УДК 351.746.1:004.9(477):355.45
https://doi.org/10.33744/2663-6352/2026-1-19-152-162
https://orcid.org/0000-0003-2666-9696
Барабаш О. О.,
доктор юридичних наук, професор,
завідувач науково-дослідної лабораторії актуальних проблем правозастосовної та правоохоронної діяльності навчально-наукового інституту права та правоохоронної діяльності, голова Ради молодих вчених Львівського державного університету внутрішніх справ
м. Львів, Україна

https://orcid.org/0009-0004-2702-494X
Афтанасів В. М.,
здобувачка вищої освіти 4 курсу навчально-наукового інституту права та правоохоронної діяльності, співголова Наукового товариства студентів (курсантів, слухачів), аспірантів, докторантів і молодих вчених Львівського державного університету внутрішніх справ
м. Львів, Україна

ЄВРОІНТЕГРАЦІЙНІ ОРІЄНТИРИ ПІДГОТОВКИ ФАХІВЦІВ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ У СФЕРІ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

Анотація. *У статті здійснено науково-прикладний аналіз євроінтеграційних орієнтирів підготовки фахівців Служби безпеки України у сфері інформаційно-аналітичної діяльності в умовах воєнного стану. У світлі зміни безпекового середовища обґрунтовано зростання ролі аналітичного забезпечення як важливого елементу оперативно-службової та контррозвідувальної діяльності, що безпосередньо впливає на ефективність протидії гібридним загрозам, кіберопераціям та інформаційно-психологічним впливам.*

Авторами проаналізовано нормативно-правові засади функціонування системи національної безпеки України, зокрема у частині адаптації до стандартів НАТО, та окреслено їх значення для формування сучасної моделі аналітичної діяльності. Встановлено, що інформаційно-аналітична складова контррозвідки є самостійним інструментом виявлення, попередження та документування загроз державній безпеці, зокрема шляхом використання OSINT та алгоритмічної аналітики.

Окрему увагу приділено аналізу практичних аспектів аналітичної діяльності Служби безпеки України під час війни, зокрема випадкам виявлення колабораційних мереж, протидії диверсійно-розвідувальним групам та нейтралізації інформаційних операцій держави-агресора. Досліджено роль відкритих джерел інформації як переважаючого сегменту сучасної розвідки та обґрунтовано необхідність їх правової інституціоналізації у структурі доказової діяльності.

У статті також висвітлено значення міжнародного співробітництва, зокрема взаємодії з Європейським поліцейським офісом, у частині обміну аналітичною інформацією, застосування стандартів кримінального аналізу та забезпечення сумісності аналітичних процедур.

Крім того, обґрунтовано необхідність модернізації системи підготовки кадрів Служби безпеки України шляхом впровадження моделі аналітика подвійної компетентності, розвитку цифрових навичок, критичного мислення та здатності до роботи в умовах інформаційної невизначеності. Запропоновано практичні напрями покращення аналітичної діяльності, зокрема

впровадження «real-time» аналітики, створення аналітичних груп швидкого реагування та використання інструментів прогностичного аналізу.

Наприкінці зроблено висновок, що ефективність інформаційно-аналітичного забезпечення Служби безпеки України безпосередньо залежить від рівня інтеграції сучасних технологій, правового регулювання аналітичних процедур та відповідності підготовки кадрів євроатлантичним стандартам.

Ключові слова: *національна безпека; Служба безпеки України; інформаційно-аналітична діяльність; контррозвідувальне забезпечення; OSINT; оперативно-службова діяльність; євроінтеграція; стратегічна аналітика; кібербезпека; кадрове забезпечення; воєнний стан; інформаційні загрози.*

BARABASH O., AFTANASIV V. EUROPEAN INTEGRATION GUIDELINES FOR THE TRAINING OF SPECIALISTS OF THE SECURITY SERVICE OF UKRAINE IN THE FIELD OF INFORMATION AND ANALYTICAL ACTIVITY

Abstract. *This article presents a scientific and applied analysis of the European integration guidelines for training specialists of the Security Service of Ukraine in the field of information and analytical activities under martial law. In light of changes in the security environment, the growing role of analytical support as a crucial element of operational, service, and counterintelligence activities is substantiated, as it directly impacts the effectiveness of countering hybrid threats, cyber operations, and information-psychological influences.*

The authors analyze the legal and regulatory framework for the functioning of Ukraine's national security system, particularly regarding its adaptation to NATO standards, and outline its significance for shaping a modern model of analytical activities. It has been established that the information-analytical component of counterintelligence is an independent tool for identifying, preventing, and documenting threats to national security, particularly through the use of OSINT and algorithmic analytics.

