**Кримінальний процес та криміналістика**

УДК 343.3(477)

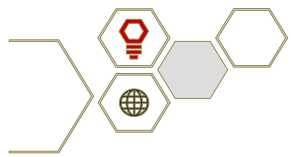
DOI <https://doi.org/10.5281/zenodo.17425822>**Роль Служби безпеки України в доказуванні злочинів проти держави****Гудима Віталій Валерійович,**

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: 02.07.2025 | Опубліковано: 25.07.2025

Анотація. Актуальність дослідження зумовлено необхідністю підвищення ефективності діяльності СБУ в доказуванні злочинів проти держави в умовах гібридної агресії, цифровізації та реформування системи кримінальної юстиції. Виявлено, що сучасні форми державної зради, шпигунства й диверсій мають складну інформаційно-аналітичну природу, що потребує оновлення правових, процесуальних і технічних механізмів фіксації й оцінювання доказів. Доведено, що від узгодженості дій СБУ з органами прокуратури та досудового розслідування залежить здатність держави забезпечувати законність і стабільність у сфері національної безпеки.

Мета статті полягає в науковому обґрунтуванні ролі СБУ в системі доказування злочинів проти держави, визначенні меж і змісту її процесуальних повноважень, аналізі практики використання матеріалів оперативно-розшукової та контррозвідувальної діяльності в кримінальному процесі, а також у формулюванні рекомендацій щодо вдосконалення правових та організаційних механізмів забезпечення національної безпеки.



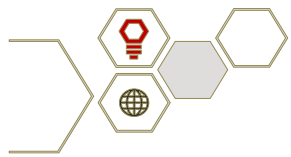
Методологія дослідження ґрунтується на системному, структурно-функціональному та порівняльно-правовому підходах, із використанням методів аналізу законодавства, судової практики, емпіричних даних СБУ та узагальнення міжнародного досвіду (СЕPOL, Eurojust, Ради Європи). Застосовано також аналітичні методи для оцінювання ефективності доказової діяльності та цифрових механізмів верифікації доказів.

Результати дослідження дали змогу встановити, що ключовими проблемами доказування злочинів проти держави є фрагментарність правового регулювання процесу легалізації оперативних матеріалів, невизначеність статусу СБУ як суб'єкта кримінального провадження, дублювання функцій з прокуратурою та відсутність єдиної системи цифрової трасології. Виявлено необхідність уніфікації процедур верифікації цифрових доказів і створення єдиного стандарту доказового менеджменту.

Висновки полягають у доведенні потреби створення єдиного процесуального стандарту легалізації матеріалів оперативного походження, розвитку цифрової криміналістики СБУ та впровадженні безпечного міжвідомчого обміну доказами. Підкреслено, що підвищення доказової спроможності СБУ сприятиме зміцненню правових гарантій і довіри до системи правосуддя.

Перспективи подальших досліджень пов'язані з розробленням концепції цифрової доказової інфраструктури України, гармонізацією національних стандартів із практикою ЄС, а також з оцінюванням впливу технологій штучного інтелекту на доказову діяльність органів безпеки.

Ключові слова: доказування, національна безпека, контррозвідувальна діяльність, допустимість доказів, цифрова криміналістика, процесуальні гарантії.



The role of the Security Service of Ukraine in proving crimes against the state

Vitaliy Hudyma,

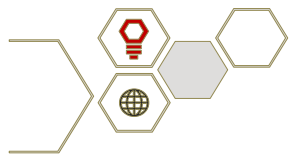
PhD in Law, Associate Professor, Department of Judiciary, Prosecutor's Office
and Advocacy, Lviv University of Business and Law, Lviv, Ukraine,

<https://orcid.org/0000-0001-6708-3910>

Abstract. The relevance of the study is determined by the growing need to enhance the efficiency of the Security Service of Ukraine (SSU) in preventing crimes against the state under conditions of hybrid aggression, digitalization, and reform of the criminal justice system. It has been revealed that modern forms of treason, espionage, and sabotage possess a complex information-analytical nature, which requires the modernization of legal, procedural, and technical mechanisms for the collection and evaluation of evidence. It has been proven that the coherence of the SBU's interaction with the prosecution and pre-trial investigation bodies directly affects the state's ability to uphold legality and stability in the sphere of national security.

The purpose of the article is to provide a scientific justification of the SSU's role in the system of proving crimes against the state, to define the scope and content of its procedural powers, to analyze the effectiveness of using materials from operational-search and counterintelligence activities in criminal proceedings, and to formulate recommendations for improving the legal and organizational mechanisms of national security assurance.

Research methodology is based on systemic, structural-functional, and comparative-legal approaches combined with analysis of legislation, judicial practice, empirical materials of the SSU, and the generalization of international experience (CEPOL, Eurojust, Council of Europe). Analytical and statistical methods were applied to assess the effectiveness of evidentiary activities and the use of digital verification technologies.



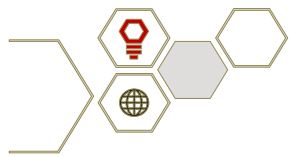
Research results indicate that the key problems of proving crimes against the state include the fragmented regulation of procedures for legalizing operational materials, the ambiguous status of the SSU as a subject of criminal proceedings, duplication of functions with the prosecution, and the absence of a unified system of digital traceability. The need to unify digital evidence verification procedures and to develop a standardized evidence management model has been identified.

