Кримінальний процес та криміналістика

УДК 343.1

DOI https://doi.org/10.5281/zenodo.17425650

Діяльність СБУ у протидії гібридним загрозам у кримінальному процесі

Гудима Віталій Валерійович,
кандидат юридичних наук, доцент, кафедра судоустрою, прокуратури та адвокатури, Львівський університет бізнесу та права, м. Львів, Україна,
https://orcid.org/0000-0001-6708-3910

Прийнято: 11.08.2025 | Опубліковано: 30.08.2025

Анотація. Актуальність дослідження зумовлено зростанням масштабів гібридних загроз, що поєднують інформаційні, кібернетичні, фінансові та правові інструменти впливу і суттєво трансформують кримінальний процес України. У сучасних умовах повномасштабної агресії російської федерації діяльність Служби безпеки України набуває системоутворювального значення для захисту національної безпеки, забезпечення правової визначеності та легітимності доказових процедур. Потреба у вдосконаленні правового статусу СБУ та її взаємодії з іншими правоохоронними органами обумовлює наукову й практичну важливість проведеного аналізу.

Метою статті є визначення правових і організаційних засад діяльності Служби безпеки України у протидії гібридним загрозам у межах кримінального процесу та обґрунтування напрямів її вдосконалення з урахуванням нових викликів безпекового середовища.

У роботі застосовано системно-структурний, порівняльно-правовий, формально-логічний і функціональний методи. Системна практика дала змогу дослідити місце СБУ в архітектурі національної безпеки, а порівняльний аналіз – зіставити українську модель з європейськими стандартами діяльності

спецслужб. Формально-логічний метод сприяв уточненню понятійно-категоріального апарату, а функціональна практика забезпечила виявлення реальних механізмів інтеграції СБУ у кримінальний процес.

Встановлено, що протидія гібридним загрозам потребує комплексної координації між СБУ, прокуратурою, судами та міжнародними партнерами. Виявлено основні проблеми правозастосування: фрагментарність нормативного регулювання, невизначеність процесуального статусу СБУ, недосконаліть цифрової верифікації доказів, зокрема колізію між державною таємницею та правом на захист. Доведено, що сучасна модель кримінального процесу вимагає переходу до цифрової доказової архітектури, орієнтованої на принцип ланцюгів електронних доказів (*e-evidence chain)*.

Отримані результати засвідчили необхідність формування сучасної концепції діяльності СБУ, заснованої на оновлених нормативно-правових засадах, цифровій верифікації доказів, ефективному парламентському контролі та інтегрованій міжвідомчій підготовці кадрів у сфері кібербезпеки й захисту прав людини, що має важливе теоретичне й практичне значення для зміцнення національної безпеки України.

Перспективним напрямом є розроблення нормативної моделі цифрової доказової інфраструктури в Україні, уніфікація стандартів доказової автентифікації з практикою ЄС та формування теоретичних засад демократичного контролю за діяльністю спецслужб у сфері кримінальної юстиції.

Ключові слова: національна безпека, кримінальне провадження, контррозвідувальна діяльність, цифрові докази, гібридна агресія, міжвідомча взаємодія, процесуальна легітимність, кібербезпека.

ISSN: 3041-2110

The role of the Security Service of Ukraine (SSU) in countering hybrid threats within criminal proceedings

Vitaliy Hudyma,
PhD in Law, Associate Professor, Department of Judiciary, Prosecutor's Office and Advocacy, Lviv University of Business and Law, Lviv, Ukraine,
https://orcid.org/0000-0001-6708-3910

Abstract. The relevance of the research is determined by the growing scale of hybrid threats that combine informational, cyber, financial, and legal instruments of influence, fundamentally transforming the criminal procedure in Ukraine. Under the conditions of russia's full-scale aggression, the activity of the Security Service of Ukraine (SSU) acquires a system-forming role in protecting national security, ensuring legal certainty, and maintaining the legitimacy of evidentiary procedures. The necessity to improve the legal status of the SSU and enhance its interaction with other law enforcement bodies defines both the scientific and practical importance of this analysis.

The purpose of the article is to identify the legal and organizational foundations of the Security Service of Ukraine's activity in countering hybrid threats within the framework of the criminal process and to substantiate directions for its improvement, taking into account contemporary challenges to national security.

The research applies system-structural, comparative-legal, formal-logical, and functional methods. The systemic approach made it possible to explore the SSU's place within the architecture of national security. At the same time, the comparative-legal analysis allowed correlating the Ukrainian model with European standards of intelligence and counterintelligence activity. The formal-logical method clarified the conceptual apparatus, and the functional approach helped to reveal the practical mechanisms of integrating the SSU into the criminal process.

It has been established that effective counteraction to hybrid threats requires complex coordination among the SSU, the Prosecutor's Office, the judiciary, and international partners. The study revealed key enforcement issues: the fragmentation of normative regulation, the lack of procedural clarity regarding the SSU's status, insufficient mechanisms for digital evidence verification, and the persistent conflict between state secrecy and the right to defense. It has been proven that the modern criminal process in Ukraine necessitates a transition toward a digital evidentiary architecture based on the *e-evidence chain* principle.

