Секція Право	
УДК 342.951:351.746.1:355.271	
Дата першого надходження статті до видання	2026-04-15
Дата прийняття статті до друку після рецензування	2026-05-15
Дата публікації/оприлюднення	2026-05-15

Правові механізми протидії агентурній діяльності спецслужб рф в умовах воєнного стану

Канавець Юрій Петрович
старший викладач кафедри 4,
Національна академія Служби безпеки України
Київ, Україна, https://orcid.org/0009-0001-4682-684X

Анотація. Стаття досліджує правові механізми протидії агентурній діяльності спецслужб російської федерації в умовах міжнародного збройного конфлікту та воєнного стану в Україні. Головна мета – сформувати цілісну, доказово стійку та права-людинно орієнтовану модель протидії, яка поєднує кримінально-правові інструменти, контррозвідувальні повноваження, процесуальні стандарти щодо цифрових доказів, санкційні режими, а також міжнародно-правову кооперацію. На основі порівняльно-правового й догматичного аналізу норм Кримінального кодексу України (державна зрада, шпигунство, диверсія, колабораційна діяльність, пособництво агресорові), Кримінального процесуального кодексу (негласні слідчі дії), спеціальних законів про контррозвідку, державну таємницю, санкції та воєнний стан, а також практики ЄСПЛ і положень Будапештської конвенції, обґрунтовано вимоги законності, необхідності та пропорційності втручань у приватність. Стаття демонструє, що чинне законодавство України забезпечує базову криміналізацію ключових діянь, однак не містить уніфікованої дефініції «агентурної діяльності» як комплексного явища, яке включає вербування, інструктування, фінансування, конспірацію, логістику, передання звітності та сприяння диверсіям. Відсутність такої дефініції знижує передбачуваність кваліфікації, ускладнює статистичний облік і транскордонну взаємодію.

Запропоновано модель подвійного нагляду за НСРД: попередній судовий дозвіл з уніфікованим тестом пропорційності та постфактум парламентський огляд агрегованих показників із незалежним технічним аудитом інфраструктури перехоплення. У межах Будапештської конвенції деталізовано порядок оперативного збереження, доступу, збирання трафіку і перехоплення контенту у реальному часі з дотриманням технічних бенчмарків ETSI Lawful Interception.

У статті запропоновано інтегровану модель поєднання санкційного інструментарію з кримінальним провадженням: створення єдиного міжвідомчого реєстру пов'язаних осіб і активів (у т.ч. криптоактивів), синхронізація рішень про блокування/замороження з арештами і спецконфіскацією, прискорений судовий перегляд санкцій та розширення охоплення на посередників і логістичні ланки. Такий підхід позбавляє агентурні мережі ресурсів на ранніх етапах та полегшує міжнародну взаємодію з ЄС/США/Великою Британією.

Ключові слова: агентурна діяльність, контррозвідка, воєнний стан, державна зрада, шпигунство, міжнародне гуманітарне право, права людини, санкції, екстрадиція.

e-ISSN: 2786-586X

Legal Mechanisms for Countering the Covert Activities of Russian Special Services under Martial Law

Kanavets Yurii
Senior Lecturer of Department 4,
National Academy of the Security Service of Ukraine
Kyiv. Ukraine, https://orcid.org/0009-0001-4682-684X

Annotation. The article examines the legal mechanisms for countering the agent activities of the Russian Federation's special services in the context of an international armed conflict and martial law in Ukraine. The main goal is to form a holistic, evidence-based and human rights-oriented counteraction model that combines criminal law instruments, counterintelligence powers, procedural standards for digital evidence, sanction regimes, and international legal cooperation. Based on a comparative legal and dogmatic analysis of the norms of the Criminal Code of Ukraine (treason, espionage, sabotage, collaboration, aiding the aggressor), the Criminal Procedure Code (covert investigative actions), special laws on counterintelligence, state secrets, sanctions, and martial law, as well as the practice of the ECHR and the provisions of the Budapest Convention, the requirements for the legality, necessity, and proportionality of interference with privacy are substantiated. The article demonstrates that the current legislation of Ukraine provides for the basic criminalization of key acts, but does not contain a unified definition of "agent activity" as a complex phenomenon that includes recruitment, instruction, financing, conspiracy, logistics, reporting and facilitation of sabotage. The absence of such a definition reduces the predictability of qualifications, complicates statistical accounting and cross-border interaction.

A model of dual supervision of the NSRD is proposed: prior judicial authorization with a unified proportionality test and ex-post parliamentary review of aggregated indicators with an independent technical audit of the interception infrastructure. The Budapest Convention details the procedure for operational storage, access, traffic collection and interception of content in real time in compliance with the ETSI Lawful Interception technical benchmarks.

The article proposes an integrated model of combining sanctions tools with criminal proceedings: the creation of a single interdepartmental register of related persons and assets (including crypto-assets), synchronization of blocking/freezing decisions with arrests and special confiscation, accelerated judicial review of sanctions and expansion of coverage to intermediaries and logistical links. This approach deprives agent networks of resources at the early stages and facilitates international interaction with the EU/USA/UK.

Keywords: agent activity, counterintelligence, martial law, treason, espionage, international humanitarian law, human rights, sanctions, extradition.