Particular attention is paid to the analysis of the practical aspects of the Security Service of Ukraine's analytical activities during wartime, specifically cases involving the detection of collaborationist networks, countering sabotage and reconnaissance groups, and neutralizing the aggressor state's information operations. The role of open-source intelligence as the predominant segment of modern intelligence is examined, and the necessity of its legal institutionalization within the framework of evidentiary activities is substantiated.

The article also highlights the importance of international cooperation, particularly collaboration with the European Police Office, regarding the exchange of analytical information, the application of criminal analysis standards, and ensuring the compatibility of analytical procedures.

In addition, the necessity of modernizing the personnel training system of the Security Service of Ukraine is substantiated through the implementation of a dual-competence analyst model, the development of digital skills, critical thinking, and the ability to work in conditions of information uncertainty. Practical directions for improving analytical activities are proposed, including the implementation of real-time analytics, the creation of rapid-response analytical teams, and the use of predictive analysis tools.

In conclusion, it is noted that the effectiveness of the information and analytical support provided by the Security Service of Ukraine directly depends on the level of integration of modern technologies, the legal regulation of analytical procedures, and the alignment of personnel training with Euro-Atlantic standards.

Key words: *national security; Security Service of Ukraine; intelligence and analysis; counterintelligence support; OSINT; operational activities; European integration; strategic analysis; cybersecurity; personnel support; martial law; information threats.*

Постановка проблеми. Сьогодні безпекове середовище нашої держави позначене винятковою складністю та інтенсивністю загроз, які, з огляду на повномасштабну збройну агресію, стали системними та багатовимірними. За оприлюдненими офіційними даними, лише протягом 2022-2025 років Службою безпеки України (далі – СБУ) викрито тисячі осіб, причетних до колаборaційної діяльності та державної зради, при цьому значна частина таких правопорушень була виявлена саме завдяки інформаційно-аналітичній роботі [1]. В той же час, як свідчать відкриті звіти Державної служби спеціального зв'язку та захисту інформації України, кількість кібератак на державні інформаційні ресурси та об'єкти критичної інфраструктури зросла у декілька разів, а у пікові періоди енергетичної кризи фіксувалися сотні інцидентів щомісяця. Прикметно, що понад 70% таких атак супроводжувалися інформаційно-психологічними операціями, які мали на меті дестабілізацію суспільних настроїв [2], що, власне кажучи, засвідчує нерозривність кібернетичного та когнітивного вимірів теперішньої війни.

Зважаючи на вищевикладене, вагоме значення має саме здатність держави до оперативного опрацювання великих масивів інформації, їх інтерпретації та трансформації у юридично значущі рішення. До слова, за оцінками фахівців у сфері безпеки, обсяг даних, що підлягає аналізу в рамках оперативно-службової діяльності, зріс у десятки разів порівняно з довоєнним періодом, що об'єктивно змінює вимоги до аналітичного апарату [3; 4]. Більше того, в умовах, коли кожен цифровий слід потенційно може містити розвідувальну цінність, інформаційно-аналітична діяльність є одним із центральних елементів забезпечення національної безпеки.

Звертаючись до нормативно-правового виміру, слід вказати, що Закон України «Про національну безпеку України» від 21.06.2018 р. №2469-VIII [5] та Стратегія національної безпеки України від 14.09.2020 р. №392/2020 [6] послідовно окреслюють курс на досягнення сумісності з євроатлантичними стандартами, що передбачає, зокрема, реформування системи підготовки кадрів сектору безпеки. Тим не менш, у цьому аспекті простежується певне протиріччя: попри наявність стратегічних орієнтирів, фактичний рівень підготовки фахівців у сфері інформаційно-аналітичної діяльності не завжди відповідає динаміці загроз. Як наголошувалося раніше у фахових дослідженнях, значна частина освітніх програм залишається орієнтованою на традиційні підходи до аналітики, що не враховують специфіку сучасної війни, де переважають кібероперації, інформаційні впливи та алгоритмічний аналіз даних [7, с. 57].

