МЕТОДИ РОЗВІДУВАЛЬНОЇ ТА КОНТРРОЗВІДУВАЛЬНОЇ ДІЯЛЬНОСТІ В УМОВАХ СУЧАСНОСТІ

METHODS OF INTELLIGENCE AND COUNTER-INTELLIGENCE ACTIVITIES IN MODERN CONDITIONS

УДК 355.404.52:351.746.1(477)
DOI https://doi.org/10.32782/pma2663-5240-2024.39.54

Качмар Б.М.
к. юрид. н.,
доцент кафедри управління фінансово-економічною безпекою
Інститут безпеки ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом»

Тимошенко О.О.
к. екон. н.,
директор
Фінансова компанія «Онлайн Фінанс»

Стаття присвячена дослідженню сучасних методів розвідувальної та контррозвідувальної діяльності в контексті сучасних глобальних безпекових викликів. Актуальність теми підкреслюється стрімким технологічним прогресом та зростанням складності таких загроз, як кібершпигунство, гібридна війна та транснаціональна злочинність. Дослідження окреслює трансформаційний вплив інновацій, таких як штучний інтелект, аналіз великих даних та геопросторовий інтелект, на практику розвідки, а також критично важливу роль традиційних підходів, таких як людський інтелект.

Розглянуто різні аспекти розвідувальної діяльності, в тому числі застосування предиктивної аналітики на основі штучного інтелекту для виявлення загроз, супутникових знімків для геопросторового аналізу і систем великих даних для виявлення закономірностей у великих масивах даних. У дослідженні також розглянуто методи контррозвідки, спрямовані на нейтралізацію дій супротивника, такі як передові протоколи кібербезпеки, процеси перевірки персоналу та заходи з протидії дезінформаційним кампаніям. Особлива увага присвячена взаємодії між технологічними можливостями та людським досвідом, що ілюструє, як ці елементи поєднуються для підвищення ефективності сучасних розвідувальних і контррозвідувальних операцій.

Встановлено важливість етичних і правових міркувань у практиці розвідки і контррозвідки, особливо в демократичних суспільствах. Баланс між забезпеченням безпеки і підтримкою громадянських свобод підкреслюється як основний виклик у застосуванні цих методів. У дослідженні також визначено вирішальну роль міжнародного співробітництва та державно-приватного партнерства у зміцненні систем безпеки, особливо у сферах кібербезпеки та захисту критичної інфраструктури.

Обґрунтовано необхідність постійних досліджень нових технологій, таких як квантові обчислення і нейронні мережі, а також розробки адаптивних стратегій для протидії майбутнім загрозам. Висновки підкреслюють необхідність інтеграції міждисциплінарних підходів, що охоплюють право, технології, соціологію і міжнародні відносини, для створення всеосяжного фундаменту для майбутніх досліджень. Сприяючи співпраці між секторами і дисциплінами, дослідження відкриває шлях до підвищення ефективності і стійкості систем розвідки і контррозвідки у все більш взаємопов'язаному світі.

Ключові слова: *методи розвідки, контррозвідувальна діяльність, стратегії контррозвідки, штучний інтелект, великі дані, геопросторовий інтелект, заходи кібербезпеки, дезінформаційні кампанії, національна безпека, технологічний прогрес, глобальні виклики*

The article is devoted to the study of modern methods of intelligence and counterintelligence activities in the context of current global security challenges. The relevance of the topic is underlined by the rapid development of technological progress and the growing complexity of threats such as cyber espionage, hybrid warfare and transnational crime. The study outlines the transformative impact of innovations such as artificial intelligence, big data analysis and geospatial intelligence on intelligence practice, as well as the critical role of traditional approaches such as human intelligence.

It examines various aspects of intelligence activities, including the use of artificial intelligence-based predictive analytics for threat detection, satellite imagery for geospatial analysis, and big data systems for identifying patterns in large data sets. The study also examines counterintelligence methods aimed at neutralising adversary actions, such as advanced cybersecurity protocols, personnel vetting processes, and measures to counter disinformation campaigns. Particular attention is paid to the interaction between technological capabilities and human expertise, illustrating how these elements combine to enhance the effectiveness of modern intelligence and counterintelligence operations.