ВСТУП

Актуальність проблеми. Агентурна діяльність спецслужб Російської Федерації – стійкий елемент гібридної війни проти України. Вона поєднує людський ресурс, кіберспроможність, фінансове забезпечення та інформаційно-психологічні операції. Воєнний стан загострює ризики для критичної інфраструктури, оборонних закупівель, органів влади та місцевого самоврядування. Правові механізми протидії мають забезпечувати швидке нейтралізування загроз без підриву верховенства права, із дотриманням ЄКПЛ та зобов'язань за міжнародним гуманітарним правом. [1]; [2]; [3] [4].

Аналіз останніх досліджень і публікацій. Дослідження НАТО та ЄС окреслюють агентурну діяльність як компонент гібридних загроз, наголошуючи на міжвідомчості заходів і стандартах доказування в кіберпросторі. Українська доктрина фокусується на кваліфікації держзради, шпигунства, диверсії та колабораціонізму, а також на процесуальних аспектах. Юриспруденція ЄСПЛ формує високі вимоги до законності

e-ISSN: 2786-586X

перехоплень і заборони провокації. Санкційне право різних країн пропонує дієві позасудові важелі із наступним судовим контролем [14].

Виділення невирішеної частини проблеми. Станом на сьогодні в українському правовому полі варто виділити:

1.Відсутність уніфікованого законодавчого визначення «агентурної діяльності» як комплексного складу з ознаками співпраці з іноземною спецслужбою.

2.Фрагментарні стандарти цифрових доказів і ланцюга збереження створюють ризики недопустимості.

3.Обмежена прозорість і зовнішній нагляд за НСРД у воєнний час.

4.Неповна інтеграція санкційних режимів із кримінальним провадженням та активами у криптосфері.

5.Недостатня уніфікація міжвідомчих SOP для HUMINT і кібероперацій з урахуванням прав людини. [21].

Мета статті – сформувати цілісну правову модель протидії агентурній діяльності рф у воєнний час, яка поєднує кримінально-правові інструменти, контррозвідувальні повноваження, санкційні режими та міжнародну кооперацію під контролем судових і парламентських інституцій.

Наукова новизна роботи полягає у наступному:

1. Вперше пропонується легальне визначення агентурної діяльності як окремого інституту з типологією дій і зв'язку з іноземною спецслужбою.
2. Розробляється матриця допустимості цифрових доказів, яка сумісна з Будапештською конвенцією та практикою ЄСПЛ.
3. Автором пропонується запровадження моделі подвійного нагляду за НСРД (судовий і парламентський) із публічними агрегованими звітами під час воєнного стану.
4. Інтегрується таргетоване санкціонування з кримінальним переслідуванням через єдиний реєстр пов'язаних осіб та активів. Практичне значення роботи полягає у підвищені доказової стійкості вироків у справах про шпигунство та держзраду; прискорення блокування фінансування агентурних мереж і конфіскації активів; зменшення ризиків порушень ст. 5, 6, 8 ЄКПЛ і пов'язаних програшів у ЄСПЛ; уніфікація міжвідомчої взаємодії та скорочення часу реагування.

Методологія дослідження.

Під час написання статті використано наступні методи дослідження та обробки інформації: порівняльно-правовий аналіз; аналіз норм КК, КПК, спеціальних законів, санкційних актів; функціональний аналіз контррозвідувальних процедур і судового контролю; емпірико-нормативний підхід до цифрових доказів та ланцюга збереження. Джерела отриманої інформації для роботи: нормативні акти України; міжнародні договори та стандарти; рішення ЄСПЛ; керівництва ENISA, ETSI, НАТО CCDCOE; офіційні санкційні переліки ЄС, OFAC, UK. До інструментів аналізу, які використані у процесі написання дослідження варто віднести індикатори оцінки ефективності. У процесі написання роботи виникли певні обмеження дослідження, зокрема обмежений доступ до закритої оперативної практики та технічних стандартів; неповнота відкритих статистичних даних про НСРД у воєнний час; ризики різноманітного трактування судової практики.

Результати

Державна зрада охоплює: перехід на бік ворога; шпигунство; надання допомоги державі-агресору; інформаційне, матеріальне, організаційне сприяння. Об'єкт – суверенітет, територіальна цілісність, обороноздатність, держбезпека. Суб'єкт – громадянин України; форми співучасті враховуються за ст. 26–30 КК [1]. У воєнний час підвищений суспільний інтерес виправдовує суворіші запобіжні заходи, але не знімає вимог доказовості умислу та причинного зв'язку. Докази: контакти з представниками

e-ISSN: 2786-586X

іноземної спецслужби; передання відомостей; виконання завдань; крипто- і готівкові транзакції; конспіративні канали зв'язку. Шпигунство (ст. 114 КК) спрямоване на збір/передачу відомостей, які становлять державну таємницю, або іншу секретну інформацію оборонного значення з метою передати іноземній державі/організації. Предмет – відомості з грифом секретності або фактичні дані, віднесені до держтаємниці за Законом «Про державну таємницю» [5]. Обов'язковий елемент – пряма або опосередкована іноземна спрямованість. Важлива межа з журналістською/експертною діяльністю: умисел і зв'язок з іноземною стороною мають бути доведені. [1],[5]. Несанкціоноване розголошення даних про оборону (ст. 114-2 КК) криміналізує поширення інформації про переміщення/розташування ЗСУ, об'єктів КІ, якщо це дозволяє їх ідентифікувати. Воєнний контекст посилює суспільну небезпечність.