Conclusions substantiate the necessity of creating a unified procedural standard for the legalization of operational materials, developing the SSU's digital forensics capacity, and establishing a secure inter-agency digital environment for evidence exchange. Strengthening the evidentiary capacity of the SSU is shown to be a prerequisite for improving legal guarantees and public trust in the justice system.

Prospects for further research include the development of a normative model of Ukraine's digital evidence infrastructure, the harmonization of national procedures with EU standards, and the assessment of the impact of artificial intelligence technologies on the evidentiary functions of security institutions.

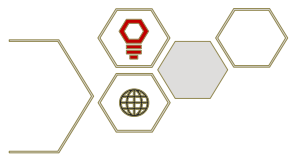
Keywords: evidence verification, national security, counterintelligence activity, admissibility of evidence, digital forensics, procedural safeguards.

Постановка проблеми. У сучасних умовах воєнного стану та тривалої збройної агресії російської федерації проти України діяльність Служби безпеки України (СБУ) у сфері доказування злочинів проти держави набуває особливої актуальності. Зміна характеру загроз – від традиційних шпигунських і терористичних актів до складних гібридних форм диверсій, інформаційного впливу й колабораційної діяльності – вимагає нового рівня процесуальної адаптивності та аналітичної компетентності органів безпеки. Проблема полягає в необхідності забезпечення балансу між оперативно-розшуковою діяльністю, яка передбачає використання засекречених методів, та вимогами кримінального процесу щодо допустимості, належності й



достовірності доказів. У практиці розслідування злочинів проти основ національної безпеки нерідко виникають колізії між інтересами державної таємниці й принципами змагальності, гласності та правової визначеності судового розгляду. Відсутність чітко унормованого механізму трансформації результатів контррозвідувальної діяльності в процесуально допустимі докази призводить до неоднакової судової практики, що створює ризики скасування вироків та зниження ефективності державної безпекової політики. З огляду на це дослідження ролі СБУ в доказуванні злочинів проти держави має важливе наукове й практичне значення, оскільки спрямоване на вдосконалення механізмів інтеграції спеціальних знань, цифрової експертизи та аналітичної розвідки в кримінальний процес, що є ключовою умовою підвищення спроможності держави до протидії сучасним загрозам її суверенітету та територіальній цілісності.

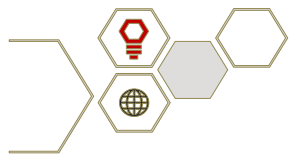
Аналіз останніх досліджень і публікацій. Аналіз наукових праць, присвячених ролі Служби безпеки України в доказуванні злочинів проти держави, дає змогу виокремити чотири основні напрями. Перший напрям стосується процесуально-правових і криміналістичних аспектів доказової діяльності СБУ. Зокрема, Г. А. Аль-Абабнех (Н. А. Al-Ababneh) та співавтори [1] доводять ефективність застосування технологій Big Data для виявлення економічних злочинів у публічних закупівлях, що безпосередньо співвідноситься з аналітично-доказовими функціями СБУ у сфері протидії фінансовим загрозам державній безпеці. Роль СБУ в системі національної безпеки аналізує В. В. Миргород [2], визначаючи, що належне документування злочинів проти держави потребує поєднання контррозвідувальних, криміналістичних і процесуальних інструментів. Водночас А. О. Гарницька і М. В. Соколовський [3] досліджують особливості доказової діяльності під час досудового розслідування терористичних правопорушень, акцентуючи на необхідності вдосконалення механізмів фіксації та легалізації електронних доказів. В. О. Ходанович і В. В. Колонюк



[4] визначають можливості судових експертиз у протидії злочинам проти інформаційної безпеки, підкреслюючи потребу технологічної інтеграції експертних і оперативно-розшукових даних у доказову базу кримінального процесу. Перспективним напрямом подальших досліджень є розроблення єдиних методичних стандартів використання результатів оперативної діяльності СБУ як належних і допустимих доказів.

Другий науковий напрям охоплює теоретико-концептуальні та політико-правові засади безпекової діяльності держави в умовах війни. У цьому аспекті П. Л. Лисянський [5] досліджує процеси мілітаризації суспільства в країнах пострадянського простору як чинник дестабілізації безпеки Європейського регіону, наголошуючи, що ефективна протидія цим тенденціям потребує зміцнення контррозвідувального потенціалу СБУ та формування інтегрованої системи аналітичного реагування на загрози. У подальшій праці П. Л. Лисянський [6] розкриває діяльність профспілкових організацій російської федерації на тимчасово окупованих територіях України як форму політичного експансіонізму, яка має бути належним чином документована СБУ в межах кримінальних проваджень. А. М. Тимчишин [7] обґрунтовує необхідність використання криміналістичних даних у процесі розроблення стратегій протидії воєнній агресії в енергетичному секторі, що забезпечує аналітичну підтримку процесу доказування злочинів проти держави. Узагальнення цього напрямку свідчить, що подальші дослідження мають бути спрямовані на створення єдиної концепції правового режиму доказування злочинів проти суверенітету України в умовах гібридної війни.

