 24.03.2022, або Bellingcat, доповідь яких пролила світло на причетність Москви до збиття літака МН17.

Окрім цього, функціонують:

– Dokaz – платформа, яка публікує докази присутності російських військових на сході України, а також матеріали щодо злочинів терористів та окупантів на Донбасі;

– СтопТерор – проєкт, який візуалізує бойові дії в Україні на інтерактивній карті та надає інформацію про незаконні збройні формування й кадрових військових РФ;

– Центр «Миротворець» – організація, що займається дослідженням ознак злочинів проти національної безпеки України, світу, безпеки людства та міжнародного правопорядку.

Крім того, з 2019 року в Україні почала діяти власна OSINT-агенція Molfar, яка проводить

розслідування як на національному, так і на міжнародному рівнях для розкриття та документування воєнних злочинів Росії у війні проти України [13, с. 762; 15, с. 83].

Таким чином, звичайний комп'ютер із доступом до Інтернету, при використанні методів OSINT, навіть у руках працівника приватної компанії, може стати справжнім технічним засобом розвідки. За його допомогою можна збирати дані як про пересування, плани та операції, так і про звірства ворожих військ. Саме завдяки цьому цей вид збору розвідувальної інформації з використанням технічних засобів є надзвичайно перспективним для подальшого розвитку. Це, до речі, добре усвідомлюють як у керівництві нашої країни, так і науковці, тому дедалі більше уваги приділяється використанню штучного інтелекту (ШІ) у сфері розвідки.

ШІ можна застосовувати для аналізу фото та відеоматеріалів з метою виявлення російських військових цілей. Взагалі, в українській армії давно зрозуміли переваги штучного інтелекту, а на його основі навіть створили власну систему розвідки, яка займається збором розвідувальних даних із різних джерел. Від внесення інформації в систему до її отримання проходить лише 28 секунд [17].

Перспективним є використання ШІ при веденні геопросторової розвідки, що підтверджується міжнародним досвідом. Штучний інтелект здатний аналізувати величезні обсяги даних і приймати швидкі та точні рішення в реальному часі. Наприклад, ШІ може обробляти аерофотознімки та відео з БПЛА або літаків, а потім коригувати вогонь артилерії по виявленій позиції противника [18, с. 136–137].

Висновки. Використання технічних засобів у розвідувальній діяльності відіграє ключову роль у забезпеченні національної безпеки та оборони держави. Аналіз законодавчої бази України свідчить про те, що технічна розвідка є невід'ємним елементом загальної системи збору розвідувальних даних. Вона охоплює широкий спектр засобів та методів, включаючи радіоелектронну, геопросторову, розвідку за відкритими джерелами та інші види розвідки.

Історичний аналіз розвитку технічної розвідки в Україні демонструє, що цей напрям почав використовуватися з часів Української революції 1917–1921 років, проходив трансформацію в період незалежності та зазнав суттєвих реформ після 2014 року. Особливе значення мали інтеграція вітчизняної розвідки в міжнародні системи обміну даними та співпраця з західними партнерами й приватними організаціями у сфері супутникового моніторингу та OSINT-досліджень.

Сучасний розвиток технологічної розвідки орієнтований на використання передових цифрових технологій. OSINT та геопросторова розвідка стали ключовими інструментами у боротьбі з сучасними викликами гібридної та під час повномасштабної війни з Росією. Завдяки поєднанню даних з різних джерел, включаючи супутникові знімки, аналіз цифрових комунікацій, українська розвідка отримує потужний інструментарій для швидкого реагування та прийняття рішень.

Окрему увагу слід приділити ролі штучного інтелекту (ШІ) в розвідувальній діяльності. Його можливості щодо автоматизації аналізу великих масивів інформації, ідентифікації об'єктів на знімках та прогнозування дій противника відкривають нові перспективи для покращення ефективності розвідки. Уже сьогодні українські збройні сили використовують ШІ для аналізу даних з супутникових знімків та перехоплених повідомлень, що значно підвищує точність і швидкість ухвалення рішень на полі бою.

Перспективами подальшого дослідження є питання інтеграції штучного інтелекту в аналіз розвідувальних даних, бо подальший розвиток технологій машинного навчання та комп'ютерного зору може суттєво покращити можливості української розвідки. Також дослідження методів автоматизованої ідентифікації цілей та аналізу супутникових знімків допоможе підвищити точність розвідувальних оцінок.