Цікаво, що у 2024-2025 роках, за даними профільних закладів вищої освіти системи МВС України, частка інформації, отриманої з відкритих джерел (зокрема, OSINT), у структурі аналітичних продуктів досягла понад 60%, що, без перебільшення, свідчить про зміну парадигми розвідувальної діяльності [8]. Так, на базі Львівського державного університету внутрішніх справ створена спеціалізована науково-дослідна лабораторія OSINT-досліджень та безпекової аналітики, діяльність якої зосереджена на підготовці здобувачів освіти до здійснення аналітичної обробки відкритих даних у безпековому секторі. В межах лабораторії відпрацьовуються навички цифрової розвідки, геолокаційного аналізу, верифікації мультимедійного контенту та ідентифікації інформаційних загроз у реальному часі. Принагідно зауважимо, що подібна інституціоналізація OSINT-підготовки безпосередньо корелює із запитами оперативно-службової діяльності, адже дозволяє формувати кадровий резерв аналітиків, здатних працювати в умовах високої інформаційної динаміки та невизначеності, що, власне кажучи, відповідає сучасним вимогам до інформаційно-аналітичного забезпечення національної безпеки. Ще генерал-лейтенант С. Вілсон, який очолював Розвідувальне управління Міністерства оборони США, свого

часу зазначав, що 90% всієї розвідувальної інформації отримується з відкритих джерел, тоді як лише 10% припадає на агентурну діяльність [цит. за 9, с. 144].

У досліджуваному контексті постає питання не тільки модернізації освітніх підходів, але й в тому числі формування нової професійної ідентичності фахівця СБУ. В аспекті євроінтеграційних орієнтирів, від такого переосмислення, зрештою, залежить спроможність держави ефективно реагувати на виклики сучасності.

Стан опрацювання проблематики інформаційно-аналітичної діяльності у сфері національної безпеки, зокрема в контексті функціонування СБУ та використання OSINT, вбачається достатньо сформованим на рівні окремих аспектів, утім, не позбавленим внутрішньої фрагментарності та методологічної незавершеності. Так, у дослідженні В. Івкової та І. Опірського здійснено ґрунтовний аналіз сучасних інструментів і підходів до проведення OSINT, де автори, апелюючи до технічного виміру інформаційної безпеки, акцентують увагу на зростанні ролі відкритих джерел як елементу розвідувальної діяльності, що, втім, розглядається переважно у площині інформаційних технологій [9]. У свою чергу, Е. Беденюк пропонує типологізацію інформаційно-аналітичних служб в Україні, визначаючи їх функціональне навантаження та напрями діяльності, однак, як видається, поза увагою залишається питання їх адаптації до умов воєнного часу та євроатлантичного вектора розвитку [10].

А. Ватраль, досліджуючи взаємозв’язок інформаційно-аналітичної та пізнавальної діяльності у контррозвідці, слушно підкреслює гносеологічну природу аналітики, розглядаючи її як форму спеціалізованого пізнання, що, втім, не охоплює сучасних технологічних інструментів, притаманних цифровій розвідці [11]. Натомість Т. Дорошенко вже звертається до проблем підготовки фахівців СБУ, обґрунтовуючи необхідність оновлення освітніх підходів з огляду на актуальні виклики безпекового середовища, охоплюючи кіберзагрози та алгоритмічну аналітику [12].

Разом із тим, організаційно-правовий аспект інформаційно-аналітичного забезпечення діяльності правоохоронних органів розкрито у роботі О. Мельнікової, де увагу зосереджено на нормативній регламентації відповідних процедур, що, безумовно, є важливим у контексті забезпечення законності аналітичної діяльності [13]. Подібним чином, В. Миргород аналізує діяльність СБУ крізь призму національної безпеки, наголошуючи на значенні аналітичного забезпечення як інструменту формування стратегічних рішень [14].

У площині євроінтеграційних процесів І. Наконечна обґрунтовує необхідність покращення інформаційно-аналітичних процедур з урахуванням європейських стандартів, однак, як видається, питання їх практичної імплементації у діяльність СБУ залишається недостатньо розкритим [15]. Водночас С. Попов та ін. досліджують інформаційно-аналітичну підтримку державної політики, акцентуючи увагу на форсайт-методах і доказовому підході, що має значний потенціал для застосування у безпековій сфері [16].

Окремої уваги заслуговують дисертаційні дослідження, зокрема робота К. Споришева, у якій здійснено аналіз механізмів державного управління інформаційно-аналітичним забезпеченням сил безпеки України. Вбачається, що саме у названому дослідженні найбільш повно розкрито інституційний вимір проблеми, утім, питання підготовки кадрів у контексті сучасних викликів, пов’язаних із війною та цифровізацією, потребує подальшого розвитку [17]. Натомість М. Сергієнко ще раніше окреслив значення аналітичної підтримки управлінських рішень у діяльності СБУ, що, попри певну часову віддаленість, є релевантним і сьогодні в частині розуміння ролі аналітики у системі національної безпеки [18]. Завершуючи огляд, слід згадати також К. Шеіна, який досліджує організаційно-функціональну структуру СБУ, створюючи підґрунтя для розуміння місця аналітичних підрозділів у її системі, хоча без детального аналізу їх діяльності [19].