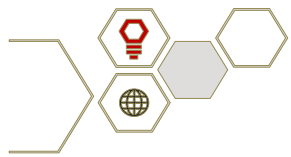
Третій напрям досліджень охоплює організаційно-правові та інституційні аспекти діяльності СБУ у сфері доказування. О. І. Хороновський [8] аналізує роль СБУ в протидії діяльності транснаціональних організованих злочинних угруповань, що діють проти об'єктів критичної інфраструктури, визначаючи її як провідного суб'єкта міжвідомчої взаємодії у сфері безпеки. Дотримання прав і свобод людини в діяльності СБУ досліджує



М. М. Погорецький [9], наголошуючи на важливості запровадження процесуального контролю та гарантій дотримання принципу змагальності в доказуванні. Узагальнення цього напрямку свідчить, що подальші дослідження мають бути спрямовані на створення внутрішньої системи управління доказовими процесами СБУ, яка забезпечить баланс між ефективністю оперативних дій і дотриманням прав людини.

Четвертий науковий напрям має міжнародно-правовий і порівняльний вимір діяльності СБУ у сфері доказування. С. Євтух (S. Yevtukh) [10] аналізує ключові операції та виклики, з якими СБУ стикається в перебігу повномасштабної російсько-української війни, підкреслюючи необхідність розширення міжнародного співробітництва у сфері контррозвідки та обміну доказовою інформацією. Правові характеристики воєнних злочинів досліджують Г. Ю. Бершов (H. Y. Bershov) та співавтори [11], визначаючи потребу адаптації українських процедур доказування до стандартів міжнародного гуманітарного права. Водночас Л. Рибальченко (L. Rybalchenko) та співавтори [12] розглядають економічну злочинність як чинник підриву державної безпеки, акцентуючи на ролі СБУ у виявленні фінансових зв'язків, що підтримують агресивні дії проти України. А. Вознюк (A. Vozniuk) [13] аналізує українську модель кримінально-правової протидії діяльності кримінальних авторитетів, визначаючи СБУ ключовим суб'єктом у документуванні транснаціональної злочинності. Узагальнення цього напрямку засвідчує, що перспективи подальших досліджень полягають у розробленні моделей міжнародної кооперації СБУ з правоохоронними структурами ЄС і НАТО з метою уніфікації стандартів доказування злочинів проти держави і підвищення їх легітимності в міжнародному правовому полі.

Виділення не вирішених раніше частин загальної проблеми. Попри наявні напрацювання у сфері кримінального процесу, залишаються нерозв'язаними питання визначення процесуального статусу СБУ, алгоритмів легалізації матеріалів оперативно-розшукової та контррозвідувальної



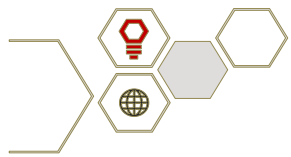
діяльності, а також інтеграції цифрових доказів у судову практику. Не досить розроблено механізми балансу між режимом державної таємниці та процесуальними гарантіями прав людини, а також стандарти міжвідомчої взаємодії під час документування злочинів проти держави. Запропоноване дослідження спрямоване на заповнення цих прогалин шляхом обґрунтування єдиного процесуального стандарту доказування, розроблення моделі інтегрованої доказової екосистеми СБУ та формування рекомендацій щодо вдосконалення цифрової експертизи й аналітичних механізмів перевірки доказів відповідно до міжнародних стандартів.

Формулювання цілей статті (постановка завдання). Мета статті полягає в науковому обґрунтуванні ролі СБУ в доказуванні злочинів проти держави, визначенні меж і змісту її процесуальних повноважень, аналізі ефективності використання матеріалів оперативно-розшукової та контррозвідувальної діяльності в кримінальному процесі, а також у формуванні рекомендацій щодо вдосконалення правових і організаційних механізмів забезпечення національної безпеки.

Для досягнення мети поставлено такі завдання:

- 1) визначити концептуальні засади та процесуальну роль СБУ в доказуванні злочинів проти держави в умовах гібридних загроз;
- 2) проаналізувати правові механізми збирання, перевірки й легалізації доказів та практику взаємодії СБУ з органами досудового розслідування і прокуратурою;
- 3) виявити проблеми допустимості доказів і сформулювати рекомендації щодо вдосконалення доказової діяльності СБУ відповідно до міжнародних стандартів.

Виклад основного матеріалу дослідження. Доказування злочинів проти держави є складним багаторівневим процесом, що поєднує правові, аналітичні та оперативні компоненти, інтегровані в систему національної безпеки. У контексті сучасних гібридних загроз, що характеризуються

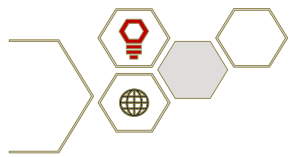


поєднанням воєнних, інформаційних, кібернетичних, економічних і психологічних впливів, традиційні підходи до збирання та оцінювання доказів утрачають ефективність. Це зумовлює необхідність переосмислення концептуальних засад доказування злочинів проти держави, де ключову роль відіграє СБУ як спеціальний суб'єкт із подвійним статусом – органу безпеки та сторони кримінального провадження. Її діяльність не обмежується виконанням слідчих дій, а включає аналітичне прогнозування, розвідувально-контррозвідувальні операції, інформаційно-технічне забезпечення та превентивні заходи, що формують основу доказового процесу. Саме СБУ забезпечує первинну ідентифікацію ознак державної зради, терористичної діяльності, диверсії чи шпигунства, а також фіксацію матеріальних і цифрових слідів злочину в умовах оперативної невизначеності (табл. 1).