The importance of ethical and legal considerations in the practice of intelligence and counterintelligence, especially in democratic societies, is established. The balance between ensuring security and maintaining civil liberties is highlighted as a major challenge in the application of these methods. The study also identifies the crucial role of international cooperation and public-private partnerships in strengthening security systems, especially in the areas of cybersecurity and critical infrastructure protection.

The study also argues for continuous research into new technologies, such as quantum computing and neural networks, and the development of adaptive strategies to counter future threats. The conclusions highlight the need to integrate interdisciplinary approaches, encompassing law, technology, sociology and international relations, to create a comprehensive foundation for future research. By fostering collaboration across sectors and disciplines, the study paves the way for more effective and resilient intelligence and counterintelligence systems in an increasingly interconnected world.

Key words: *intelligence methods, counterintelligence activities, counterintelligence strategies, artificial intelligence, big data, geospatial intelligence, cybersecurity measures, disinformation campaigns, national security, technological progress, global challenges*

Актуальність теми дослідження. Актуальність дослідження методів розвідувальної та контррозвідувальної діяльності в сучасному світі обумовлена потребою забезпечення національної та глобальної безпеки. В епоху стрімкого технологічного прогресу,

геополітичної напруженості та зростаючої залежності від інформації, розвідка та контррозвідка стали незамінними інструментами для підтримки суверенітету, захисту критичної інфраструктури та протидії транснаціональним загрозам. Поширення цифрових технологій, зростання кібершпигунства і зростаюча витонченість державних і недержавних суб'єктів створили динамічне і складне середовище, яке вимагає постійних інновацій та адаптації розвідувальних практик.

Тема дослідження є особливо актуальною з огляду на зростаючу складність і динаміку глобальної безпеки. Поширення гібридної війни, яка поєднує традиційну військову тактику з кібероперaціями та дезінформаційними кампаніями, підкреслює необхідність створення надійних систем розвідки та контррозвідки. Крім того, етичні та правові аспекти цієї діяльності, особливо в демократичних суспільствах, зумовлюють необхідність вивчення того, як її можна проводити ефективно, не ставлячи під загрозу громадянські свободи.

Вивчаючи методи, що використовуються в розвідці і контррозвідці, дослідники можуть отримати уявлення про стратегії і технології, які лежать в основі цієї діяльності, а також про їхню ефективність і обмеження. Такі дослідження також сприяють розумінню того, як країни можуть збалансувати безпеку і конфіденційність, забезпечуючи відповідність розвідувальних практик міжнародним нормам і внутрішньому законодавству. У світі, який дедалі більше формується під впливом інформації, ця тема залишається на передньому краї академічних і практичних дискусій у галузі безпекових досліджень, що робить її своєчасною і важливою.

Метою дослідження є аналіз та оцінка методів розвідувальної та контррозвідувальної діяльності в сучасному світі, з акцентом на їх еволюції, застосуванні та ефективності у вирішенні сучасних безпекових викликів.

Аналіз останніх досліджень і публікацій. Аналіз досліджень і публікацій, присвячених методам розвідувальної та контррозвідувальної діяльності, свідчить про значну еволюцію підходів, зумовлену технологічним прогресом і зміною характеру глобальних загроз. Науковці та практики підкреслюють вирішальну роль інтеграції традиційних практик з інноваційними технологіями, такими як штучний інтелект, аналіз великих даних та геопросторовий інтелект (Fox S., Лукіянчук А., Мірошніченко О., Mackdo A., Peotta L., Gomes F., Гуцало М., Буряченко Є. В., Пашковський М. І., Павлиш Т. Г., Терещенко О. О., Легомінова С., Щавінський Ю., Рабчун Д., Запорожченко М., Будзинський О., Назаров О. А., Бондаренко С. Ю.). У літературі підкреслюється трансформаційний вплив цих досягнень на підвищення точності, швидкості і масштабу розвідувальних операцій. Дослідження також підкреслюють зростаючу залежність від заходів кібербезпеки, оскільки зусилля контррозвідки все більше зосереджуються на зменшенні ризиків, пов'язаних з кібершпигунством, інсайдерськими загрозами і кампаніями з дезінформації.