У підсумку, попри наявність значного наукового доробку, поза належною увагою залишаються питання трансформації підготовки фахівців СБУ у сфері інформаційно-аналітичної діяльності в умовах воєнного стану, зокрема з урахуванням ролі OSINT, алгоритмічної аналітики та євроатлантичних стандартів, що, власне кажучи, і зумовлює наукову новизну та спрямованість цього дослідження.

Метою статті є доктринально-прикладне обґрунтування євроінтеграційних орієнтирів підготовки фахівців СБУ в сфері інформаційно-аналітичної діяльності крізь призму зміни безпекового середовища в умовах війни, зокрема шляхом аналізу нормативно-правових засад, операційно-аналітичної практики СБУ, сучасних форм і методів аналітичного забезпечення контррозвідувальної та кібербезпекової діяльності, а також визначення вимог до професійних компетентностей персоналу відповідно до стандартів євроатлантичного безпекового простору.

Виклад основного матеріалу. У нормативно-правовій площині функціонування сектору безпеки і оборони України, зокрема в умовах дії правового режиму воєнного стану, інформаційно-аналітична діяльність СБУ є спеціальним інструментом оперативно-службової діяльності, що безпосередньо корелює із реалізацією контррозвідувальних, антитерористичних та кібербезпекових функцій. Насамперед, слід звернутися до положень Закону України «Про правовий режим воєнного стану» від 12.05.2015 р. №389-VIII, який, зосереджуючись на розширенні повноважень суб'єктів сектору безпеки, передбачає необхідність оперативного прийняття управлінських рішень на підставі достовірної аналітичної інформації, що формується, зокрема, аналітичними підрозділами СБУ [20]. Безумовно, в умовах сьогодення інформаційно-аналітична діяльність стає складовою оперативного планування, де аналітичний продукт має чітко визначений прикладний характер та інтегрується у цикл прийняття рішень на рівні оперативних штабів.

Звертаючись до практики, доцільно згадати серію контррозвідувальних операцій СБУ, що мали на меті нейтралізацію агентурно-диверсійних мереж, які діяли в прифронтових регіонах. Зокрема, у 2023-2024 роках СБУ системно викривала агентів, які здійснювали збір розвідувальної інформації щодо дислокації підрозділів Збройних Сил України, маршрутів переміщення військової техніки та об'єктів критичної інфраструктури. Так, за офіційними даними, у 2023 році було викрито 47 агентурних мереж, а від початку 2024 року – ще 11 [21]. У зазначених операціях аналітичні підрозділи здійснювали аналіз комунікацій (SIGINT), поведінкових патернів та фінансових транзакцій, що дало змогу ідентифікувати зв'язки між окремими агентами та їх кураторами. Принагідно зауважимо, що наведені приклади засвідчують чималу ефективність використання методів кореляційного аналізу та профілювання, що, власне кажучи, наближає українську практику до стандартів аналітичної діяльності, притаманних безпековим структурам держав-членів НАТО.

Окремо варто зупинитися на операціях СБУ у сфері протидії інформаційно-психологічним спеціальним операціям противника. Як наголошувалося раніше, в умовах гібридної війни інформаційний простір є середовищем ведення інформаційних бойових дій, в яких аналітичні підрозділи виконують функції моніторингу, ідентифікації та нейтралізації дезінформаційних кампаній. Зокрема, у 2022-2025 роках СБУ неодноразово викривала мережі бот-ферм, які використовувалися для поширення наративів, спрямованих на дестабілізацію внутрішньополітичної ситуації [22]. Відповідно, застосовувалися алгоритми аналізу великих даних для виявлення нетипових поведінкових моделей акаунтів, визначення джерел координації та здійснення блокування відповідних ресурсів у взаємодії з іншими державними органами.

Упродовж 2025 року діяльність Оперативного центру реагування на кіберінциденти засвідчила стійке зростання інтенсивності кіберзагроз: було опрацьовано близько 17,3 тис. подій щодо інформаційної безпеки, з яких 730 визначено як кіберінциденти різного ступеня складності.

Велику частку серед них становили інциденти, пов'язані з поширенням і використанням шкідливого програмного забезпечення. Разом із тим, узагальнення характеру зафіксованих атак дає підстави стверджувати, що їх стратегічна мета полягала у встановленні латентного контролю над інформаційними системами з подальшим використанням такого доступу для здійснення кіберрозвідувальної діяльності або незаконного привласнення фінансових ресурсів [23, с. 4].