Інша ситуація, диверсія (ст. 113 КК) – дії, спрямовані на ослаблення держави: вибухи, підпали, аварії на КІ, отруєння ресурсів, інші підривні акти. Часто поєднується з тероризмом (ст. 258 та пов'язані склади), якщо мета залякування населення/влади. Для кваліфікації важливий умисел на підрив обороноздатності або економічної безпеки. Колабораційна діяльність і пособництво агресорові (ст. 111-1, 111-2 КК) охоплює: публічне заперечення агресії; інформаційну підтримку окупаційної влади; участь в окупаційних адмініструваннях; передачу матеріальних ресурсів; організацію політичних заходів на користь агресора. На даний момент необхідна чітка індивідуалізація ролей, уникнення «колективної відповідальності» за ознакою громадянства або походження. [1]. Чинний КК інкримінує окремі діяння, але не дає системної категорії для «агентурної діяльності» як сукупності: вербування, інструктування, конспірація, фінансування, логістика, передання звітів, контрспостереження. Це ускладнює уніфікацію кваліфікації, статистику і міжнародну взаємодію. На практиці елементи розпорошуються між ст. 111, 114, 113, 258-3, 361–363-1 тощо. Доцільно ввести спеціальну норму/визначення у Закон «Про контррозвідувальну діяльність» із відсилкою у КК (примітка до глави IX Особливої частини), щоб легітимно охопити весь цикл агентурного впливу [1].

Закон «Про контррозвідувальну діяльність» визначає завдання, принципи, суб'єктів і засоби КРД; Закон «Про СБУ» – організацію, повноваження, гарантії законності. КПК регламентує негласні слідчі (розшукові) дії, коли мета – здобуття доказів у кримінальному провадженні. Вони між собою перетинаються, але мають різну процесуальну природу: матеріали КРД стають доказами лише після належної процесуалізації через КПК.. Ключові інструменти – аудіо-, відеоконтроль особи/місця; зняття інформації з транспортних телекомунікаційних мереж; арешт, огляд і виїмка кореспонденції; контроль за вчиненням злочину; встановлення місцезнаходження радіоелектронного засобу; спостереження; використання конфідентів та оперативних комбінацій (контрольовані зустрічі, «оперативна легенда»). У сфері кібер – негласний доступ до інформаційних систем за судовим дозволом; мережеве моніторингування й технічні закладки, що відповідають принципу мінімізації даних [2],. Кожна НСРД потребує ухвали слідчого судді з конкретизацією: особи/об'єкта; місця; строку; переліку технічних засобів; меж доступу до даних; підстав (обґрунтована підозра, неможливість досягти мети менш інвазивними засобами). Матеріали повинні забезпечувати автентичність і цілісність (хеш-суми, журнал доступів, протоколи з додатками). Порушення веде до виключення доказів («плоди отруйного дерева»), що відображено як у національній практиці, так і у стандартах ЄСПЛ [15].

Фактично виника необхідність уточнення процесуальних фільтрів. Зокрма пропонуються: уніфіковані шаблони клопотань із обов'язковим тестом трьох критеріїв (законна мета; необхідність; пропорційність); вимога вказувати категорії даних до збору і правила мінімізації третіх осіб; обов'язковий постфактум-аудит випадкових вибірок НСРД незалежним підрозділом прокуратури; процесуалізація матеріалів КРД через

e-ISSN: 2786-586X

швидкі «мости» у КПК (стандартизовані акти передачі, експертні висновки про збереження даних). Це зменшить ризики визнання недопустимості та позовів до ЄСПЛ. [21].

ДБР і Нацполіція виконують НСРД за своїми підслідностями; СБУ координує контррозвідувальні заходи щодо агентурної активності. Необхідні SOP для спільних груп для уникнення дублювання і конфліктів юрисдикцій.

Закон України «Про правовий режим воєнного стану» визначає правові підстави обмежень: комендантська година; особливий порядок в'їзду/виїзду; обмеження свободи пересування; контроль за комунікаціями; примусове відчуження майна; посилення охорони КІ; спеціальні режими доступу до об'єктів оборони. Ці інструменти опосередковано підтримують протидію агентурі, уможливлюючи швидке блокування каналів, логістики та переміщень підозрюваних осіб. [7]. Держава може відступити від окремих зобов'язань «у разі війни чи іншої надзвичайної ситуації, що загрожує життю нації», але: (1) обмеження мають бути суворо необхідними; (2) не можуть суперечити іншим міжнародним зобов'язанням; (3) не стосуються ядрових прав (право на життя з вузькими винятками, заборона катувань, рабства, зворотної сили кримінального закону). Навіть під час дерогацій зберігається судовий контроль, доступ до захисту та вимоги справедливого суду за ст. 5 і 6, у тій мірі, яка є сумісною з ситуацією надзвичайності. [ЄКПЛ ст. 15; практика ЄСПЛ: Lawless v. Ireland; A. and Others v. UK]. Обмеження перехоплень та НСРД у воєнний час не мають перетворюватися на невибіркове масове стеження. ЄСПЛ у справах Roman Zakharov v. Russia та Szabó and Vissy v. Hungary вимагає: чіткі і передбачувані норми; незалежний дозвільний орган; часові межі; зберігання і знищення даних за правилами; повідомлення особи ex post facto, коли це не шкодить слідству чи безпеці; ефективні засоби правового захисту. Вбудовування цих стандартів у воєнні процедури знижує ризик порушень ст. 8 ЄКПЛ [19]. Навіть у режимі воєнного стану залишаються: судовий дозвіл на обшук і НСРД (крім невідкладних випадків з наступною легалізацією); право на захисника; заборона провокації злочину; заборона катувань і нелюдського поводження; вимога допустимості та належності доказів; презумпція невинуватості; доступ до суду для оскарження запобіжних заходів. Будь-які відхилення мають бути прямо передбачені законом, часово обмежені і підлягати контролю. Ризики: розширене тлумачення «допомоги державі-агресору» до мирної опозиційної думки; використання санкційних механізмів для позасудового тиску без належного перегляду; «конвеєрні» НСРД без індивідуалізації підстав; недотримання ланцюга збереження цифрових доказів. Запобіжники: тест трирівневої пропорційності в кожному клопотанні; агреговані звіти про НСРД до парламентського наглядового органу; незалежний технічний аудит інфраструктури перехоплення; обов'язкове журналювання і хешування цифрових даних; процесуальні інструкції для легалізації матеріалів КРД у КПК. [21].