Таблиця 1

Концептуальні засади доказування злочинів проти держави в умовах гібридних загроз

Параметр	Традиційний підхід	Сучасний (гібридний) підхід	Роль СБУ
Мета доказування	Установлення факту вчинення злочину	Виявлення комплексного впливу на державну безпеку, включно з латентними загрозами	Формування аналітичної моделі загрози на основі інтеграції оперативних і цифрових даних
Джерела доказів	Свідчення, документи, речові докази	Цифрові артефакти, метадані, результати кіберрозвідки, інформаційно-психологічні впливи	Використання технічних каналів збору інформації та аналітичних платформ
Методи отримання	Слідчі дії, запити, експертизи	Негласні заходи, OSINT, SIGINT, кібермоніторинг, аналітичні звіти	Проведення контррозвідувальних і кібероперацій із процесуальним документуванням
Оцінювання доказів	Формально-юридичний підхід	Комбінований: правовий, інформаційно-аналітичний, криміналістичний	Інтеграція експертного аналізу й цифрової трасології в процес доказування
Кінцева мета	Підтвердження складу злочину	Установлення механізму дії гібридної загрози та її суб'єктів	Формування доказового комплексу для притягнення до відповідальності осіб,



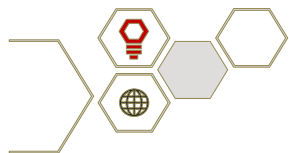
			що діють в інтересах держави-агресора
--	--	--	---------------------------------------

Джерело: сформовано автором на основі [5, с. 30–32; 6, с. 52–53; 7, с. 213–214; 2, с. 223–224; 10, р. 139–141; 11, р. 44–45]

Ці параметри на практиці відображають логіку дій СБУ – від аналітичного виявлення злочину до його процесуального доведення. На етапі формування аналітичної моделі загрози СБУ поєднує фінансову розвідку, кібермоніторинг і криміналістичний аналіз. Так, у січні 2024 року служба викрила масштабну схему розкрадання понад 1,5 млрд грн, призначених для закупівлі мінометних снарядів: виявлено транзакції через підставні фірми в Хорватії та Чехії, вилучено електронні листування та платіжні ордери, що стали основою доказування у справі [14].

Джерела доказів дедалі частіше мають цифрову природу. У 2023 році СБУ нейтралізувала агентурну мережу, яка передавала дані про ЗСУ через зашифровані месенджери. Під час обшуків вилучено понад 40 електронних носіїв – ноутбуки, сервери, смартфони, де знайдено координати військових об'єктів, передані ворогу. Після цифрової експертизи ці матеріали стали доказами державної зради [15]. Значна частина доказової бази нині формується за допомогою технічних засобів, як-от перехоплення трафіку, хешування, криптографічна перевірка цілісності даних. За даними Генпрокуратури, у 2023–2024 роках СБУ передала до суду понад 700 справ щодо злочинів проти держави, і понад 60% із них завершилися обвинувальними вироками [16]. Це демонструє, що технологічна доказовість і аналітична точність стають визначальними чинниками успіху в протидії злочинам проти держави.

Процедура збирання, перевірки й легалізації доказів, отриманих СБУ, має складну нормативну природу, оскільки поєднує елементи кримінального процесуального, оперативно-розшукового та контррозвідувального права. На відміну від інших органів досудового розслідування, СБУ функціонує в умовах режиму секретності, де результати оперативної діяльності часто не

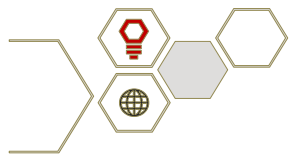


можуть бути безпосередньо використані як докази. Тому процес легалізації таких матеріалів вимагає юридичного «перекодування» – від первинного збору інформації до її процесуального оформлення відповідно до вимог Кримінального процесуального кодексу України (КПК) (зокрема, статей 84, 99, 246, 252, 257) [17], Закону України «Про оперативно-розшукову діяльність», Закону України «Про контррозвідувальну діяльність» [18] та Закону України «Про Службу безпеки України» [19]. Ці акти закріплюють принципи допустимості, верифікації та документальної фіксації доказів, проте не створюють єдиного алгоритму перетворення оперативних матеріалів у процесуальні докази, що зумовлює потребу в комплексному підході, який СБУ напрацьовує на практиці (табл. 2).

Таблиця 2

Нормативно-процедурні механізми легалізації доказів, отриманих СБУ

Етап	Правовий зміст	Основні нормативні джерела	Механізми реалізації на практиці	Ключові виклики
Збирання	Отримання інформації під час негласних дій – спостереження, прослуховування, аналіз цифрових каналів	Закон України «Про оперативно-розшукову діяльність», Закон України «Про контррозвідувальну діяльність»	Використання технічних засобів SIGINT, агентурних джерел, OSINT-аналітики	Узгодження дій із прокуратурою, обмеження щодо розсекречення
Фіксація	Формалізація результатів спостереження у службових документах	КПК України (ст. 104, 252), Закон України «Про СБУ»	Оперативні рапорти, акти, відеозаписи, фототаблиці	Невідповідність процесуальній формі, потреба в судовому дозволі
Перевірка	Експертна оцінка достовірності та цілісності отриманих даних	КПК України (ст. 101, 242)	Комп'ютерно-технічна, лінгвістична, криптографічна експертиза	Установлення автентичності цифрових файлів
Легалізація	Офіційне долучення оперативних матеріалів до кримінального провадження	КПК України (ст. 99, 257), Закон України «Про прокуратуру»	Протокол передачі, прокурорська санкція, судова ухвала	Ризик утрати доказової сили через формальні порушення
Оцінення судом	Визнання доказів	КПК України (ст. 85, 94)	Допит експертів, огляд	Контроль за процесуальною