У контексті діяльності СБУ, йдеться не тільки про посягання на окремі інформаційні ресурси, а, передусім, про загрозу державній безпеці. З огляду на це, одним із пріоритетних напрямів функціонування СБУ є виявлення, попередження та нейтралізація кіберінцидентів, що можуть бути інструментом як фінансово мотивованих злочинів, так і елементом гібридної війни.

Очевидно, слід говорити про те, що в часі війни інформаційно-аналітичне забезпечення контррозвідувальної діяльності має в тому числі концептуально-правове значення, стаючи самостійним елементом механізму гарантування державної безпеки. В даному випадку аналітик виступає не стільки технічним обробником даних, скільки носієм функції інтелектуально-правової інтерпретації, здатним шляхом інтеграції різнорідних інформаційних потоків формувати змістовно завершені аналітичні конструкції, релевантні для прийняття владних рішень у сфері контррозвідувальної діяльності.

При цьому сучасна парадигма здобуття розвідувальної інформації характеризується поліцентричністю джерел та методів. Зокрема, OSINT (Open source intelligence) охоплює обробку відкритих, необмежених у доступі інформаційних ресурсів; HUMINT (Human intelligence) передбачає отримання відомостей через комунікативну взаємодію з особами, включно із застосуванням інструментів соціальної інженерії; IMINT (Imagery Intelligence) базується на використанні візуалізованих даних, зафіксованих технічними засобами; SIGINT (Signals intelligence) – на перехопленні сигналів комунікаційного характеру; MASINT (Measurement and signature intelligence) – на аналітичному опрацюванні специфічних техніко-наукових параметрів; а GEOINT (Geospatial Intelligence) – на синтезі просторово-координатної інформації із зображеннями [9, с. 144-145]. Власне, конвергенція вищенаведених методів формує складну доказово-аналітичну основу, що визначає в подальшому як ефективність контррозвідувальних заходів, так і межі їх правомірної реалізації.

До слова, Закон України «Про Службу безпеки України» від 25.03.1992 р. №2229-XII [24] прямо передбачає здійснення контррозвідувальної діяльності як однієї з основних функцій СБУ (ст. 12, п. 4, 6, 7 ст. 24 Закону), що, у свою чергу, зумовлює необхідність високого рівня аналітичної підготовки кадрів.

У світлі наведеного, узагальнення емпіричних даних та практики оперативно-службової діяльності СБУ об'єктивно вимагає їх систематизації крізь призму функціонально-операційних характеристик інформаційно-аналітичної діяльності. Насамперед, мова йде не стільки про констатацію окремих прикладів чи інструментів, скільки про розкриття внутрішньої логіки їх використання – взаємозв'язків між напрямами аналітики, застосованим інструментарієм та професійними компетентностями персоналу. У такій перспективі стає можливим відобразити як реальний зміст аналітичної роботи в умовах воєнного стану, так і окреслити вимоги, яким повинні відповідати фахівці відповідного профілю. Для цього доцільним є звернення до таблиці, яка системно репрезентує основні напрями інформаційно-аналітичної діяльності СБУ, їх операційно-тактичне наповнення та компетентнісні характеристики.

Таблиця 1. Операційно-аналітичні напрями діяльності СБУ в умовах воєнного стану та вимоги до професійних компетентностей персоналу

Напрям інформаційно-аналітичної діяльності	Операційно-тактичний зміст	Методи/технології	Необхідні компетентності персоналу

Контррозвідувальна аналітика	Виявлення, документування та нейтралізація агентурних мереж; аналіз розвідувально-підривної діяльності	HUMINT, SIGINT, аналіз зв'язків (link analysis), профілювання	Оперативне мислення, аналітична логіка, знання контррозвідки, навички роботи з закритими даними
Кібербезпекова аналітика	Аналіз кібератак, виявлення вразливостей, прогнозування кіберзагроз	Digital forensics, reverse engineering, big data analytics	Технічна підготовка, знання кібербезпеки, алгоритмічне мислення
Інформаційно-психологічна аналітика	Моніторинг інформаційного простору; виявлення дезінформаційних кампаній	OSINT, sentiment analysis, соціометричний аналіз	Критичне мислення, знання медіасередовища, когнітивна аналітика
Оперативно-стратегічна аналітика	Підготовка аналітичних довідок для прийняття рішень на рівні РНБО	Scenario planning, risk assessment, foresight-аналіз	Стратегічне мислення, системний аналіз, правове розуміння безпеки
Міжвідомча аналітична координація	Інтеграція даних між СБУ, ЗСУ, розвідувальними органами	Data fusion, міжсистемна інтеграція	Комунікаційні навички, розуміння міжвідомчих процедур

Створено авторами.