Відповідно до міжнародного законодавства, шпигунство не є воєнним злочином саме по собі, але шпигуни не користуються комбатантським імунітетом і підлягають національній юрисдикції за умови справедливого суду. Диверсії проти цивільних об'єктів можуть кваліфікуватися як воєнні злочини за сукупністю з нормами ІГП. Це накладає підвищені вимоги до розмежування цивільних і військових цілей у доказуванні та забезпечення процесуальних прав обвинувачених. [Додатковий протокол I, ст. 46; Коментарі МКЧХ].

Варто зазначити, українська модель має достатній набір матеріально-правових інструментів для переслідування агентурної діяльності, але бракує єдиного легального визначення, що структурує повний цикл агентурних дій. Процесуальна частина забезпечує судовий контроль НСРД, однак потребує уніфікації фільтрів, мінімізації даних і стандартів цифрової доказової дисципліни. Воєнний стан виправдовує вузькі, необхідні дерогації, але не скасовує ядра гарантій ЄКПЛ; інтеграція практики ЄСПЛ і Rule

e-ISSN: 2786-586X

of Law Checklist у процедури – ключ до правової стійкості вироків та мінімізації стратегічних ризиків у міжнародних судах [19].

Обговорення

Наявність процесуальної підстави для певних дій: ухвала слідчого судді з чітким визначенням об'єкта, видів даних, строків і технічних засобів; для невідкладних дій – наступна легалізація з обґрунтуванням неможливості попереднього дозволу [КПК гл. 21]. Відповідність міжнародним стандартам: конкретність цілей, мінімізація обсягу, часові межі та незалежний контроль. [18]. Територіальна і предметна юрисдикція: збір даних у транснаціональних провайдера/платформ – через MLAT, 24/7 мережу Будапештської конвенції або інші законні канали. [9]. Переконливе підтвердження, що дані походять з конкретного джерела і не змінені: форензічні образи (bit-by-bit), цифрові підписи провайдерів, супровідні листи (provider's declaration), вбудовані метадані. Технічні атрибути: хеш-суми (SHA-256/ SHA-512) з фіксацією часу, MAC-часи файлів, лог-файли систем аудиту. Незмінність від моменту вилучення до дослідження: контрольні хеші при кожному доступі; зберігання оригіналу офлайн у сейфі доказів; робота лише з верифікованими копіями документів. Для мережевих трас: цілісні PCAPи з незалежною часовою синхронізацією, журнали IDS/IPS, NetFlow з підписами. Повна простежуваність: хто, коли, де, з якою метою і яким інструментом мав доступ; кожен етап – окремий запис і підпис відповідальної особи. Формалізовані акти передачі, уніфіковані ідентифікатори носіїв, пломбування з фотофіксацією; журнал подій із неможливістю редагування. Усі експертизи мають бути перевірені. Відтворюваність: опис налаштувань інструментів, версій ПЗ, алгоритмів; збереження форензічних контейнерів для незалежної повторної перевірки. Серед процесуальних гарантій: повідомлення стороні захисту про методики, доступ до копій даних у режимі, сумісному із держтаємницею; можливість контрекспертизи. Для роботи з цифровими доказами необхідні поетапні процедури, підготовка і санкціонування:

1. Формулювання мети збору даних з тестом необхідності/пропорційності; перелік конкретних категорій даних (контент, метадані, трафік, геолокація).
2. Узгодження технічного плану з фахівцем IT/форензіки; визначення мінімально інвазивних засобів (напр., таргетований DPI замість масового моніторингу).
3. Отримання судового дозволу із зазначенням: обсягу, строків, інструментів, порядку зберігання і знищення надлишкових даних.

Вилучення і хешування (imaging and hashing)

4. Для носіїв: створення bit-by-bit образу за допомогою write-blocker; обчислення хешів оригіналу і образу (SHA-256/512), фіксація у протоколі з часовою міткою (UTC) і підписами.
5. Для мобільних пристроїв: логічний/фізичний дамп із сертифікованими інструментами; окрема фіксація secure enclave/криптоключів, якщо можливо й законно.
6. Для мережевих даних: безперервний захват PCAP/NetFlow із цифровим підписом сенсорів; синхронізація часу всіх сенсорів.