The obtained results confirm the need to develop a modern concept of the Security Service of Ukraine's activity based on updated legal foundations, digital verification of evidence, effective parliamentary oversight, and integrated interagency training in cybersecurity and human rights. It has significant theoretical and practical importance for strengthening Ukraine's national security.

Future research should focus on developing a regulatory model for Ukraine's digital evidence infrastructure, harmonizing national standards of evidentiary authentication with EU practice, and elaborating theoretical foundations for democratic oversight of intelligence agencies within the criminal justice system.

Keywords: national security, criminal proceedings, counterintelligence activity, digital evidence, hybrid aggression, interagency cooperation, procedural legitimacy, cybersecurity.

Постановка проблеми. Сучасна трансформація безпекового середовища України, зумовлена російською агресією та поширенням гібридних форм протидії державності, вимагає переосмислення ролі спеціальних служб у кримінальному процесі. Гібридні загрози поєднують ознаки злочинних, інформаційних і воєнних дій, створюючи багаторівневі ризики для національної безпеки та правопорядку. В цих умовах система кримінальної юстиції стикається з новими викликами, пов'язаними з необхідністю фіксації, кваліфікації та доведення злочинів, що здійснюються

через кіберпростір, інформаційно-психологічний вплив чи диверсійно-підривну діяльність. Проблема полягає в тому, що чинні процесуальні механізми не завжди дають змогу ефективно реагувати на динаміку та прихований характер таких діянь. Водночас діяльність Служби безпеки України (СБУ) потребує чіткого правового врегулювання в межах кримінального провадження, особливо під час документування злочинів проти основ національної безпеки, коли поєднуються контррозвідувальні, аналітичні та слідчі функції. Відсутність системного узгодження між оперативно-розшуковими заходами та процесуальними процедурами, зокрема на етапах збирання, перевірки й легалізації доказів, створює ризики як для належного формування доказової бази, так і для дотримання прав людини під час досудового розслідування.

Наукова актуальність проблеми визначається необхідністю вироблення нових практик інтеграції контррозвідувальних механізмів у кримінально-процесуальну діяльність, розроблення чітких критеріїв допустимості доказів, отриманих у ході спеціальних операцій, та вдосконалення правового статусу органів безпеки у структурі кримінальної юстиції. З практичного погляду її розв’язання сприятиме підвищенню ефективності державної протидії гібридним загрозам, забезпеченню прозорості процедур і формуванню балансу між інтересами національної безпеки та принципами верховенства права.

Аналіз останніх досліджень і публікацій. Аналіз наукових праць, присвячених діяльності Служби безпеки України у протидії гібридним загрозам у кримінальному процесі, дає змогу виокремити чотири основні напрями. Перший напрям охоплює теоретико-концептуальні та політико-правові засади формування безпекової політики держави в умовах гібридної агресії. Дослідник П. Л. Лисянський [1] аналізує феномен регіонального сепаратизму в Україні як складника гібридної війни російської федерації, акцентуючи на тому, що протидія дестабілізаційним проявам вимагає

 ISSN: 3041-2110

зміцнення контррозвідувального потенціалу Служби безпеки України та вдосконалення правових механізмів реагування на загрози територіальній цілісності. Автор П. Л. Лисянський [2] доводить, що діяльність політичних партій російської федерації на тимчасово окупованих територіях є інструментом політичного експансіонізму, а СБУ має бути основним суб'єктом у системі протидії політичному впливу держави-агресора. Вчений А. М. Тимчишин [3] визначає, що ефективне застосування спеціальних знань у правоохоронній діяльності є передумовою формування нових практик документування гібридних злочинів, зокрема тих, що спрямовані на підрив національної безпеки. Перспективним у цьому напрямі є дослідження еволюції концепції гібридної загрози та її адаптації у правову доктрину національної безпеки України.

Другий напрям стосується процесуально-правових та криміналістичних аспектів діяльності Служби безпеки України. У праці науковця А. М. Тимчишина [4] обґрунтовано використання криміналістичних даних у розробленні стратегій протидії воєнній агресії, зокрема в енергетичному секторі, що потребує залучення СБУ як суб'єкта аналітичного забезпечення. Дослідники О. П. Метелев та Є. В. Коваленко [5] доводять необхідність нормативного закріплення процедур використання цифрової інформації, отриманої під час оперативно-розшукових та контррозвідувальних дій, у доказовій базі кримінального провадження. Автор В. В. Миргород [6] аналізує сучасну роль СБУ у системі національної безпеки, наголошуючи на тому, що протидія гібридним викликам вимагає синхронізації кримінально-правових і контррозвідувальних інструментів. Перспективним напрямом подальших досліджень є розроблення уніфікованих методів використання оперативних матеріалів як доказів у справах, пов'язаних з гібридними посяганнями.