Основний зміст дослідження. Сучасні методи інтелекту зазнали значної трансформації завдяки технологічному прогресу, який покращує процеси збору, аналізу та прийняття рішень. Штучний інтелект став основою сучасного аналізу, уможливлюючи автоматизовану обробку даних, розпізнавання образів і предиктивну аналітику. Алгоритми ШІ можуть обробляти величезні обсяги інформації з різних джерел, виявляючи потенційні загрози з безпрецедентною швидкістю і точністю [1]. Зокрема, моделі машинного навчання застосовуються в боротьбі з тероризмом для аналізу контенту в соціальних мережах, виявлення екстремістських наративів і прогнозування ймовірності насильницьких дій.

Супутникові знімки також революціонізували збір розвідувальної інформації, надаючи геопросторові дані в реальному часі, які мають вирішальне значення для моніторингу військової діяльності, змін у навколишньому середовищі та розвитку інфраструктури [2]. Знімки високої роздільної здатності в поєднанні з аналізом зображень за допомогою штучного інтелекту дозволяють розвідувальним службам з надзвичайною точністю виявляти підозрілу діяльність, наприклад, пересування військ або незаконне будівництво. Під час військових конфліктів супутникові дані виявилися незамінними для картографування місцевості, оцінки збитків і координації зусиль з надання гуманітарної допомоги.

Поєднання цих технологій дозволяє проводити багатовимірні розвідувальні операції, інтегруючи людську розвідку HUMINT, розвідку сигналів SIGINT і розвідку з відкритих джерел OSINT в цілісні стратегії. OSINT, зокрема, використовує загальнодоступну інформацію із засобів масової інформації, форумів і наукових публікацій для покращення обізнаності про обстановку [3]. Покладання на технології у XXI столітті зумовило необхідність врахування етичних міркувань, особливо щодо приватності, оскільки розвідувальна діяльність перетинається з громадянськими свободами. Дані методи підкреслюють баланс між інноваціями і підзвітністю в розвідувальному ландшафті, що розвивається.

Головними дійовими особами в операціях HUMINT є агенти та інформатори, які надають унікальну інформацію, часто недоступну за допомогою технічних засобів. Люди діють у різних середовищах, від зон конфліктів до корпоративних структур, збираючи розвідувальну інформацію, яка формує стратегічні рішення і підвищує обізнаність про ситуацію.

Агенти, часто впроваджені в цільові організації або громади, відіграють важливу роль у здобутті чутливої інформації. Їх цінність полягає в здатності розуміти місцеву динаміку, інтерпретувати культурні нюанси та отримувати доступ до зон з обмеженим доступом або інформації. Такі оперативники необхідні в антитерористичних операціях, де розуміння ідеологічних мотивацій та організаційних структур вимагає безпосередньої взаємодії з особами, пов'язаними з екстремістськими угрупованнями [4]. З іншого боку, інформатори, як правило, є особами, які надають розвідувальну інформацію добровільно або під впливом певних стимулів, таких як фінансова компенсація або юридична поблажливість. Вони особливо ефективні в кримінальних розслідуваннях, пропонуючи інформацію з перших рук про незаконні мережі, в тому числі наркоторгівлю або організовані злочинні синдикати.

Значення полягає в його адаптивності і глибині. У дипломатичній розвідці агенти можуть взаємодіяти з іноземними офіційними особами, щоб зрозуміти політичні зміни, тоді як у військовому контексті інформатори надають критично важливі дані про пересування військ противника, укріплення або маршрути постачання [5]. Під час холодної війни дані операції відігравали ключову роль у виявленні шпигунської діяльності та здобутті секретної інформації від держав-суперників. Незважаючи на розвиток новітніх технологій спостереження, HUMINT зберігає свою актуальність завдяки здатності отримувати якісні розвідувальні дані, такі як наміри, лояльність і внутрішні конфлікти, які складно розпізнати лише за допомогою цифрових засобів.