Усі доступи проходять проходять журналювання доступів (access logging).Централізований журнал із записом: ідентифікатор користувача, дата/час, дія, об'єкт, мета доступу, підстава (ухвала/доручення). Тригери сповіщень на аномальні дії (масове копіювання, позачасовий доступ, експорт за межі сегменту). Джерело отримання даних: класифікація за надійністю (A–E) і підтверджуваністю; пріоритет офіційних записів і первинних матеріалів. У процесі геолокації аналізуються тіні, ландшафту, картографіїя, порівняння з кліматичними даними; перевірка EXIF/метаданих і виявлення маніпуляцій (ELA/error level analysis). Додатково аналізується хронологія: кореляція часових міток з подіями (вибухи/повітряні тривоги), даними ADS-B/ AIS, сейсмічними логами; OSINT-профілювання, аналіз історії постингу, мережі підписників на предмет бот-мереж. Відбувається документування: збереження

e-ISSN: 2786-586X

оригінальних URL, хешування файлів, архівація сторінок (Wayback/локальний WARC), скрінкасти процесу верифікації. Фінтех-дані: банківські виписки, дані платіжних провайдерів, криптотранзакції тощо. Метод кореляції: побудова часових рядів і графів зв'язків; пошук спільних патернів (зустріч дзвінка з готівковим зняттям; одночасні переміщення і переклади коштів); визначення ступеня ймовірності збігу. Усунення хибних відповідностей: нормалізація часових поясів; верифікація геолокації альтернативними джерелами; виключення подій з високою базовою частотою (ларж-скейл outage тощо). Збереження і знищення даних фіксуються в ухвалі/наказі; надлишкові дані третіх осіб підлягають швидкій мінімізації/псевдонімізації або знищенню з актом. Експертиза і судове представлення формується через експертний звіт: опис джерел, методів, інструментів, контрольних значень хешів, невизначеностей і обмежень; відтворювані кроки. Демонстраційні матеріали: таймлайни, heatmaps руху, кореляційні таблиці; пояснювальні схеми для суду. У межах захисту прав усі сторони отримують доступ до копій/виписок; можливість ставити запитання експерту; у справах держтаємниці – перегляд у секретному режимі з протоколом.

Відповідно до деталізації вимог Будапештської конвенції (ст. 16–21): відбувається оперативне збереження комп'ютерних даних та можливість негайного наказу про «freeze» даних у провайдера; фіксація часу, категорій даних і періоду збереження; заборона доступу до вмісту без окремої санкції. Документування взаємодії з провайдером: підтвердження отримання, ідентифікація відповідальної особи, журнали технічних дій. Отримання мінімальних метаданих для ідентифікації інших юрисдикцій і подальших MLAT-запитів; принцип пропорційності і обмеження обсягу. Вилучення комп'ютерних даних. Правова підстава для доступу/вилучення; можливість негайного копіювання і створення форензічних образів; фіксація integrity-хешів; недопущення змін у джерельній системі (write-blocking/forensic boot). Окремі категорії цифрових доказів: специфічні вимоги: наприклад, месенджери з E2E-шифруванням, збір метаданих у провайдера зв'язку, резервних копій у хмарі, форензіка з кінцевих пристроїв; юридична неможливість «бекдорів» не означає незаконних обхідних шляхів. Валідність даних чатів через крос-перевірку: дампи обох сторін, телеком-логи, резервні копії, створення контрольних хешів. У роботі з цифровими доказами існують гарантії дотримання прав людини: чіткий перелік категорій даних; автоматичне видалення непотрібних третіх осіб; за можливості після завершення ризиків – інформування осіб про втручання і доступ до засобів юридичного захисту [17].

Нагляд і гарантії – обов'язкова процедура. Мета нагляду – забезпечити законність, необхідність і пропорційність втручань у приватність, а також доказову стійкість матеріалів НСРД. Подвійна модель поєднує попередній судовий контроль і постфактум парламентський огляд із незалежним технічним аудитом. Така архітектура відповідає вимогам передбачуваності, незалежності та ефективних засобів захисту [23]. До компонентів подвійного нагляду належать:

- Судовий дозвіл на законну перевірку мети, необхідності й пропорційності конкретного заходу; індивідуалізація об'єкта, строків, переліку даних і технічних засобів; вимога мінімізації та регламентації знищення надлишкових даних; контроль негайних/невідкладних дій через наступну легалізацію;
- Аналіз агрегованих показників НСРД без доступу до персоніфікованих даних; оцінка трендів, відмов суддів, частки продовжень, інцидентів недопустимості доказів; рекомендації щодо змін політик і видання обов'язкових приписів органам виконавчої влади; публічний щоквартальний/щорічний звіт у межах дозволеної відкритості.
- Незалежний технічний аудит: перевірка архітектури перехоплення і зберігання на відповідність принципу мінімізації та безпеці; випробування ланцюга збереження (chain of custody) і журналів доступу (append-only); оцінка відповідності технічним бенчмаркам (ETSI LI), криптозахисту, часової синхронізації.

e-ISSN: 2786-586X

- Формування технічних приписів і контроль їх виконання.

Ролі та відповідальність органів нагляду позначені у таблиці 1.