Більше того, звернення до проблематики професійної підготовки фахівців інформаційно-аналітичного профілю СБУ неминуче актуалізує питання співвідношення так званих «hard skills» та «soft skills», які, власне кажучи, у сучасних безпекових реаліях стають взаємодоповнюючими, а подекуди й взаємозалежними.

На наше переконання, переважання виключно технократичного підходу до підготовки аналітиків, коли акцент робиться на володінні інструментарієм OSINT, цифрової криміналістики, аналізу великих даних, SIGINT або кіберрозвідки, без належного розвитку когнітивних і поведінкових характеристик, призводить до зниження ефективності аналітичного продукту як такого. До «hard skills» у даному контексті, безумовно, належать навички обробки масивів даних, застосування алгоритмічної аналітики, робота з геоінформаційними системами, цифрова верифікація мультимедійного контенту, а також знання нормативно-правових засад оперативно-розшукової діяльності та контррозвідки [25, с. 276]. Варто наголосити, що саме названі компетентності дають можливість здійснювати первинну ідентифікацію загроз, документування протиправної діяльності та формування доказової бази, легітимної для застосування у кримінальному провадженні. Втім, як показує практика, навіть найбільш технічно підготовлений аналітик не здатен забезпечити належний рівень аналітичного узагальнення без розвинених «soft skills».

У свою чергу, до «soft skills», які мають визначальне значення для діяльності аналітичних підрозділів СБУ, слід віднести критичне мислення, здатність до аналітичної інтерпретації неоднорідної інформації, комунікативну гнучкість у межах міжвідомчої координації, стресостійкість в умовах оперативного навантаження, а також етичну відповідальність за результати аналітичної діяльності [25, с. 277]. В даному випадку аналітик є суб'єктом прийняття рішень, здатним оцінювати достовірність інформації, прогнозувати розвиток подій та формувати рекомендації для керівництва.

В аспекті обраної тематики, звернення до євроатлантичних орієнтирів підготовки фахівців СБУ у сфері інформаційно-аналітичної діяльності неминуче актуалізує не тільки питання впровадження стандартів НАТО, але й інституційні практики правоохоронного співробітництва в межах ЄС, передусім через діяльність Європолу (англ. «Europol») як основного координаційного центру аналітичного обміну інформацією. В даному випадку стандарти розвідувального циклу НАТО поєднуються з кримінально-аналітичними процедурами Європолу, створюючи, власне кажучи, єдине методологічне середовище для підготовки аналітиків безпекового сектору.

Як наголошується у практиці Європолу, інформаційно-аналітична діяльність ґрунтується на принципах «intelligence-led policing», де аналітичний продукт – це визначальний елемент прийняття управлінських рішень [26]. У межах інституційної структури Європолу функціонують спеціалізовані аналітичні платформи, зокрема SIENA («Secure Information Exchange Network Application»), які забезпечують захищений обмін інформацією між правоохоронними органами держав-членів та партнерських країн [27]. У світлі цього, підготовка фахівців СБУ має передбачати не тільки опанування стандартів обробки інформації, але й здатність працювати у багаторівневих системах міжнародного інформаційного обміну з дотриманням режимів конфіденційності та класифікації даних.

Окремо варто зупинитися на аналітичних підходах, що застосовуються Європолом, зокрема в кримінальному аналізі («criminal intelligence analysis»). Зокрема, тут варто говорити про використання методів аналізу зв’язків, розпізнавання закономірностей, поведінкового аналізу та профілювання ризиків [28]. Очевидно, наведені інструменти мають безпосереднє значення і для діяльності СБУ, особливо в частині протидії транснаціональним загрозам (напр., кіберзлочинність, фінансування тероризму та діяльність диверсійно-розвідувальних груп). В той же час Європол акцентує на доказовій придатності аналітичних матеріалів у кримінальному провадженні, що, безумовно, корелює із завданнями СБУ як правоохоронного органу спеціального призначення.

Звертаючись до практичного виміру, слід вказати, що співпраця України з Європолом вже має інституційне закріплення, зокрема через Угоду між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016 р., що відкриває можливості для участі українських правоохоронних органів у спільних аналітичних операціях та обміні інформацією [29]. У світлі зазначеного, підготовка кадрів СБУ має бути зорієнтована на опанування процедур взаємодії з міжнародними партнерами, охоплюючи використання уніфікованих форматів аналітичної звітності, дотримання стандартів захисту персональних даних та забезпечення юридичної валідності отриманої інформації.