Таким чином, розвиток технічної розвідки має ключове значення для підвищення обороноздатності України в умовах сучасної війни. Впровадження передових технологій, інтеграція ШІ та розширення OSINT-можливостей допоможуть забезпечити ефективний збір та аналіз інформації для ухвалення стратегічних і тактичних рішень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Сервецький І. Розвідувальні органи: їх роль і місце у забезпеченні національної безпеки України. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*, 2022. 1 (59), 25–31. https://doi.org/10.32689/2522-4603.2020.1.4
2. СБУ, Наказ «Про затвердження Зводу відомостей, що становлять державну таємницю» від 23.12.2020 N 383
3. Верховна Рада України. Закон України «Про розвідку» №2396-VIII, 2020. URL: https://zakon.rada.gov.ua/laws/show/2396-19#Text.

4. Сідак В. С. Національні спецслужби в боротьбі за державність України (1917–1921 рр.) : дис. ... д-ра істор. наук : 21.00.04. К., 1998. 441 с.
5. ЦДАВО України, ф. 1074., оп.2., спр 37., арк. 35.
6. Бібліотека Народова в Варшаві, спр. 68867., арк. 293–303
7. Вєдєнєєв, Дмитро Валерійович. Меч і тризуб. Розвідка і контррозвідка руху українських націоналістів та УПА. 1920-1945 / Д. В. Вєдєнєєв, Г. С. Биструхін. Київ: Генеза, 2006. 408 с. : іл. (Таємні війни: історія та сучасність).
8. Скрипник О. В. Українська розвідка: 100 років боротьби, протистоянь, звершень. ADEF-Ukraïna, 2020. 344 с.
9. Подліпаєв В. О. «Геопросторова розвідка, як шлях реалізації геоінформаційного підходу у комплексній обробці розвідувальної інформації.» Системи обробки інформації 5 (2013): 53–55.
10. Жиров Г., Кольцов Р., Шмиголь Є. Геопросторова розвівдка з використанням геоіффрормаційних та краудосонгових систем. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*, 2016. (51), 159–163.
11. Коломійцев О. В., Пустоваров В. В., Катунін А. М., Бердочник А. Д., Беспалько О. В. Використання цифрових фотознімків SAR-супутників у розвідувальній діяльності та їх обробка на основі використання інформаційних технологій. 2023.
12. Rheinmetall та ICEYE надають Україні супутникові знімки. Суспільне Новини. 2024. URL: https://suspilne.media/877793-rheinmetall-ta-iceye-nadaut-ukraini-suputnikovi-znimki/.
13. Уфімцева О. С. Використання OSINT в умовах збройної агресії РФ проти України. Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття» (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 761–763.
14. Вєдєнєєв Д. В., Лисенко О. Є. Організація українських націоналістів і зарубіжні спецслужби (1920-1950-ті рр.). 2009.
15. Мигько О. В., et al. Використання технологій OSINT для отримання розвідувальної інформації. *Системи управління, навігації та зв'язку*, 2016. 4, 81–84.
16. Кудінов С. Міжнародний досвід партнерства приватних компаній та спеціальних служб в інтересах забезпечення національної безпеки та його значення для України. *Інформація і право*, 2024. 3 (50), 176–181.
17. В Україні на базі штучного інтелекту розробили систему розвідки. Мілітарний. 2024. URL: https://mil.in.ua/uk/news/v-ukrayini-na-bazi-shtuchnogo-intelektu-rozrobyly-systemu-rozvidky/
18. BORISOV O. V. Роль нейромережі у військовій розвідці та бойових діях. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*, 2023. 50, 136–141.

REFERENCES:

1. Servetskyi, I. (2022). Rozviduvalni orhany: yikh rol i mistse u zabezpechenni natsionalnoi bezpeky Ukrainy [Intelligence agencies: their role and place in ensuring the national security of Ukraine]. *Naukovi pratsi Mizhrehionalnoi Akademii upravlinnia personalom. Yurydychni nauky*, 1 (59), 25–31. https://doi.org/10.32689/2522-4603.2020.1.4
2. SBU, Nakaz „Pro zatverdzhennia Zvodu vidomostei, shcho stanovliat derzhavnu taiemnytsiu" [SBU, Order „On approval of the Collection of information constituting a state secret"] vid 23.12.2020 N 383
3. Verkhovna Rada Ukrainy. Zakon Ukrainy "Pro rozvidku" [Verkhovna Rada of Ukraine. Law of Ukraine "On Intelligence"] №2396-VIII, 2020. Retrieved from: https://zakon.rada.gov.ua/laws/show/2396-19#Text.
4. Sidak, V. S. (1998). Natsionalni spetssluzhby v borotbi za derzhavnist Ukrainy (1917–1921 rr.) [National special services in the struggle for the statehood of Ukraine (1917–1921)] : dys. ... d-ra istor. nauk : 21.00.04. K., 441 s.
5. TsDAVO Ukrainy [Central State Security Service of Ukraine], f. 1074., op.2., spr 37., ark. 35.
6. Biblioteka Narodova v Varshavi [Narodowa Library in Warsaw], spr. 68867., ark. 293–303
7. Viedienieiev, Dmytro Valeriiovych. (2006). Mech i tryzub. Rozvidka i kontrrozvidka rukhu ukrainskykh natsionalistiv ta UPA [Sword and Trident. Intelligence and counterintelligence of the Ukrainian nationalist movement and the UPA]. 1920–1945. D. V. Viedienieiev, H. S. Bystrukhin. Kyiv: Heneza, 408 c. : il. (Taiemni viiny: istoriia ta suchasnist).
8. Skrypnyk, O. V. (2020). Ukrainska rozvidka: 100 rokiv borotby, protystoian, zvershen [Ukrainian intelligence: 100 years of struggle, confrontation, achievements]. ADEF-Ukraïna, 344 s.
9. Podlipaiev, V. O. (2013). "Heoprostorova rozvidka, yak shliakh realizatsii heoinformatsiinoho pidkhodu u kompleksnii obrobtsi rozviduvalnoi informatsii ["Geospatial intelligence as a way to implement a geoinformation approach in the complex processing of intelligence information]." *Systemy obrobky informatsii*. 5, 53–55.
10. Zhyrov, H., Koltsov, R., Shmyhol, Ye. (2016). Heoprostorova rozvivdka z vykorystanniam heoifrormatsiinykh ta kraudosonhovykh system [Geospatial intelligence using geoinformation and crowdsourcing systems]. *Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka,* (51), 159–163.
11. Kolomiitsev, O. V., Pustovarov, V. V., Katunin, A. M., Berdochnyk, A. D., Bespalko, O. V. (2023). Vykorystannia tsyfrovykh fotoznimkiv SAR-suputnykiv u rozviduvalnii diialnosti ta yikh

obrobka na osnovi vykorystannia informatsiinykh tekhnolohii [Use of digital SAR satellite images in reconnaissance activities and their processing based on the use of information technologies].
12. Rheinmetall ta ICEYE nadaiut Ukraini suputnykovi znimky [Rheinmetall and ICEYE provide Ukraine with satellite images]. Suspilne Novyny. 2024. Retrieved from: https://suspilne.media/877793-rheinmetall-ta-iceye-nadaut-ukraini-suputnikovi-znimki/.
13. Ufimtseva, O. S. (2022). Vykorystannia OSINT v umovakh zbroinoi ahresii RF proty Ukrainy [The use of OSINT in the context of the armed aggression of the Russian Federation against Ukraine]. Yevropeiskyi vybir Ukrainy, rozvytok nauky ta natsionalna bezpeka v realiiakh masshtabnoi viiskovoi ahresii ta hlobalnykh vyklykiv KhKhI stolittia" (do 25-richchia Natsionalnoho universytetu "Odeska yurydychna akademiia" ta 175-richchia Odeskoi shkoly prava) : u 2 t. : materialy Mizhnar.nauk.-prakt. konf. (m. Odesa, 17 chervnia 2022 r.) / za zahalnoiu redaktsiieiu S. V. Kivalova. Odesa : Vydavnychyi dim "Helvetyka", T. 1. S. 761–763.
14. Viedieneiev, D. V., Lysenko, O. Ye. (2009). Orhanizatsiia ukrainskykh natsionalistiv i zarubizhni spetssluzhby (1920-1950-ti rr.) [The organization of Ukrainian nationalists and foreign intelligence services (1920–1950s)].
15. Myhko, O. V., et al. (2016). Vykorystannia tekhnolohii OSINT dlia otrymannia rozviduvalnoi informatsii [The use of OSINT technologies to obtain intelligence information]. *Systemy upravlinnia, navihatsii ta zviazku*, 4, 81–84.
16. Kudinov, S. (2024). Mizhnarodnyi dosvid partnerstva pryvatnykh kompanii ta spetsialnykh sluzhb v interesakh zabezpechennia natsionalnoi bezpeky ta yoho znachennia dlia Ukrainy [International experience of partnership between private companies and special services in the interests of ensuring national security and its significance for Ukraine]. *Informatsiia i pravo*, 3 (50), 176–181.
17. V Ukraini na bazi shtuchnoho intelektu rozrobyly systemu rozvidky [In Ukraine, an intelligence system was developed based on artificial intelligence]. Militarnyi. 2024. Retrieved from: https://mil.in.ua/uk/news/v-ukrayini-na-bazi-shtuchnogo-intelektu-rozrobyly-systemu-rozvidky/
18. BORISOV, O. V. (2023). Rol neiromerezhi u viiskovii rozvidtsi ta boiovykh diiakh [The role of neural networks in military intelligence and combat operations]. *COMPUTER-INTEGRATED TECHNOLOGIES: EDUCATION, SCIENCE, PRODUCTION*, 50, 136–141.

Дата надходження статті: 20.06.2025
Дата прийняття статті: 20.07.2025
Опубліковано: 10.10.2025