Таблиця 1.

Ролі, повноваження і межі доступу

Суб'єкт	Повноваження	Межі доступу	Основні виходи	Ризики
Слідчий суддя	Санкціонування НСРД; продовження; контроль невідкладних дій	Повний доступ до матеріалів клопотання, техплану, підстав	Ухвала з умовами мінімізації; відмова; зобов'язання знищити надлишкові дані	Формалізм; «штампування» ухвал
Апеляційний суд	Перегляд законності ухвали, доказів	Доступ до досьє провадження в частині НСРД	Скасування/залишення ухвали; орієнтири практики	Затримки; брак техкомпетенції
Парламентський комітет/комісія	Стратегічний огляд агрегованих даних; рекомендації	Лише агреговані/деідентифіковані показники; доступ до внутрішніх регламентів	Щорічні звіти; приписові рекомендації	Політизація; розкриття таємниці
Омбудсмен	Моніторинг прав людини; розгляд скарг	Персоніфікований доступ за згодою суду/закону	Спецзвіт про права людини у сфері НСРД	Обмежений мандат у держтаємниці
Незалежний технічний аудитор	Аудит систем; перевірка журналів; тестування безпеки	Технічні інтерфейси та журнали без персональних даних	Технічний звіт; plan of remedial actions	«Регуляторне захоплення»
Прокуратура (нагляд за слідством)	Законність дій слідства; процесуалізація КРД	Повний доступ до проваджень	Скасування незаконних постанов; інструкції	Конфлікт інтересів

Джерело: складено автором

Мінімальні стандартні операційні процедури існують для різних форм нагляду: чек-лист пропорційності: легітимна мета; необхідність; найменша інвазивність; часові межі; категорії даних; правила мінімізації/знищення; захист третіх осіб (для суддів); стандартизований формат агрегованого звіту (таблиці KPI, тренди, heatmaps відмов по регіонах/органах парламенту) та інші.

Подвійний нагляд із незалежним технічним аудитом створює багаторівневий запобіжник від зловживань і процесуальних помилок. Суд забезпечує індивідуальну законність і пропорційність, парламентський орган – системну підзвітність, а технічний аудитор – фактичну відповідність інфраструктури принципу мінімізації й безпеці. Разом це підвищує допустимість і транскордонну прийнятність доказів та знижує ризики порушень за ст. 5, 6 і 8 ЄКПЛ. [21].

e-ISSN: 2786-586X

Таблиця 2.

Інструменти протидії, гарантії та ризики

Інструмент	Правова основа	Ціль	Ключові гарантії	Ризики
Держзрада/шпигунство/диверсія	КК України ст. 111, 114, 113	Ізоляція агентури	Справедливий суд, допустимість доказів	Надмірна інкримінація
НСРД та КРД	КПК гл. 21; Закон про КРД	Раннє виявлення	Судовий контроль, ланцюг збереження	Масове стеження
Санкції/замороження активів	Закон «Про санкції»; акти ЄС/США/ВБ	Позбавлення ресурсів	Судовий перегляд	Помилкова ідентифікація
Контроль КІ/FDI	Регулювання КІ; EU 2019/452	Недопуск проникнення	Пропорційність	Геоекономічні спори
Міжнародна допомога	MLAT; Будапештська конвенція	Докази з-за кордону	Гарантії запитуваної держави	Затримки
Екстрадиція	Європейська конвенція 1957	Видача підозрюваних	Заборона катувань	Політичний виняток

Джерело: складено автором

Обговорення

Ідентифікована прогалина у дефініції агентурної діяльності знижує передбачуваність кваліфікації та ускладнює міжнародну взаємодію. Запропоновані стандарти цифрових доказів підвищують стійкість вироків і зменшують ризик виключення доказів через порушення ланцюга збереження. Подвійний нагляд формує легітимність НСРД у воєнний час і мінімізує системні порушення ст. 8 ЄКПЛ. Інтеграція санкцій і кримінального процесу дозволяє блокувати фінансування агентурних мереж на ранніх стадіях. [9]. Документи ЄС та НАТО наголошують на міжвідомчих механізмах і кібердоказах.

Легальна типологія агентурних дій із критеріями зв'язку з іноземною спецслужбою (вербування, фінансування, завдання, звітність, безпечний зв'язок). Матриця допустимості цифрових доказів з обов'язковим журналюванням і відкритими технічними протоколами. Подвійний нагляд із агрегованими відкритими звітами та незалежним технологічним аудитом НСРД.

Практичне значення дослідження дозволить зменшити час від виявлення до арешту активів і нейтралізації агентурної мережі. Єдиний реєстр пов'язаних осіб та активів з інтеграцією санкційних списків, банківських KYC/AML-даних і даних бірж криптоактивів дає змогу формувати «готові до дії» пакети арешту з мінімальним доопрацюванням. Це скорочує цикл «виявлення → арешт/замороження → спецконфіскація» з тижнів до днів. Стандартизований порядок freeze-запитів до провайдерів за моделлю Будапештської конвенції (оперативне збереження даних) і уніфіковані шаблони судових ухвал зменшують процесуальні затримки та кількість повернень клопотань на доопрацювання. Все це спільно дозволить підвищити якість експертиз і відсотка вироків, які витримують касаційний та міжнародний контроль. Спеціалізація судових експертів з кіберфорензіки, стандарти опису невизначеностей та технічних обмежень, а

e-ISSN: 2786-586X

також доступ захисту до робочих копій забезпечують баланс змагальності й підвищують довіру суду до цифрових масивів. Уніфіковані чек-листи пропорційності для суддів і прокурорів вирівнюють практику застосування НСРД, зменшуючи ризики скасування вироків у касації та у Страсбурзі за ст. 6 і 8 ЄКПЛ. [HUDOC: Roman Zakharov v. Russia; Szabó and Vissy v. Hungary; Bykov v. Russia; Teixeira de Castro v. Portugal]. Якщо конкретизувати, внаслідок спільних дій можна конкретно отримати наступні операційні ефекти:

- скоротити час freeze-відповіді від провайдерів до 24 годин у 75% випадків, що напряму впливає на успішність арештів активів і збереження ефемерних логів. [9];
- зменшити частку виключених цифрових доказів до ≤3% завдяки повному ланцюгу збереження та верифікованим методикам експертизи;
- знизити кількість обґрунтованих скарг до ЄСПЛ за ст. 8/13 завдяки парламентському огляду агрегованих показників і незалежних аудитів, які фіксують виконання тестів необхідності й пропорційності.

Сумарно ці результати означають швидшу нейтралізацію агентурних мереж, стійкіші вироки, менші правові й репутаційні ризики для держави та вищу сумісність із партнерами ЄС/НАТО у спільних розслідуваннях.

Висновки

1. Необхідно уніфіковано визначити агентурну діяльностть у законодавстві. Зокрема, сформулювати в спеціальному законі визначення, яке охоплює: вербування, інструктування, фінансування, матеріально-технічне забезпечення, приховані канали зв'язку, передання відомостей, впливові операції, сприяння диверсіям. Критерії встановлення зв'язку з іноземною спецслужбою: наявність контактів із кадровим співробітником або його посередником; докази інструктажу чи завдань; фінансові/матеріальні транзакції; використання конспіративних методів; звітність про виконання. Це підвищить правову визначеність, полегшить кваліфікацію та міжнародну допомогу[14].
2. Посилення процесуальних стандартів для цифрових доказів. Запровадити обов'язкові SOP: фіксація часу і місця вилучення; подвійне хешування; окремі копії для сторін; журналювання кожної дії; атестація інструментів; верифікація OSINT через багатоджерельне зіставлення; інтеграція телеком-логів, метаданих і фінансових слідів (включно з криптогаманцями). Закріпити в КПК посилені вимоги до ланцюга збереження та електронних підписів експертів. Це зменшить ризик виключення доказів і підвищить транснаціональну прийнятність матеріалів. [9].
3. Подвійний нагляд під час воєнного стану. Зберегти судовий дозвіл як базовий фільтр; публікувати щоквартальні агреговані звіти: кількість санкціонованих НСРД, частка продовжень, відсоток матеріалів, включених до обвинувальних актів, кількість відмов суддів. Запровадити технологічний аудит інфраструктури перехоплення на предмет відповідності принципу мінімізації даних [21]. Створити єдиний реєстр пов'язаних осіб/активів із ознаками участі в агентурних мережах; синхронізувати рішення РНБО про санкції з арештами/спецконфіскацією у КПК; передбачити прискорений судовий перегляд санкцій із процесуальними гарантіями. Розширити охоплення на посередників і логістичні ланки, включно з операторами криптобірж і платіжних провайдерів. Це мінімізує ресурси агентурних мереж і пришвидшить правозастосування [10].
4. У воєнний час дерогації мають бути вузькими, необхідними і тимчасовими, із чітким нормативним обґрунтуванням. Заборонити провокацію злочину; документувати відсутність інстигування у контрольованих операціях. Забезпечити доступ захисту до матеріалів, що становлять держтаємницю, у режимних приміщеннях із допуском. Впровадити регулярний омбудсменський моніторинг місць несвободи. Це знижує ризики програшів у ЄСПЛ і підвищує легітимність. [8].

e-ISSN: 2786-586X

5. Створити навчальні модулі для прокурорів, слідчих і суддів з технічних аспектів цифрових доказів і HUMINT; затвердити міжвідомчі SOP для вербувальної контрдіяльності, документації конспіративних контактів, обробки фінансових потоків; інтегрувати best practices CCDCOE і ENISA. Це підвищить спроможність держави й уніфікує правозастосування [14].

6. Індикатори ефективності і правова стійкість. Визначити KPI: кількість зірваних операцій; частка вироків, що встояли в касації; час від ідентифікації до блокування активів; відсоток НСРД, що матеріалізувалися в доказах; частка скарг, задоволених ЄСПЛ проти України. Регулярний публічний звіт за цими метриками полегшить корекцію політик. [HUDOC analytics; OECD методики оцінювання як аналог].