Слід звернути увагу і на той момент, що в умовах війни кадровий потенціал будь-яких правоохоронних органів є особливо важливим, адже саме від рівня підготовки аналітиків залежить ефективність оперативно-службової діяльності в цілому. Врешті, варто відмітити, що формування професійних навичок має здійснюватися не тільки в рамках формальної освіти, але й в тому числі через систему безперервного професійного розвитку (зокрема, тренування, симуляції оперативних ситуацій та участь у реальних операціях).

Висновки. Підсумовуючи, слід відмітити, що інформаційно-аналітична діяльність СБУ в умовах воєнного часу є тим інструментом оперативно-службового впливу, який безпосередньо визначає якість контррозвідувальних, антитерористичних та кібербезпекових заходів.

Переходячи до пропозицій, передусім, у практичному вимірі доцільно впровадити модель оперативної аналітики реального часу («real-time intelligence»), яка передбачає синхронізацію потоків OSINT, SIGINT та внутрішніх баз даних СБУ із подальшою автоматизованою обробкою за допомогою алгоритмічних інструментів. В той же час, вбачається необхідним створення

внутрішніх аналітичних центрів швидкого реагування, інтегрованих у структуру оперативних підрозділів.

Безумовно, найбільш значущим та пріоритетним напрямом удосконалення є кадрове забезпечення. На наше переконання, слід впровадити модель аналітика подвійної компетентності – фахівця, який одночасно володіє юридичними знаннями та навичками цифрової аналітики. Принагідно зауважимо, що підготовка таких кадрів має здійснюватися через використання симуляційних навчальних середовищ, максимально наближених до реальних умов оперативно-службової діяльності, включаючи моделювання інформаційних операцій противника та сценаріїв гібридних загроз. Так, окремі елементи такої підготовки вже впроваджуються, однак вони не відтворюють повного циклу аналітичної та контррозвідувальної діяльності. Відтак доцільно істотно посилити практичну складову шляхом регулярного моделювання реальних оперативних ситуацій із відпрацюванням взаємодії аналітичних і оперативних підрозділів у режимі реального часу.

Ще одним перспективним напрямом, який, вбачається, недостатньо реалізований станом натепер, є впровадження прогностичної аналітики («predictive intelligence») у діяльність СБУ. Тут варто говорити про використання методів машинного навчання для виявлення латентних загроз, прогнозування поведінки ворожих агентурних мереж та визначення потенційних точок дестабілізації.

У світлі євроінтеграційних орієнтирів, окремо доцільно запропонувати впровадження обов’язкової сертифікації аналітиків СБУ за стандартами, наближеними до практик НАТО (зокрема, оцінка здатності працювати з багатоджерельною інформацією, здійснювати критичний аналіз та формувати аналітичні продукти, придатні для використання у міжнародному середовищі).

Врешті решт, подальший розвиток інформаційно-аналітичної діяльності СБУ має відбуватися у напрямі формування нової аналітичної парадигми, де співіснують технологічна інноваційність, правова визначеність та оперативна доцільність.

ЛІТЕРАТУРА

1. Захист національної державності. Служба безпеки України. URL: https://ssu.gov.ua/zakhyst-natsionalnoi-derzhavnosti
2. Звіт за третій квартал 2022 року. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. 2022. URL: https://scpc.gov.ua/uk/articles/163
3. Звіт за друге півріччя 2022 року. Служба безпеки України. URL: https://antycorportal.nazk.gov.ua/uploads/uo/00034074/report-367/nacp-report-367.pdf
4. Річний аналітичний огляд: жовтень 2023-вересень 2024. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf
5. Про національну безпеку України: Закон України від 21.06.2018 №2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
6. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України»: Указ Президента України від 14.09.2020 №392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text
7. Актуальні проблеми державотворення та правотворення: конституційні, загальнотеоретичні та філософсько-правові аспекти: монографія / кол. авт.; за заг. ред. Д. Забзалюка. Львів: Растр-7, 2026. С. 51-73.