Третій напрям охоплює організаційно-правові аспекти діяльності СБУ, зокрема її повноваження у кримінальному процесі та утримання балансу між безпекою і правами людини. Науковець В. В. Козар [7] проаналізував систему

суб'єктів протидії кримінальним правопорушенням в Україні та особливості їхнього адміністративно-правового статусу, що дає змогу уточнити інституційне місце СБУ у структурі суб'єктів кримінальної юстиції та визначити напрями вдосконалення її управлінських і координаційних функцій. Дослідник М. М. Погорецький [8] аналізує гарантії дотримання прав і свобод людини під час діяльності СБУ, наголошуючи на необхідності процесуального контролю за реалізацією безпекових функцій. Вчені О. М. Герасименко та С. М. Невмержицький [9] досліджують роль СБУ у запобіганні та припиненні кримінальних правопорушень на об'єктах критичної інфраструктури, визначаючи напрями посилення міжвідомчої взаємодії. Подальші дослідження в цьому напрямі доцільно спрямувати на створення єдиної моделі взаємодії між контррозвідувальними, аналітичними та слідчими підрозділами СБУ у межах кримінального процесу.

Четвертий напрям охоплює міжнародно-правовий та порівняльний вимір діяльності Служби безпеки України в умовах гібридної війни. Автор М. Балан [10] розглядає взаємодію слідчого з іншими суб'єктами кримінального провадження під час розслідування порушень державного кордону України, що безпосередньо корелює з функціями СБУ у сфері прикордонної безпеки. Науковець С. Євтух (S. Yevtukh) [11] аналізує основні операції та виклики, з якими СБУ стикається під час повномасштабного російського вторгнення, підкреслюючи значення міжнародного обміну розвідувальною інформацією. Дослідники Р. С. Орловський та В. М. Козак (R. S. Orlovskyi & V. M. Kozak) [12] розглядають кримінально-правовий захист державної таємниці в Україні та Європейському Союзі, окреслюючи напрями гармонізації законодавства у сфері безпеки. Науковець Ю. Кривицький зі співавторами (Y. Kryvytskyi et al.) [13] досліджують реформу правової системи України в контексті євроінтеграції та гібридних загроз, наголошуючи на потребі посилення інституційної ролі СБУ в системі стратегічної безпеки. Перспективним напрямом подальших досліджень є

аналіз механізмів інтеграції СБУ у спільну систему контррозвідувальної співпраці з державами ЄС і НАТО та імплементація стандартів безпеки Європейського Союзу у національну практику.

Виділення невирішених раніше частин загальної проблеми. Попри наявність наукових напрацювань щодо протидії гібридним загрозам, залишається низка нерозв'язаних аспектів, зокрема відсутність чіткої правової моделі інтеграції матеріалів контррозвідувальної діяльності у кримінальний процес, недостатність єдиних стандартів цифрової верифікації доказів та обмежена узгодженість міжвідомчих механізмів взаємодії. Недослідженими залишаються питання балансування між державними інтересами та процесуальними гарантіями прав людини, зокрема адаптації українського законодавства до європейських стандартів доказовості. Запропоноване дослідження спрямоване на подолання цих прогалин шляхом формування цілісної моделі безпеково-процесуальної юстиції, розроблення механізмів легалізації контррозвідувальних матеріалів, обґрунтування єдиної системи цифрової трасології доказів та узгодження правозастосовної практики СБУ з міжнародними принципами верховенства права і демократичного контролю.

Формулювання цілей статті (визначення завдання). Мета статті – визначити правові та організаційні засади діяльності СБУ у протидії гібридним загрозам у межах кримінального процесу та обґрунтувати напрями її вдосконалення з урахуванням сучасних викликів національній безпеці.

Для досягнення мети дослідження сформульовано такі завдання:

1. Дослідити правову природу та специфіку гібридних загроз, що трансформують зміст і функції кримінального процесу у сфері національної безпеки, та проаналізувати нормативно-інституційну основу діяльності СБУ щодо їхньої нейтралізації.

2. Визначити особливості міжвідомчої взаємодії СБУ, органів досудового розслідування, прокуратури та судів і виявити проблеми

 ISSN: 3041-2110

правозастосування у використанні матеріалів оперативно-розшукової та контррозвідувальної діяльності.

3. Обґрунтувати напрями вдосконалення законодавчого регулювання та підвищення ефективності державної системи протидії гібридним загрозам у кримінальному процесі.

Виклад основного матеріалу дослідження. Гібридні загрози у сучасному правовому дискурсі розглядаються як комплексна форма деструктивного впливу, що поєднує військові, інформаційні, економічні, кібернетичні та психологічні засоби, спрямовані на підрив державного суверенітету, стабільності правопорядку та довіри до інститутів влади. Їхня сутність полягає у розмитті меж між війною та злочином, між воєнними діями та кримінальним правопорушенням, що створює для системи кримінальної юстиції нові виклики щодо кваліфікації діянь, збору доказів та притягнення винних до відповідальності. У правовому вимірі гібридні загрози набувають ознак особливого феномена, що потребує поєднання норм кримінального, інформаційного, кібербезпекового та адміністративного права. Вони змінюють саму логіку функціонування кримінального процесу, що повинен адаптуватися до умов невизначеності, багаторівневості загроз і високої швидкості їхньої реалізації (табл. 1).