Операції вимагають ретельного управління для зменшення ризиків, пов'язаних з вербуванням, навчанням і захистом агентів та інформаторів. Етичні дилеми, в тому числі маніпулювання вразливими особами, створюють значні проблеми, особливо в демократичних країнах, які наголошують на правах людини. Проте стратегічна інтеграція з іншими розвідувальними дисциплінами підвищує загальну ефективність розвідувальних операцій, гарантуючи, що людські знання доповнюють технологічні досягнення.

Однією з найбільш сучасних технологій в порівнянні з попередньою є технологія розвідки з відкритих джерел OSINT, що стала невід'ємним елементом сучасних розвідувальних операцій, використовуючи загальнодоступні дані для збору дієвої інформації в різних сферах. OSINT охоплює інформацію з різних джерел, в тому числі з новин, соціальних мереж, наукових публікацій, урядових звітів і загальнодоступних баз даних [6]. Її широке поширення зумовлене експоненціальним зростанням цифрової інформації та відносною легкістю доступу до таких даних, що робить її економічно вигідною та ефективною розвідувальною дисципліною.

Моніторинг соціальних мереж є важливим застосуванням, що дозволяє аналітикам відстежувати тенденції, оцінювати суспільні настрої і виявляти потенційні загрози. У контексті безпеки спецслужби використовують алгоритми для виявлення поширення дезінформації, відстеження діяльності екстремістських груп або моніторингу комунікацій, пов'язаних з незаконною діяльністю [7]. Аналітики з кібербезпеки часто сканують форуми і темні інтернет-майданчики на предмет ознак запланованих кібератак, витоків даних або продажу конфіденційної інформації. Урядові установи та приватні організації використовують ці методи, щоб передбачити ризики та вчасно вжити контрзаходів.

Також технології часто застосовуються у геополітичному аналізі, де загальнодоступні супутникові знімки, торговельна статистика та дипломатичні комунікації дають чіткіше розуміння міжнародних подій. Під час конфліктних ситуацій дослідники можуть використовувати супутникові знімки для моніторингу розгортання військ, оцінки пошкоджень інфраструктури або перевірки заяв конфліктуючих сторін. Фінансова розвідка, отримана за допомогою OSINT — відстеження глобальних торговельних потоків або аналіз корпоративної звітності, допомагає виявити економічні зловживання або порушення санкцій.

Незважаючи на свої переваги, OSINT стикається з такими проблемами, як достовірність даних, величезні обсяги інформації та етичні міркування, особливо щодо конфіденційності. Аналітики повинні відрізняти достовірні джерела від дезінформації і застосовувати методології, які поважають правові та етичні межі [8]. Як розвідувальна дисципліна, що розвивається, технологічний аспект демонструє можливості загальнодоступних даних у вирішенні складних проблем безпеки і прийнятті обґрунтованих рішень.

Сучасні методи контррозвідки зазнали значного розвитку, щоб протистояти зроста-

ючій складності загроз у взаємопов'язаному світі. Зростання кібершпигунства, інсайдерських загроз і дезінформаційних кампаній вимагає інноваційних підходів, що поєднують технології, людський контроль і стратегічні операції. Заходи з кібербезпеки, перевірка і відбір персоналу, а також спеціалізовані контррозвідувальні операції є наріжним каменем сучасних зусиль із захисту національної безпеки і організаційної цілісності.

Кібербезпека стала критично важливим аспектом контррозвідки, особливо в боротьбі з кібершпигунством. Державні та недержавні суб'єкти все частіше націлюються на конфіденційні урядові бази даних, корпоративну інтелектуальну власність та об'єкти критичної інфраструктури. Передові заходи кібербезпеки передбачають розгортання систем виявлення вторгнень, захисту кінцевих точок і протоколів шифрування для захисту конфіденційної інформації. Машинне навчання і штучний інтелект широко використовуються для виявлення незвичайної мережевої активності, виявлення сучасних постійних загроз і прогнозування потенційних вразливостей. Організації часто проводять тестування на проникнення, щоб імітувати атаки та оцінити свій захист. Платформи розвідки кіберзагроз збирають інформацію про відомих зловмисників та їхню тактику, допомагаючи організаціям передбачати та протидіяти спробам шпигунства.