Список використаних джерел

1. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
3. Про контррозвідувальну діяльність: Закон України від 26.12.2002 № 374-IV. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
4. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
5. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
6. Про санкції: Закон України від 14.08.2014 № 1644-VII. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
7. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua (дата звернення: 19.05.2026).
8. Конвенція про захист прав людини і основоположних свобод від 04.11.1950. URL: https://echr.coe.int (дата звернення: 19.05.2026).
9. Конвенція про кіберзлочинність (Будапештська конвенція) від 23.11.2001. URL: https://coe.int (дата звернення: 19.05.2026).
10. Додатковий протокол до Женевських конвенцій від 12 серпня 1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол I), від 08.06.1977. URL: https://icrc.org (дата звернення: 19.05.2026).
11. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. URL: https://eur-lex.europa.eu (дата звернення: 19.05.2026).
12. ETSI Lawful Interception (LI) standards. URL: https://etsi.org (дата звернення: 19.05.2026).
13. ENISA Guidelines on Electronic Evidence. URL: https://enisa.europa.eu (дата звернення: 19.05.2026).
14. NATO Glossary of Terms and Definitions (AAP-06). URL: https://nato.int (дата звернення: 19.05.2026).
15. Bykov v. Russia: Judgment of the European Court of Human Rights of 10 March 2009 (Application no. 4378/02). URL: https://hudoc.echr.coe.int.
16. Roman Zakharov v. Russia: Judgment of the European Court of Human Rights of 4 December 2015 (Application no. 47143/06). URL: https://hudoc.echr.coe.int.
17. A. and Others v. the United Kingdom: Judgment of the European Court of Human Rights of 19 February 2009 (Application no. 3455/05). URL: https://hudoc.echr.coe.int.
18. Teixeira de Castro v. Portugal: Judgment of the European Court of Human Rights of 9 June 1998 (Application no. 25829/94). URL: https://hudoc.echr.coe.int.

e-ISSN: 2786-586X

19. Szabó and Vissy v. Hungary: Judgment of the European Court of Human Rights of 12 January 2016 (Application no. 37138/14). URL: https://hudoc.echr.coe.int.
20. Ramanauskas v. Lithuania: Judgment of the European Court of Human Rights of 5 February 2008 (Application no. 74420/01). URL: https://hudoc.echr.coe.int.
21. Venice Commission. Rule of Law Checklist. URL: https://venice.coe.int.
22. EEAS materials on hybrid threats. European External Action Service. URL: https://eeas.europa.eu.
23. OFAC Russia-related Sanctions. U.S. Department of the Treasury. URL: https://home.treasury.gov.
24. ICRC Customary IHL Database. International Committee of the Red Cross. URL: https://icrc.org.

References

1. Criminal Code of Ukraine: Law of Ukraine dated 05.04.2001 No. 2341-III. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
2. Criminal Procedure Code of Ukraine: Law of Ukraine dated 13.04.2012 No. 4651-VI. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
3. On counterintelligence activities: Law of Ukraine dated 26.12.2002 No. 374-IV. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
4. On the Security Service of Ukraine: Law of Ukraine dated 25.03.1992 No. 2229-XII. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
5. On state secrets: Law of Ukraine dated 21.01.1994 No. 3855-XII. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
6. On sanctions: Law of Ukraine dated 14.08.2014 No. 1644-VII. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
7. On the legal regime of martial law: Law of Ukraine dated 12.05.2015 No. 389-VIII. URL: https://zakon.rada.gov.ua (date of access: 19.05.2026).
8. Convention for the Protection of Human Rights and Fundamental Freedoms of 04.11.1950. URL: https://echr.coe.int (accessed 19.05.2026).
9. Convention on Cybercrime (Budapest Convention) of 23.11.2001. URL: https://coe.int (accessed 19.05.2026).
10. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), of 08.06.1977. URL: https://icrc.org (accessed 19.05.2026).
11. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union. URL: https://eur-lex.europa.eu (accessed 19.05.2026).
12. ETSI Lawful Interception (LI) standards. URL: https://etsi.org (accessed 19.05.2026).
13. ENISA Guidelines on Electronic Evidence. URL: https://enisa.europa.eu (accessed 19.05.2026).
14. NATO Glossary of Terms and Definitions (AAP-06). URL: https://nato.int (accessed 19.05.2026).
15. Bykov v. Russia: Judgment of the European Court of Human Rights of 10 March 2009 (Application no. 4378/02). URL: https://hudoc.echr.coe.int.
16. Roman Zakharov v. Russia: Judgment of the European Court of Human Rights of 4 December 2015 (Application no. 47143/06). URL: https://hudoc.echr.coe.int.
17. A. and Others v. the United Kingdom: Judgment of the European Court of Human Rights of 19 February 2009 (Application no. 3455/05). URL: https://hudoc.echr.coe.int.
18. Teixeira de Castro v. Portugal: Judgment of the European Court of Human Rights of 9 June 1998 (Application no. 25829/94). URL: https://hudoc.echr.coe.int.

e-ISSN: 2786-586X

19. Szabó and Vissy v. Hungary: Judgment of the European Court of Human Rights of 12 January 2016 (Application no. 37138/14). URL: https://hudoc.echr.coe.int.

20. Ramanauskas v. Lithuania: Judgment of the European Court of Human Rights of 5 February 2008 (Application no. 74420/01). URL: https://hudoc.echr.coe.int.

21. Venice Commission. Rule of Law Checklist. URL: https://venice.coe.int.

22. EEAS materials on hybrid threats. European External Action Service. URL: https://eeas.europa.eu.

23. OFAC Russia-related Sanctions. U.S. Department of the Treasury. URL: https://home.treasury.gov.

24. ICRC Customary IHL Database. International Committee of the Red Cross. URL: https://icrc.org.

e-ISSN: 2786-586X