Таблиця 1

Основні характеристики гібридних загроз у правовій площині та їхній вплив на кримінальний процес

Ознака гібридної загрози	Правовий прояв	Вплив на кримінальний процес
Інформаційно-психологічна дія	Поширення дезінформації, маніпуляція суспільною свідомістю	Ускладнює встановлення умислу, мотивів, причинного зв’язку злочину
Кіберкомпонент	Несанкціонований доступ до даних, порушення цілісності цифрових доказів	Потребує спеціалізованих знань та технічної експертизи при збиранні доказів
Економічно-фінансова диверсія	Використання тіньових схем, підрив фінансової стабільності	Ускладнює ідентифікацію суб’єктів злочину та джерел фінансування

ISSN: 3041-2110

Ознака гібридної загрози	Правовий прояв	Вплив на кримінальний процес
Дипломатично-правовий тиск	Залучення зовнішніх виконавців, використання міжнародних механізмів	Створює колізії юрисдикції та ускладнює міжнародне співробітництво
Використання приватних структур	Діяльність під прикриттям недержавних компаній чи ЗМІ	Потребує адаптації процесуальних норм до нових форм суб'єктності

Джерело: сформовано автором на основі [1, с. 112–113; 2, с. 247–248; 4, с. 213–214; 5, с. 179–180; 6, с. 223–224; 11, p. 139–140]

Гібридні загрози істотно трансформують архітектоніку кримінального процесу, змінюючи його доказову базу, суб'єктний склад і технологію розслідування. Особливої актуальності набуває інформаційно-психологічна дія, що формує нову сферу доказування, у межах якої об'єктом слідства є не фізична дія, а інформаційний вплив. Так, у 2023 році Служба безпеки України ліквідувала понад двадцять ботоферм і мереж інтернет-агентів, які координувалися з-за кордону та поширювали наративи про «втому суспільства від війни» й «нелегітимність влади» [14; 15]. Зібрані цифрові артефакти – логи, IP-трафік, візуалізовані графи комунікацій – були використані як докази у справах за статтями 109 та 111 Кримінального кодексу України. Саме на цьому ґрунті формується новий тип доказу – «цифровий інформаційний слід», що поєднує технічну фіксацію з контекстним аналізом умислу.

Подальший розвиток гібридних впливів, особливо у кіберпросторі, висуває вимогу до технологічної верифікації доказів. Після спроб атак угруповань Sandworm та APT28 на енергетичну інфраструктуру у 2022–2023 роках [16; 17] СБУ спільно з державним CERT-UA розробила процедуру цифрового chain of custody – неперервного ланцюга автентифікації електронних даних. Це стало підґрунтям для запровадження нового формату технічної експертизи, у межах якої доказ оцінюється не лише за змістом, а й за «життєвим циклом» – від моменту вилучення до судового розгляду.

Водночас із кіберзагрозами посилюється й економічно-фінансовий вимір гібридної агресії, що проявляється через фінансування агентурних мереж за допомогою криптовалют. Так, у 2024 році СБУ спільно з Бюро

економічної безпеки України (БЕБ) задокументувала схему переказу понад 60 млн грн через біржі Binance та EXMO, що використовувалася для забезпечення діяльності російських спецслужб [18]. У цьому контексті актуалізується створення нової процесуальної категорії – «анонімізованого фінансового доказу», тобто даних, отриманих із блокчейн-трасування, що мають зберігати доказову силу без розкриття персональних ідентифікаторів.

Одночасно дипломатично-правовий тиск формує додаткову низку проблем, зокрема колізії юрисдикції, коли проведення слідчих дій потребує залучення іноземних держав, що нерідко використовують процедурні прогалини для затягування екстрадиції або блокування доказових запитів. З метою мінімізації таких ризиків СБУ спільно з МЗС поступово впроваджує механізми «юридичного віддзеркалювання», спрямовані на узгодження процесуальних стандартів з партнерами ЄС і забезпечення цілісності доказового ланцюга.

Нарешті, використання приватних структур як інструменту гібридного впливу створює нову правову ситуацію. IT-компанії, телеком-оператори й медіаплатформи дедалі частіше є одночасно потенційними співучасниками та носіями доказів. Унаслідок цього в кримінальному процесі формується категорія «функціональної відповідальності» приватних суб'єктів, зокрема їхнього обов'язку сприяти збиранню, збереженню та захисту цифрових даних, що мають доказове значення.

Нормативно-правова система, що регламентує повноваження СБУ у протидії гібридним загрозам у кримінальному провадженні, вибудувана за поліцентричним принципом і охоплює конституційний, законодавчий, підзаконний і міжнародно-правовий рівні. Її практичне значення полягає у створенні правових умов для поєднання оперативно-розшукових, контррозвідувальних і процесуальних функцій та для легалізації даних спеціальних операцій у доказовому полі кримінального процесу (табл. 2).