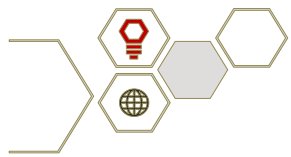


	належними та допустимими		носіїв, оцінювання ланцюга зберігання	чистою походження доказів
--	--------------------------	--	---------------------------------------	---------------------------

Джерело: сформовано автором на основі [3, с. 1072–1073; 4, с. 155–156; 12, р. 80–81; 17–21]

У практиці СБУ ці механізми працюють як багаторівнева система правової легітимації оперативної інформації. Наприклад, у справі 2024 року про передачу секретних даних через зашифровані месенджери було проведено багатоступеневу процедуру перевірки. Первинні результати контррозвідувального моніторингу були зафіксовані у внутрішньому акті, після чого прокурор звернувся до суду із клопотанням про їх долучення. Експерти СБУ здійснили криптографічне хешування файлів, створивши цифровий «ланцюг збереження доказів». Саме цей механізм забезпечив допустимість даних у суді, де вони були використані для доведення державної зради [22].

Інший показовий приклад стосується вербування українських військових у соціальних мережах. СБУ ідентифікувала понад 120 акаунтів, керованих із території окупованого Криму, які поширювали дезінформацію та пропонували співпрацю за грошову винагороду. Дані з серверів, отримані в співпраці з Державною службою спеціального зв'язку та захисту інформації, пройшли незалежну експертизу й були легалізовані як докази контррозвідувальної діяльності [23]. Обидва приклади показують, що легалізація доказів у сучасних умовах – це не лише формальна процедура, а технологічно й юридично складний процес, який перетворює аналітичні дані на процесуально стійку доказову базу. Сучасна правова модель СБУ демонструє поступову еволюцію від традиційного документування до системи цифрової трасології, де важливою є не лише змістова достовірність, а й підтверджена технічна цілісність даних. Це підсилює правову позицію держави у справах проти суб'єктів гібридної агресії, адже дозволяє



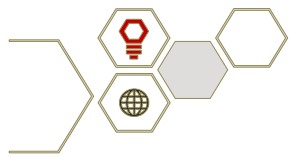
обґрунтовувати провину з використанням доказів, що відповідають як процесуальним, так і технологічним стандартам доказовості.

У системі доказування злочинів проти основ національної безпеки ефективна взаємодія СБУ з органами досудового розслідування й прокуратурою є ключовою умовою перетворення оперативної інформації на процесуально визнані докази. У законодавчому полі така співпраця закріплена нормами КПК України (зокрема ст. 36–41) [17], Закону України «Про прокуратуру» [21] та відповідними положеннями Закону України «Про Службу безпеки України» [20]. Проте на практиці вона часто супроводжується проблемами: затримками в передачі матеріалів, обмеженням прокурора в доступі до засекречених даних, нерівномірною участю СБУ в слідчих діях і різночитанням критеріїв допустимості доказів. Попри формальну визначеність повноважень, взаємодія на практиці набуває гібридного характеру, поєднуючи правові, аналітичні й організаційні елементи співпраці.

Таблиця 3

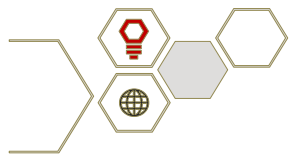
Практичні моделі взаємодії СБУ з прокуратурою та слідчими структурами в документуванні злочинів проти національної безпеки

Елемент взаємодії	Правова основа	Функціональний зміст	Практичне значення
Координація дій	КПК України (ст. 36–38), Закон «Про прокуратуру»	Узгодження плану розслідування, часових меж, обміну інформацією	Забезпечення єдиного алгоритму дій між СБУ, слідством і прокуратурою
Оперативне забезпечення	Закон України «Про СБУ» (ст. 24–25)	Проведення контррозвідувальних заходів, спостереження, кібермоніторинг	Створення первинної бази цифрових та матеріальних доказів
Процесуальне керівництво	КПК України (ст. 36, 37)	Санкціонування, контроль і координація дій досудового розслідування	Забезпечення процесуальної чистоти отриманих доказів
Експертна верифікація	КПК України (ст. 101, 242)	Перевірка достовірності цифрових, фінансових і технічних даних	Підтвердження автентичності доказів у судовому процесі
Представлення в суді	КПК України (ст. 85, 94)	Участь експертів СБУ, спільна підготовка позиції сторони обвинувачення	Підвищення доказової сили матеріалів і переконливості обвинувачення



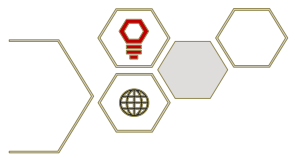
Джерело: сформовано автором на основі [1, с. 8865–8867; 2, с. 225–226; 4, с. 159–160; 8, с. 309–310; 13, р. 15–16; 17; 20; 21]