Процеси відбору і перевірки персоналу є ще одним важливим компонентом сучасної контррозвідки. Для виявлення потенційних інсайдерських загроз використовуються комплексні перевірки, психологічні оцінки та постійний моніторинг. Процеси перевірки часто включають перевірку на поліграфі, фінансовий аудит і оцінку поведінки в соціальних мережах, щоб виявити вразливі місця, які можуть бути використані противником [9]. Програми безперервної оцінки використовують автоматизовані інструменти для моніторингу змін у поведінці працівників або обставин, таких як неочікувані фінансові труднощі або зміни в міжособистісних стосунках. Подібні заходи є вкрай необхідними в середовищі з доступом до секретної або конфіденційної інформації, оскільки інсайдери залишаються однією з найскладніших загроз, яким можна протидіяти.

Контррозвідувальні операції, спрямовані на дезінформаційні кампанії, стали особливо актуальними в цифрову епоху, коли соціальні мережі та онлайн-платформи посилюють вплив неправдивих наративів. Уряди та організації наймають команди для моніторингу, виявлення та протидії таким кампаніям, часто використовуючи інструменти аналізу даних та аналізу настроїв для відстеження походження та поширення дезінформації. Стратегічні комунікаційні кампанії та ініціативи з перевірки фактів використовуються для нейтралізації дезінформації, зберігаючи при цьому довіру громадськості [10]. Під час геополітичних конфліктів контррозвідувальні органи можуть використовувати стратегічні наративи, щоб заплутати супротивників або захистити секретні операції - практика, яка вимагає точності та координації, щоб уникнути правових та етичних пасток.

Інтеграція технологій і традиційних методів контррозвідки забезпечує багаторівневий захист від все більш витончених загроз. Співпраця між державним і приватним секторами відіграє життєво важливу роль у сучасній контррозвідці, особливо в захисті ланцюгів постачання, критичної інфраструктури і нових технологій, таких як штучний інтелект і квантові обчислення. Міжурядова співпраця також розширює можливості, оскільки угоди про обмін розвідувальною інформацією дають уявлення про спільні загрози і методології їх подолання.

Сучасні методи контррозвідки стикаються з викликами, в тому числі з етичними наслідками стеження, збереженням оперативної таємниці в цифрову епоху і управлінням зростаючою витонченістю супротивників. Незважаючи на ці перешкоди, розробка адаптивних та інноваційних стратегій гарантує, що зусилля контррозвідки залишатимуться надійними, проактивними та ефективними для захисту національної безпеки та організаційної стійкості. Оскільки ландшафт загроз продовжує розвиватися, інтеграція передових технологій з людським досвідом залишатиметься ключовим фактором успіху контррозвідувальних операцій. Дослідження з розвідки та контррозвідки створюють широке підґрунтя для розуміння практичного застосування, успіхів та викликів цих операцій. Вони ілюструють стратегічні, оперативні та технологічні аспекти захисту національної безпеки і протидії глобальним загрозам. Успішні розвідувальні операції і контррозвідувальні зусилля підкреслюють важливість ретельного планування, адаптивності і співпраці між відомствами і країнами.

Зовсім недавно зусилля контррозвідки у сфері кібербезпеки зірвали витончені шпигунські кампанії, націлені на урядові і корпоративні системи. Завдяки поєднанню технічної криміналістики, міжнародної співпраці і підтримки приватного сектору були виявлені і знешкоджені сучасні групи постійних загроз, пов'язані з національними державами.

В одному випадку багатонаціональні зусилля успішно ліквідували мережу кібершпигунства, націлену на оборонних підрядників і об'єкти критичної інфраструктури. Такі операції демонструють зростаючу роль кіберпотужностей в контррозвідці, де виявлення і пом'якшення загроз вимагає аналізу в режимі реального часу і транскордонної координації.

Висновки та перспективи подальших досліджень

Висновки дослідження методів розвідки та контррозвідки в сучасному світі підкреслюють їхню важливість у забезпеченні національної та глобальної безпеки. Технологічний прогрес значно трансформував традиційні підходи, впровадивши сучасні інструменти, такі як штучний інтелект, великі дані, кіберзахист та автоматизований аналіз відкритих джерел. Незважаючи на впровадження новітніх технологій, традиційні методи, зокрема людська розвідка, залишаються невід'ємною складовою ефективної системи безпеки, забезпечуючи доступ до якісної інформації, яка недоступна за допомогою технологічних засобів. Водночас, розвиток контррозвідки орієнтується на багаторівневий підхід, який охоплює захист від кіберзагроз, моніторинг внутрішніх ризиків та протидію дезінформаційним кампаніям.