Таблиця 2

Нормативно-правові засади та інституційні механізми реалізації повноважень СБУ у протидії гібридним загрозам у кримінальному провадженні

Рівень регулювання	Основні акти та положення	Інституційні механізми реалізації
Конституційний	Конституція України (ст. 17, 19, 92) – визначає безпеку як одну з основних функцій держави; визначає принцип законності у діяльності органів влади	Парламентський контроль за діяльністю СБУ через профільний Комітет Верховної Ради; обов'язковість дотримання прав людини під час реалізації повноважень
Законодавчий	Закон України «Про Службу безпеки України» (1992); Кримінальний процесуальний кодекс України (КПК, 2012); Закон «Про національну безпеку України» (2018); Закон «Про основні засади забезпечення кібербезпеки України» (2017)	Розслідування злочинів проти основ національної безпеки (ст. 216 КПК); використання контррозвідувальних матеріалів як доказів (ст. 99 КПК); координація з іншими органами сектору безпеки
Підзаконний	Постанови КМУ, накази СБУ, МВС і БЕБ про міжвідомчу взаємодію; стандарти технічного захисту інформації (ДСТУ 4145:2023)	Створення спільних слідчих груп; електронний документообіг між відомствами; уніфікація форматів цифрових доказів
Міжнародно-правовий	Будапештська конвенція про кіберзлочинність (2001); Меморандуми про співпрацю з ЄС, НАТО, Europol; участь у Центрі протидії гібридним загрозам (Гельсінкі)	Міжнародний обмін цифровими доказами; спільні розслідування; використання механізмів транскордонного доступу до даних

Джерело: сформовано автором на основі [19-24]

У практичному вимірі Конституція України [19] формує нормативне підґрунтя діяльності СБУ як складника сектору національної обороноздатності, визначаючи засади захисту державного суверенітету, територіальної цілісності та конституційного ладу. Її положення конкретизуються у Законі України «Про Службу безпеки України» [20], що визначає завдання органу з протидії розвідувально-підривній діяльності та злочинам проти держави, зокрема у сфері гібридних впливів. На підставі ст. 216 Кримінального процесуального кодексу (КПК) України [21] СБУ здійснює досудове розслідування злочинів проти основ національної безпеки,

шпигунства й тероризму, а ст. 99 КПК забезпечує використання матеріалів контррозвідувальної діяльності як доказів. У сучасній практиці це дає змогу легалізувати результати цифрового моніторингу, OSINT-розвідки, дані блокчейн-транзакцій або кіберінцидентів після експертної верифікації. Так формується процесуальний міст між оперативною діяльністю й кримінальним переслідуванням, що раніше був відсутній у національній системі доказування.

Закон України «Про національну безпеку України» [22] і Закон України «Про основні засади забезпечення кібербезпеки України» [23] створюють нормативну рамку для міжвідомчої взаємодії між СБУ, Державною службою спеціального зв'язку та захисту інформації України, Міністерством внутрішніх справ України, Національною поліцією та Бюро економічної безпеки України (БЕБ). На їхній основі у 2023–2024 роках були створені міжвідомчі слідчі групи для розслідування злочинів, пов'язаних з кібератаками на енергетичну інфраструктуру та фінансуванням підривних мереж рф. Обмін доказовими матеріалами забезпечується через державну систему «Трембіта», що дає можливість фіксувати рух даних і підвищує рівень їхньої доказової вірогідності. На міжнародному рівні правове забезпечення участі СБУ у спільних кібероперацій спирається на Будапештську конвенцію про кіберзлочинність [24], що регламентує транскордонну взаємодію у сфері збирання цифрових доказів, та на співпрацю України з Europol, Eurojust і CERT-EU. У 2023 році у межах міжнародної операції *Eastwood* проти проросійського хакерського угруповання NoName057(16) українські фахівці взаємодіяли з Europol у форматі обміну цифровими доказами [25]. Водночас відповідно до проєкту Ради Європи CyberUA реалізується навчальна програма для СБУ, прокуратури та МВС з імплементації стандартів e-evidence chain – цифрового ланцюга автентифікації доказів [26]. Ці механізми були практичним кроком до впровадження європейських стандартів доказової верифікації у кримінальному процесі України. Отже, нормативно-правова база

діяльності СБУ у протидії гібридним загрозам є не лише декларативною, а функціонує як комплексний регулятор, що поєднує національні та міжнародні інструменти правозастосування у сфері безпеки, формуючи підґрунтя для становлення в Україні безпеково-процесуальної моделі кримінальної юстиції.

Взаємодія СБУ з органами досудового розслідування, прокуратурою та судами у справах, пов'язаних з гібридними формами агресії, є визначальним елементом забезпечення кримінально-процесуальної стійкості держави. Такі злочини (фінансування агентурних мереж, інформаційно-психологічні операції, кібератаки чи підрив економічної безпеки) мають комплексний характер, що вимагає скоординованих дій кількох інституцій. З огляду на це сучасна модель взаємодії СБУ з правоохоронними органами поєднує процесуальні, аналітичні та технологічні компоненти, засновані на принципах цифрової доказовості, оперативного реагування та міжнародної сумісності (табл. 3).