На практиці взаємодія СБУ з прокуратурою та органами досудового розслідування реалізується як безперервний процес обміну аналітичними, технічними та процесуальними даними. Спочатку СБУ збирає оперативну інформацію – від моніторингу цифрових каналів до контррозвідувального спостереження, після чого результати оформлюються в службові рапорти й передаються прокурору для легалізації. Такий підхід дозволяє зберегти неперервність доказового ланцюга – від моменту фіксації факту до його процесуальної оцінки в суді. Яскравим прикладом є справа, розслідувана в травні 2025 року, коли СБУ на Одещині затримала інженера оборонного заводу, який передавав російським спецслужбам креслення військової техніки. Оперативники задокументували факт передачі інформації через зашифровані канали зв'язку, а прокуратура забезпечила санкціонування обшуків і вилучення технічних носіїв. Отримані матеріали після експертизи було визнано судом належними доказами державної зради [24]. Подібна модель співпраці продемонстрована й у спільній операції СБУ та ДБР у 2024 році, коли вдалося зупинити спробу створення псевдодержавного утворення на півдні України. СБУ збрала та обробила понад 2,3 ТБ цифрових даних, зокрема повідомлення з месенджерів і транзакції фінансування, тоді як прокуратура забезпечила внесення відомостей до ЄРДР і підготовку повідомлень про підозру 12 фігурантам за статтями 109 і 111 КПК України [25]. Ще один результативний приклад – викриття в Кривому Розі коригувальника ракетних ударів рф. Оперативники СБУ зафіксували передачу координат через Telegram, після чого прокурори організували технічну експертизу смартфона. Хеш-коди цифрових файлів підтвердили незмінність даних і дозволили суду кваліфікувати ці відомості як допустимі цифрові докази [26]. Таким чином, сучасна модель взаємодії між СБУ, прокуратурою та органами досудового розслідування ґрунтується на поєднанні аналітичної



компетентності, технічної точності та процесуальної чіткості. Її результатом стає підвищення доказової надійності справ, що безпосередньо зміцнює спроможність держави реагувати на злочини проти її суверенітету та безпеки.

Правозастосовна практика СБУ у справах про злочини проти держави виявляє низку системних проблем, пов'язаних із допустимістю доказів, збереженням державної таємниці та дотриманням процесуальних гарантій. Основна проблема полягає в невизначеності статусу матеріалів оперативно-розшукової та контррозвідувальної діяльності. Значна частина доказів формується до моменту відкриття кримінального провадження, тому суди часто ставлять під сумнів їх допустимість через відсутність процесуального оформлення, передбаченого статтями 99 і 252 КПК України [17]. Нерідко результати негласних дій мають форму аналітичних довідок, технічних звітів або цифрових копій без чіткої ідентифікації джерела, що створює ризик відхилення таких доказів під час судового розгляду. Проблемним є також баланс між режимом державної таємниці та принципами відкритості судового процесу. Частина матеріалів у справах про державну зраду або шпигунство містить дані з обмеженим доступом, що унеможливорює їх повне дослідження стороною захисту [9, с. 106–107]. Це породжує колізію між необхідністю зберігати секретність і правом обвинуваченого на ознайомлення з доказами. Судова практика демонструє, що навіть часткове розсекречення інформації потребує тривалої процедури погодження, що затягує розгляд справ [5, с. 31–32]. Суттєвим викликом залишається верифікація цифрових доказів. Багато матеріалів, зібраних СБУ, мають електронну природу – метадані, скріншоти, відеозаписи, аудіофайли. Без належного фіксування ланцюга збереження (chain of custody) вони можуть бути поставлені під сумнів. Недостатній рівень технічної експертизи або відсутність стандартизованих процедур криптографічного підтвердження цілісності даних знижує їх доказову силу. Ще однією проблемою є дублювання повноважень між СБУ, прокуратурою та ДБР. Відсутність чіткої процедури визначення провідного органу у справах за

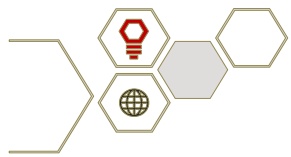


статтями 109–114 КПК України призводить до конкуренції юрисдикцій і ускладнює доказову координацію [7, с. 214–215; 13, р. 15–16]. Це створює ризик втрати безперервності доказового ланцюга, коли матеріали оперативного походження передаються без єдиної системи обліку чи хронології [2, с. 226].

Окремо слід відзначити правову колізію між забезпеченням безпеки держави та дотриманням процесуальних прав особи. У практиці СБУ іноді спостерігається надмірне покладання судів на оперативні матеріали без повного відтворення процесу їх отримання, що підриває принцип змагальності [9, с. 108; 11, р. 47]. Деякі судові рішення демонструють тенденцію до прийняття рапортів або зведених довідок як фактичних доказів, що суперечить вимогам щодо їх перевірки шляхом експертизи або допиту відповідних посадових осіб.

Удосконалення механізмів доказування злочинів проти держави передбачає комплексне оновлення правових, технологічних й інституційних засад діяльності СБУ відповідно до міжнародних стандартів доказового права. Насамперед необхідно запровадити єдиний процесуальний стандарт легалізації матеріалів оперативного походження, що визначатиме порядок їх трансформації в допустимі докази відповідно до статей 84, 99 і 252 КПК України [17]. Це забезпечить уніфікацію судової практики, зменшить ризик суб'єктивного трактування допустимості доказів і створить послідовний ланцюг їх збереження.

Важливим напрямом є розвиток цифрової експертизи та аналітичної спроможності СБУ. Формування спеціалізованих центрів цифрової криміналістики, які використовують алгоритми штучного інтелекту, OSINT-аналітику й криптографічні методи перевірки даних, підвищить точність і швидкість верифікації доказів. Такий підхід відповідає європейській практиці доказового аудиту й дозволить підтверджувати автентичність матеріалів незалежними технічними засобами.