Перспективи подальших досліджень охоплюють аналіз впливу новітніх технологій, таких як квантові обчислення та нейромережі, на діяльність розвідки та контррозвідки. Також необхідно глибше дослідити міжнародний досвід співпраці у протидії глобальним загрозам, включаючи кіберзлочинність та дезінформацію. Важливим напрямом є вивчення правових механізмів регулювання діяльності у сфері розвідки та контррозвідки, щоб адаптувати їх до сучасних реалій і забезпечити ефективність при збереженні демократичних принципів. Інтеграція міждисциплінарних підходів, що охоплюють право, інформаційні технології, соціологію та міжнародні відносини, дозволить створити більш цілісну наукову базу для розробки нових стратегій у сфері безпеки.

ЛІТЕРАТУРА:

1. Fox S. Domesticating artificial intelligence: Expanding human selfexpression through applications of artificial intelligence in presumption. *Journal of Consumer Culture.* 2016, Вип. 8, С. 55-72.

2. Лукіянчук А., Мірошніченко О. Застосування геоінформаційних систем для вирішення завдань навігаційного забезпечення військ. *Вісник Київського національного університету імені Тараса Шевченка*. 2022. №3(51). С. 85-87.

3. Macêdo A., Peotta L., Gomes F. A review of the intersection techniques on HUMINT and OSIN. *International Journal on Cybernetics & Informatics*. 2023. Vol. 12, No. 1. P. 53-57. URL: https://ijcionline.com/paper/12/12123ijci05.pdf

4. Гуцало М. Деякі теоретичні аспекти побудови сучасної антитерористичної парадигми. *Національний інститут стратегічних досліджень.* 2018. С. 155–163. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/hutsalo_deiaki-1.pdf

5. Буряченко Є. В. Дипломатична служба та її специфіка. Автореферат дисертації на здобуття наукового ступеня кандидата політичних наук. Київ: Київський національний університет імені Тараса Шевченка, 2005. 20 с. URL: https://ktpu.kpi.ua/wp-content/uploads/2015/06/Buryachenko_avtoreferat.pdf

6. Пашковський М. І. Особливості використання OSINT при документуванні та розслідуванні колабораційної діяльності. *Актуальні питання кримінально-правової кваліфікації, документування та розслідування колабораціонізму* : матеріали Всеукр. науково-практ. конф., м. Одеса, 21 лип. 2022 р. Одеса, 2022. С. 82–86. URL: https://www.academia.edu/83765676

7. Павлиш Т. Г., Терещенко О. О. Аналіз інформації із соціальних мереж під час розслідування та в ході протидії злочинам. *Українська поліцеїстика: теорія, законодавство, практика.* 2022. №1(3). С. 49–56. URL: https://policeyistika.dnuvs.in.ua/wp-content/uploads/2022/04/pavlish.pdf

8. Легомінова С., Щавінський Ю., Рабчун Д., Запорожченко М., Будзинський О. Небезпека інструментів OSINT та способи пом'якшення наслідків їх використання для організації. *Кібербезпека: освіта, наука, техніка.* 2024. №1(25). С. 294–303. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/630

9. Назаров О.А. Проблемні питання використання поліграфа в діяльності органів внутрішніх справ України щодо протидії злочинам. *Актуальні питання теорії та практики використання поліграфа* : збірка статей. за заг. ред. В. О. Шаповалова. К. : Освіта України, 2015. 220 с. (Серія: Бібліотека Колегії поліграфологів України), С 38-46.

10. Бондаренко С. Ю. Негативні наслідки та шляхи протидії дезінформації в соціальних мережах як масовому негативному явищу. *Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи: тези доп. учасників міжн. наук.-практ. конф.* (Анн-Арбор Харків, 12-13 груд. 2023 р.), 2023. С. 200-204. URL: https://doi.org/10.32782/PPSS.2023.