Таблиця 3

Форми та механізми взаємодії СБУ з органами досудового розслідування, прокуратурою та судами у процесі документування злочинів гібридного характеру

Рівень взаємодії	Основні напрями співпраці	Практичні механізми реалізації
Міжвідомчий (національний)	Координація дій між СБУ, Офісом Генерального прокурора, Національною поліцією та Бюро економічної безпеки України	Спільні слідчі групи, оперативні штаби при РНБО, обмін доказовими матеріалами через електронні системи державної взаємодії
Процесуальний	Узгодження доказової бази, легалізація матеріалів контррозвідувальної діяльності, участь у досудових слідчих діях і судових засіданнях	Використання матеріалів оперативно-розшукових дій як доказів; цифровий облік і трасування електронних доказів
Судовий	Представництво в кримінальних провадженнях щодо державної зради, шпигунства, фінансування тероризму	Експертна участь у судових засіданнях, судово-технічна експертиза цифрових носіїв, передача матеріалів через систему «Е-Суд»
Міжнародний	Співпраця з Europol, Eurojust, CERT-EU, Міжнародним	Спільні розслідування, транскордонний обмін цифровими

Рівень взаємодії	Основні напрями співпраці	Практичні механізми реалізації
	центром протидії гібридним загрозам (Гельсінкі)	доказами, імплементація стандартів e-evidence у практику досудового розслідування

Джерело: сформовано автором на основі [7, с. 125–126; 8, с. 108–109; 9, с. 344–345; 10, с. 292–293; 11, p. 142–144; 13]

На міжвідомчому рівні СБУ координує дії з Офісом Генерального прокурора та БЕБ під час розслідування злочинів, пов'язаних з фінансуванням збройної агресії. Так, у 2025 році СБУ спільно з БЕБ викрила директора київського банку, який через криптовалютні перекази забезпечував фінансування російських сил, використовуючи анонімні електронні рахунки. Цей випадок був показовим для вдосконалення процедур ідентифікації цифрових транзакцій та залучення фінансових експертів у досудовому процесі [27]. На процесуальному рівні важливим залишається питання інтеграції цифрових доказів у кримінальне провадження. Завдяки взаємодії СБУ з урядовою командою CERT-UA у 2025 році вдалося запобігти масштабним кібератакам типу WRECKSTEEL, спрямованим на системи державного управління. Отримані технічні артефакти – журнали подій, IP-логування, фрагменти шкідливого коду – були оформлені як електронні докази з дотриманням стандартів e-evidence chain, що забезпечило їхню процесуальну допустимість [28]. На судовому рівні СБУ бере участь як експертний суб'єкт у підтвердженні автентичності цифрових матеріалів, що передаються через систему «Е-Суд». Зокрема, у справах про державну зраду у 2024–2025 роках суди почали приймати технічні висновки фахівців СБУ як доказову базу, що зменшило час розгляду та підвищило ефективність правосуддя. Нарешті, міжнародна взаємодія розвивається через участь СБУ у спільних операціях з Europol та Eurojust, що дає змогу отримувати цифрові сліди із закордонних серверів, зокрема тих, де розміщуються центри управління кібератаками. Такі спільні операції (Eastwood та програма Ради Європи CyberUA) сприяють гармонізації українських процедур доказовості з європейськими правовими стандартами [29]. Ці механізми діють не як ізольовані інституційні блоки, а як

єдина інтегрована екосистема доказового забезпечення, у якій міжвідомча координація, технічна експертиза, процесуальна легітимність і міжнародна співпраця формують стійку архітектуру протидії гібридним загрозам у кримінальному процесі.

Водночас використання матеріалів оперативно-розшукової та контррозвідувальної діяльності у кримінальному процесі України супроводжується системним конфліктом між цілями безпеки та принципами змагальності й правової визначеності [5, с. 179–180; 8, с. 105–106]. Основна проблема полягає у трансформації засекречених результатів негласних заходів у допустимі докази [9, с. 339–340]. Процесуальне законодавство не визначає єдиного алгоритму легалізації таких матеріалів, що призводить до фрагментарності практики: суди по-різному тлумачать належність аналітичних довідок, оперативних звітів або цифрових артефактів до доказової бази [7, с. 609]. Ця невизначеність підсилює ризик вибіркового застосування норм і фактичного переважання оперативного інтересу над гарантіями справедливого суду [8, с. 108–109]. Не менш проблемною є ситуація з верифікацією цифрових доказів. Відсутність єдиних протоколів електронної трасології, незалежних експертних центрів і чітких стандартів збереження метаданих створює простір для маніпуляцій та заперечування автентичності [5, с. 181; 11, p. 142–143]. Нерідко це призводить до того, що докази, отримані в межах контррозвідувальної діяльності, формально визнаються допустимими, але не набувають переконливої доказової сили [9, с. 344–345]. Значущою є і колізія між державною таємницею та правом сторони захисту на доступ до інформації [12, p. 100–101]. Судова практика має тенденцію до обмеження обсягу розсекречених матеріалів, що фактично позбавляє захисників можливості перевіряти правдивість даних і підриває принцип рівності сторін [8, с. 110; 13]. Це спричиняє порушення балансу між інтересами національної безпеки та верховенством права [6, с. 225–226].