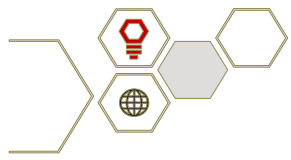
Необхідним є посилення міжвідомчої інтеграції між СБУ, прокуратурою, ДБР і Національною поліцією шляхом створення єдиного захищеного середовища обміну доказами. Використання протоколів шифрування, електронних підписів і автоматичного журналювання доступу забезпечить прозорість походження доказів і захист від маніпуляцій.

Слід також розширити систему незалежної експертної перевірки доказів, що ґрунтуватиметься на досвіді Eurojust і Ради Європи, де цифрові артефакти проходять подвійний аудит – технічний і процесуальний. Це зміцнить довіру судів та сторони захисту до доказової бази, сформованої СБУ.

Крім того, важливим є підвищення кадрової компетентності та інституційної спроможності служби. Запровадження навчальних програм із цифрової криміналістики, доказового права та міжнародних стандартів прав людини відповідно до підходів CEPOL [27] сприятиме формуванню нової культури доказового менеджменту.

Загалом, ефективне оновлення системи доказування має поєднувати технологічну точність, процесуальну чіткість і правову збалансованість. Реалізація цих заходів дозволить СБУ перейти від епізодичного до системного управління доказами, забезпечивши їх надійність, допустимість і відповідність міжнародним стандартам справедливого судового розгляду.

Висновки. Дослідження довело, що діяльність СБУ в доказуванні злочинів проти держави є ключовим складником системи національної безпеки, яка забезпечує легітимність і достовірність кримінального процесу в умовах гібридних загроз. Установлено, що доказування таких злочинів має інтегрований характер і поєднує контррозвідувальні, аналітичні та криміналістичні механізми, однак їх практична реалізація потребує оновлення нормативних і технологічних засад. Основними проблемами визначено відсутність єдиного процесуального стандарту легалізації матеріалів оперативного походження, невизначеність меж повноважень СБУ в кримінальному провадженні, дублювання функцій з прокуратурою та ДБР, а

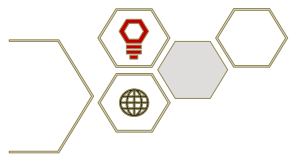


також нерозвиненість цифрової трасології доказів. Додаткові труднощі пов'язані з обмеженим доступом сторони захисту до засекречених матеріалів і нестачею кваліфікованих кадрів у сфері цифрової криміналістики. Запропоновано запровадити єдиний національний стандарт легалізації оперативних матеріалів відповідно до статей 84, 99 і 252 КПК України, створити центри цифрової криміналістики СБУ з використанням алгоритмів штучного інтелекту, забезпечити безпечний міжвідомчий обмін доказами та запровадити незалежну експертну перевірку за моделлю Eurojust. Важливим напрямом є підвищення професійної підготовки кадрів за підходами CEPOL, що передбачають інтеграцію європейських стандартів доказового менеджменту.

Перспективи подальших досліджень полягають у розробленні нормативної моделі цифрової доказової інфраструктури України, гармонізації національних процедур із практикою ЄС та формуванні демократичного контролю за діяльністю спецслужб у кримінальному процесі. Реалізація цих напрямів сприятиме зміцненню доказової спроможності СБУ та підвищенню довіри до системи правосуддя.

Список використаних джерел

1. Al-Ababneh H. A., Fedorchuk Y., Tymchyshyn A., Pishchenko G., Hrytsai S. The use of Big Data in the detection of economic crimes in public procurements. *Journal of Theoretical and Applied Information Technology*. 2024. Vol. 102, № 24. P. 8861–8871. URL: <https://www.jatit.org/volumes/Vol102No24/3Vol102No24.pdf>(дата звернення: 10.05.2025).
2. 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>



3. Гарницька А. О., Соколовський М. В. Особливості доказової діяльності під час досудового розслідування терористичних кримінальних правопорушень. *Аналітично-порівняльне правознавство*. 2025. № 2. С. 1071–1075. DOI: <https://doi.org/10.24144/2788-6018.2025.02.159>

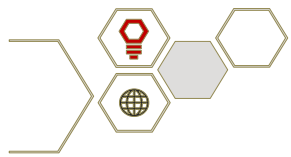
4. Ходанович В. О., Колонюк В. В. Сучасні можливості окремих видів судових експертиз у протидії злочинам проти інформаційної безпеки України. *Науковий вісник Ужгородського національного університету*. 2024. Т. 4, № 85. С. 154–161. DOI: <https://doi.org/10.24144/2307-3322.2024.85.4.22>

5. Лисянський П. Л. Процеси мілітаризації суспільства в країнах пострадянського простору як загроза безпековій ситуації в європейському регіоні. *Актуальні проблеми політики*. 2024. № 74. С. 27–38. DOI: <https://doi.org/10.32782/app.v74.2024.4>

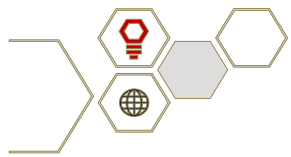
6. Лисянський П. Діяльність профспілкових організацій РФ на тимчасово окупованих територіях України, як інструмент посилення політики експансіонізму. *Наукові праці Міжрегіональної Академії управління персоналом*. *Політичні науки та публічне управління*. 2024. № 3(75). С. 51–57. DOI: [https://doi.org/10.32689/2523-4625-2024-3\(75\)-8](https://doi.org/10.32689/2523-4625-2024-3(75)-8).