8. Роль OSINT-досліджень у підвищенні рівня національної безпеки України: матеріали круглого столу (м. Львів, 7 травня 2025 р.) / укладач І.О. Ревак. - Львів: ЛьвДУВС, 2025. 249 с.
9. Івкова В.С., Опірський І.Р. Дослідження існуючих засобів та підходів до проведення OSINT в контексті інформаційної безпеки особи та держави. Комп'ютерні системи та мережі. Львів: Видавництво Львівської політехніки, 2025. Том 7. № 1. С. 143-159. DOI: https://doi.org/10.23939/csn2025.01.143
10. Беденюк Е.Б. Інформаційно-аналітичні служби в Україні: типологія, функції, напрями діяльності. Робота на здобуття кваліфікаційного ступеня магістра: спец. 029 Інформаційна, бібліотечна та архівна справа / наук. кер. О. Б. Герасимчук; Волинський національний університет імені Лесі Українки. Луцьк, 2024. 76 с. URL: https://evnuir.vnu.edu.ua/bitstream/123456789/26580/1/bedeniuke_2024.pdf
11. Ватраль А.В. Взаємозв'язок інформаційно-аналітичної та пізнавальної діяльності в контррозвідці. Інформаційна безпека людини, суспільства, держави. 2018. №2 (24). С. 75-83.
12. Дорошенко Т.В. Реалії та перспективи підготовки фахівців Служби безпеки України для підрозділів за напрямом інформаційно-аналітичної діяльності. Інформаційна безпека людини, суспільства, держави. 2025. №1 (38). С. 16-27. DOI: https://doi.org/10.511369/2707-7276-2025-1(38)-2
13. Мельнікова О.О. Організаційно-правові основи інформаційно-аналітичного забезпечення діяльності правоохоронних органів. Південноукраїнський правничий часопис. 2023. №2. С. 43-51. DOI: https://doi.org/10.32850/sulj.2023.2.7
14. Миргород В.В. Діяльність Служби безпеки України в контексті національної безпеки. Науковий вісник Ужгородського національного університету. 2024. Серія: Право. Вип. 82. Ч. 2. С. 222-227. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.35
15. Наконечна І.В. Інформаційно-аналітичні процедури забезпечення національної безпеки України в умовах євроінтеграції. Правові новели. 2023. №19. С. 77-84. DOI: https://doi.org/10.32782/ln.2023.19.11
16. Попов С., Вошко І., Коваль З., Маміч В., Розмазнін О., Душкін Ю. Інформаційно-аналітична, доказова і форсайт підтримки державної політики у сфері національної безпеки: порівняльний аналіз. Актуальні проблеми державного управління. 2021. №3 (84). С. 167-174.
17. Споришев К.О. Механізми державного управління системою інформаційно-аналітичного забезпечення сил безпеки України. Реферат дис. … наук. ступеня доктора наук з державного управління (спец.: 25.00.05). Національний університет цивільного захисту України. Харків, 2024. 36 с.
18. Сергієнко М.Г. Інформаційно-аналітична підтримка управлінських рішень у діяльності Служби безпеки України як суб'єкта національної безпеки. Теорія та практика державного управління. 2012. Вип. 3 (38). С. 123-130.
19. Шеін К.А. Система, організація та функції Служби безпеки України. Юність науки – 2025: збірник тез доповідей XV Міжнародної науково-практичної конференції студентів, аспірантів і молодих вчених (м. Чернігів, 23-25 квітня 2025 р.). Чернігів: НУ «Чернігівська політехніка», 2025. С. 536-537.
20. Про правовий режим воєнного стану: Закон України від 12.05.2015 №389-VIII. URL: https://zakon.rada.gov.ua/laws/show/389-19#Text
21. СБУ викрила 11 агентурних мереж РФ від початку 2024 року – Малюк. 2024. URL: https://surl.li/cncbrk
22. Безкарність у мережі. Де вироки організаторам ворожих ботоферм – розслідування. 2025. URL: https://surl.li/sfqeqt

23. 2025 Річний звіт. Система виявлення вразливостей і реагування на кіберінциденти та кібератаки. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України. URL: https://scpc.gov.ua/api/files/80f81334-75fc-44f4-9403-62a9a8e1bc7f
24. Про Службу безпеки України: Закон України від 25.03.1992 №2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12
25. Шаршаткін Д., Маміч В., Маляганов В. Розвиток «жорстких» (hard skills) та «м'яких» (soft skills) навичок у підготовці фахівців інформаційно-аналітичної діяльності. Військова освіта. 2021. №2 (44). С. 275-282. DOI: https://doi.org/10.33099/2617-1783/2021-44/275-282
26. AI and policing. The benefits and challenges of artificial intelligence for law enforcement. An Observatory Report from the Europol Innovation Lab. Publications Office of the European Union. 2024. 60 p. DOI: https://doi.org/10.2813/0321023
27. Secure Information Exchange Network Application (SIENA). Ensuring the secure exchange of information between Europol and its partners. 2026. URL: https://www.europol.europa.eu/how-we-work/services-support/siena
28. Intelligence Analysis. Europol. 2025. URL: https://www.europol.europa.eu/how-we-work/services-support/intelligence-analysis
29. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво від 14.12.2016. URL: https://zakon.rada.gov.ua/laws/show/984_001-16#Text

---

Дата першого надходження рукопису до видання: 02.03.2026
Дата прийнятого до друку рукопису після рецензування: 20.03.2026
Дата публікації: 17.04.2026