ISSN: 3041-2110

Таким чином, оптимізація діяльності СБУ у сфері протидії гібридним загрозам вимагає системного вдосконалення законодавчої, процесуальної та організаційної основ її функціонування. Передусім доцільним є оновлення Закону України «Про Службу безпеки України» з урахуванням європейських стандартів парламентського контролю, підзвітності та процесуальної автономії. Необхідно чітко визначити співвідношення між оперативно-розшуковою, контррозвідувальною та досудово-слідчою діяльністю СБУ, щоб уникнути дублювання повноважень з Національною поліцією та БЕБ. У контексті кримінального процесу потребує конкретизації статус СБУ як органу досудового розслідування. Одночасно доцільно законодавчо розмежувати компетенцію між контррозвідувальними підрозділами, що здійснюють збирання інформації, та слідчими, які її процесуально оформлюють. Така практика підвищить доказову чистоту матеріалів, отриманих у результаті негласних заходів, і мінімізує ризики оскарження доказів у суді. Для забезпечення процесуальної визначеності та прозорості доказових процедур необхідно створити єдину національну систему цифрової верифікації доказів за принципом e-evidence chain, інтегровану з платформами «Трембіта» та «Е-Суд». Її функцією має бути автоматична фіксація всіх дій зі збирання, передавання й використання доказів із забезпеченням електронного журналу доступу. Це гарантуватиме збереження цифрової цілісності та відповідність доказів стандартам Ради Європи. У сфері кадрової та інституційної політики доцільно запровадити постійні програми міжвідомчої підготовки слідчих, прокурорів і судових експертів у напрямі кібербезпеки, цифрової криміналістики та прав людини. Спільна сертифікація таких програм під егідою Ради Європи або Європолу підвищить довіру до національної юстиції та зміцнить міжнародне співробітництво. Крім того, варто розвивати інституційні механізми демократичного нагляду за діяльністю СБУ, зокрема створити незалежну наглядову раду з представників парламенту, судової влади та громадянського суспільства з правом доступу до узагальненої

 ISSN: 3041-2110

інформації про результати оперативно-розшукової діяльності. Така система балансу влади сприятиме збереженню ефективності контррозвідувальних заходів, не порушуючи при цьому принципів верховенства права та захисту прав людини. Загалом запропоновані заходи спрямовані на перехід від реактивної до проактивної моделі національної безпеки, у якій СБУ буде не лише органом реагування, а інтегрованим елементом системи стратегічної стійкості держави перед гібридними загрозами.

Висновки. У результаті проведеного дослідження визначено, що СБУ є основною інституцією державного механізму протидії гібридним загрозам у кримінальному процесі, поєднуючи функції контррозвідки, досудового розслідування, аналітичного оброблення даних і кіберзахисту. Встановлено, що гібридний характер злочинів зумовлює потребу в оновленні доказових стандартів, орієнтованих не лише на фіксацію фізичних дій, а й на перевірку цифрових слідів, інформаційних впливів і фінансових потоків. Серед основних проблем виокремлено фрагментарність законодавчого регулювання повноважень СБУ, невизначеність процедури легалізації матеріалів оперативно-розшукової діяльності, відсутність єдиних правил цифрової верифікації доказів та колізію між режимом секретності та правом на захист. Додатковим обмеженням залишається недостатня інтеграція національної практики у європейський простір правосуддя. Рекомендовано оновити Закон України «Про Службу безпеки України» з чітким визначенням процесуального статусу СБУ, створити єдину систему e-evidence chain для верифікації цифрових доказів, розвивати міжвідомчу підготовку кадрів у сфері кібербезпеки та прав людини, зокрема запровадити незалежний механізм парламентського і громадського контролю. Перспективи подальших досліджень пов’язані з формуванням науково обґрунтованої моделі безпеково-процесуальної юстиції, що б забезпечувала баланс між ефективністю контррозвідувальних дій, верховенством права та захистом прав людини в умовах гібридної агресії.

ISSN: 3041-2110

Список використаних джерел

1. Лисянський П. Л. Регіональний сепаратизм в Україні: шляхи вирішення та механізми протидії : дис. докт. філос., Одеса, 2023. 274 с. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/3a2edc05-98f4-4fb1-b7e5-2039fc6ef3df/content (дата звернення: 12.06.2025).

2. Лисянський П. Діяльність політичних партій РФ на тимчасово окупованих територіях України як інструмент експансіонізму РФ. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2024. Вип. 2, № 19. С. 243–259. DOI: https://doi.org/10.29038/2524-2679-2024-02-243-259.

3. Тимчишин А. М. Генезис наукових уявлень про спеціальні знання у забезпеченні діяльності органів кримінальної юстиції. *Актуальні питання діяльності підрозділів кримінальної поліції:* зб. матеріалів Всеукр. наук.-практ. конф. (м. Кропивницький, 14 квітня 2023 року). Кропивницький: ДонДУВС, 2023. С. 45–48. URL: https://dnuvs.ukr.education/wp-content/uploads/2023/06/zbirnyk_materialiv_konferencziyi_ord_ta_ib_14_04_2023.pdf#page=46 (дата звернення: 12.06.2025).

4. Тимчишин А. М. Використання криміналістичних даних для розробки стратегій протидії воєнній агресії в секторі енергетичної безпеки. *Національна безпека: загрози та виклики:* матеріали всеукр. наук.-педагог. підвищення кваліф. (1 квітня – 12 травня 2024 року). Львів – Торунь : Liha-Pres, 2024. С. 212–216. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/22907/1/%D0%90dvanced_training_UzhNU.pdf#page=212 (дата звернення: 12.06.2025).