7. Тимчишин А. М. Використання криміналістичних даних для розробки стратегій протидії війсьній агресії в секторі енергетичної безпеки. *Національна безпека: загрози та виклики* : матеріали всеукр. наук.-педагог. підвищення кваліф. (1 квітня – 12 травня 2024 р.). 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: 10.05.2025).

8. Хороновський О. І. Роль Служби безпеки України у протидії діяльності транснаціональних організованих злочинних угруповань на шкоду об'єктам критичної інфраструктури. *Актуальні проблеми вітчизняної юриспруденції*. 2024. № 1. С. 306–310. DOI: <https://doi.org/10.32782/2408-9257-2024-1-54>.



9. 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>.
10. 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>.
11. Bershov H. Y., Hrytenko O. A., Khashev V. H., Fialka M. I. Assessing and evaluating the general legal characteristics of war crimes: a basic necessity or a confused platform. *Ius Humani. Revista de Derecho*. 2022. Vol. 11, № 1. P. 43–60. DOI: <https://doi.org/10.31207/ih.v11i1.295>.
12. Rybalchenko L., Ryzhkov E., Ohrimenco S. Economic crime and its impact on the security of the state. *Philosophy, Economics and Law Review*. 2021. Vol. 2. P. 78–91. DOI: <https://doi.org/10.31733/2786-491X-2021-2-78-91>.
13. Vozniuk A. Criminal and legal counteraction to the activities of criminal authorities: The Ukrainian model. *Scientific Journal of the National Academy of Internal Affairs*. 2022. Vol. 27, № 1. P. 9–19. DOI: 10.56215/0122271.9
14. Ukraine's Security Service arrests five people accused of \$40m arms fraud. *The Guardian*: вебсайт. 2024. URL: <https://www.theguardian.com/world/2024/jan/28/ukraine-security-service-arrests-five-people-40m-arms-fraud-corruption-clampdown-ministry-of-defence-mortar-shells> (дата звернення: 10.05.2025).
15. Ukraine Uncovers Major Military Corruption Scam. *RFE/RL*: вебсайт. 2024. URL: <https://www.rferl.org/a/ukraine-military-corruption-arrests/32795104.html> (дата звернення: 10.05.2025).
16. СБУ не повинна розслідувати злочини. Статистика за 8 років. *Pravda*: вебсайт. 2020. URL: <https://www.pravda.com.ua/columns/2020/11/10/7272981/> (дата звернення: 10.05.2025).



17. Кримінальний процесуальний кодекс України від 01.08.2025 №4651-VI *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text> (дата звернення: 10.05.2025).

18. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text> (дата звернення: 10.05.2025).

19. Про контррозвідувальну діяльність. Закон України від 26.12.2002 №374-IV. *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/374-15#Text> (дата звернення: 10.05.2025).

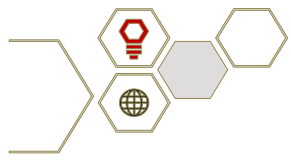
20. Про Службу безпеки України. Закон України від 25.03.1992 №2229-XII. *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/2229-12#Text> (дата звернення: 10.05.2025).

21. Про прокуратуру. Закон України від 14.10.2014 №1697-VII. *Верховна Рада України*: вебсайт. URL: <https://zakon.rada.gov.ua/laws/show/1697-18#Text> (дата звернення: 10.05.2025).

22. СБУ затримала посадовицю однієї із міськрад на Миколаївщині. Її підозрюють у держзраді. *Радіо Свобода*: вебсайт. URL: <https://www.radiosvoboda.org/a/news-sbu-mykolayivshchyna-ahentka-rf-miskrada/33399853.html> (дата звернення: 10.05.2025).

23. Колаборанти, агентурна мережа РФ і воєнні злочинці: в СБУ розповіли про роботу контррозвідки». *Укрінформ*: вебсайт. 2025. URL: <https://www.ukrinform.ua/rubric-society/3974346-kolaboranti-agenturna-mereza-rf-i-voenni-zlocinci-v-sbu-rozpovili-pro-robotu-kontrrozvidki.html> (дата звернення: 10.05.2025).

24. СБУ: інженера оборонного заводу затримали за підозрою в зборі даних для російських спецслужб. *Радіо Свобода*: вебсайт. URL: <https://www.radiosvoboda.org/a/news-sbu-inzhener-zatrymannia-pidozra-zbir-danykh/33420090.html> (дата звернення: 10.05.2025).



25. ДБР викрило багатомільйонну схему закупівлі техніки для війська. *Державне бюро розслідувань*: вебсайт. URL: <https://dbr.gov.ua/news/dbr-vikrilo-bagatomiljonnu-shemu-zakupivli-tehniki-dlya-vijska.-zbitki-perevishhuyut-64-miljoni-griven> (дата звернення: 10.05.2025).

26. СБУ затримала коригувальника ракетних ударів по Кривому Рогу. *Новини LIVE*: вебсайт. URL: <https://society.novyny.live/sbu-zaderzhala-korrektirovshchika-raketnykh-udarov-po-krivomu-rogu-49620.html> (дата звернення: 10.05.2025).

27. Training & Education. *CEPOL*: вебсайт. 2025. URL: <https://www.cepol.europa.eu/training-education> (дата звернення: 10.05.2025).