5. Метелев О. П., Коваленко Є. В. До питання використання у кримінальному процесі цифрової інформації, отриманої під час контррозвідувальної та оперативно-розшукової діяльності. *Науковий вісник Ужгородського університету: серія Право.* 2023. Т. 2, № 80. С. 177–182. DOI: https://doi.org/10.24144/2307-3322.2023.80.2.27.

6. Миргород В. В. Діяльність Служби безпеки України в контексті національної безпеки. *Науковий вісник Ужгородського національного університету. Серія Право.* 2024. Т. 2, № 82. С. 222–227. DOI: https://doi.org/10.24144/2307-3322.2024.82.2.35.

7. Козар В. В. Система суб'єктів протидії кримінальним правопорушенням в Україні та особливості їх адміністративно-правового статусу. *Вісник Кримінологічної асоціації України*. 2023. Вип. 30, № 3. С. 603-612. DOI: https://doi.org/10.24144/2307-3322.2025.89.3.49.

8. Погорецький М. М. Права і свободи людини в діяльності Служби безпеки України: питання гарантій. *Вісник кримінального судочинства.* 2021. № 3–4. С. 100–111. DOI: https://doi.org/10.17721/2413-5372.2021.3-4/100-111.

9. Герасименко О. М., Невмержицький С. М. Припинення Службою безпеки України кримінальних правопорушень на об'єктах критичної інфраструктури як складник системи протидії: теоретичний та правовий аспекти. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. Т. 3, №. 89. С. 335–347. DOI: https://doi.org/10.24144/2307-3322.2025.89.3.49.

10. Балан М. Взаємодія слідчого та інших суб'єктів кримінального провадження при розслідуванні порушень державного кордону України. *Цивільне право і процес.* 2020. № 3. С. 290–295. DOI: https://doi.org/10.32849/2663-5313/2020.3.48.

11. Yevtukh S. The Security Service of Ukraine: key operations and challenges during the full-scale russian-Ukrainian war. *Military Science.* 2025. Vol. 2, № 4. P. 137–147. DOI: https://doi.org/10.62524/msj.2024.2.4.12.

12. Orlovskyi R. S., Kozak V. M. Criminal law protection of state secrets in the context of hybrid warfare: a comparative analysis of Ukraine and the European union. *Kriminologija & socijalna integracija: časopis za kriminologiju, penologiju i poremećaje u ponašanju.* 2025. Vol. 33, № 1. P. 85–106. DOI: https://doi.org/10.31299/ksi.33.1.5.

13. Kryvytskyi Y., Kuznetsova L., Chekaliuk V., Maidaniuk I., Khriapynskyi A. The legal system reform of Ukraine in the context of EU integration and hybrid threats. *Sapienza: International Journal of Interdisciplinary Studies.* 2024. Vol. 5, № 4. Article e24077. DOI: https://doi.org/10.51798/sijis.v5i4.879.

14. СБУ викрила мережу інтернет-пропагандистів РФ у кількох областях України. *Detector Media*: вебсайт. 2023. URL: https://detector.media/infospace/article/210541/2023-04-26-sbu-vykryla-merezhu-internet-propagandystiv-rf-u-kilkokh-oblastyakh-ukrainy (дата звернення: 12.06.2025).

15. СБУ викрила мережу інтернет-агентів РФ у п’яти регіонах України. *ТСН:* вебсайт. 2023. URL: https://tsn.ua/ukrayina/sbu-vikrila-merezhu-internet-agentiv-rf-u-5-regionah-zaklikali-do-genocidu-ta-udariv-raketami-satana-2315257.html (дата звернення: 12.06.2025).

16. Russian spies behind cyberattack on Ukrainian power grid in 2022 – researchers. *Reuters:* вебсайт. 2023. URL: https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09 (дата звернення: 12.06.2025).

17. Ukraine says it thwarted Russian cyberattack on electricity grid. *Reuters*: вебсайт. 2022. URL: https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12 (дата звернення: 12.06.2025).

18. СБУ заблокувала схему фінансування російського криміналу. *Ukrinform:* вебсайт. 2024. URL https://www.ukrinform.ua/rubric-society/3219173-sbu-zablokuvala-shemu-finansuvanna-rosijskogo-kriminalu.html (дата звернення: 12.06.2025).

19. Конституція України (1996, зі змінами). *Верховна Рада України:* вебсайт. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр (дата звернення: 12.06.2025).

20. Про Службу безпеки України: Закон України від 25.03.1992 р. № 2229-XII. *Верховна Рада України*: вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 12.06.2025).

21. Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI. *Верховна Рада України*: вебсайт. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 12.08.2025).

22. Про національну безпеку України: Закон України від 19.06.2003 р. № 964-IV. *Верховна Рада України*: вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 12.06.2025).

23. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Верховна Рада України*: вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 12.08.2025).

24. Convention on Cybercrime (Budapest Convention, 2001). *Council of Europe*: вебсайт. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (дата звернення: 12.06.2025).

25. Global operation targets NoName057(16) pro-Russian cybercrime network. *Europol:* вебсайт. 2023. URL: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network (дата звернення: 12.06.2025).

26. CyberUA: Support to cybersecurity, data protection and electronic evidence in Ukraine. *Council of Europe*: вебсайт. 2024. URL: https://www.coe.int/en/web/kyiv/cyberua (дата звернення: 12.06.2025).