Системи протидії тероризму в Європейському Союзі в умовах сучасної геополітичної нестабільності

Counter-Terrorism Systems in the European Union in the Context of Contemporary Geopolitical Instability

Сергій Євтух
аспірант кафедри національної безпеки, публічного управління та адміністрування, e-mail: phd256232_yesv@student.ztu.edu.ua, ORCID ID: https://orcid.org/0009-0006-1799-5026

Serhii Yevtukh
PhD Student of the Department of National Security, Public Administration and Administration, e-mail: phd256232_yesv@student.ztu.edu.ua, ORCID ID: https://orcid.org/0009-0006-1799-5026

Державний університет "Житомирська політехніка", м. Житомир, Україна

Zhytomyr Polytechnic State University, Zhytomyr, Ukraine

Received: April 23, 2026 | Revised: June 23, 2026 | Accepted: June 30, 2026

УДК 355.40:061.1ЄС

DOI: https://doi.org/10.33445/sds.2026.16.3.5

Мета роботи. Комплексне дослідження систем протидії тероризму в Європейському Союзі шляхом аналізу їхніх інституційних, правових та організаційних механізмів, оцінки ефективності наявних підходів і виявлення ключових проблем та викликів у сфері забезпечення безпеки.

Метод дослідження. Використано системний, інституційний, компаративно-правовий та системно-структурний підходи. Застосовано методи аналізу і синтезу наукових джерел, контент-аналізу нормативно-правових актів та стратегічних документів Європейського Союзу, порівняльного аналізу діяльності безпекових інституцій, статистичного аналізу даних Europol, ENISA та інших європейських організацій, а також елементи сценарного аналізу для оцінювання перспектив розвитку системи протидії тероризму.

Результати дослідження. Проаналізовано сучасну архітектуру системи протидії тероризму в Європейському Союзі та визначено роль Europol, Eurojust, Frontex, Шенгенської інформаційної системи й інших інституцій у забезпеченні безпеки. Виявлено основні тенденції трансформації терористичних загроз, зокрема поширення цифрової радикалізації, кібертероризму та гібридних форм протиборства. Обґрунтовано напрями підвищення ефективності міждержавної координації, інформаційного обміну, використання цифрових технологій і розвитку предиктивних механізмів реагування на сучасні безпекові виклики.

Теоретична цінність дослідження. Поглиблено наукове розуміння функціонування сучасної антитерористичної архітектури Європейського Союзу, закономірностей трансформації терористичних загроз та ролі цифрових технологій у забезпеченні безпеки в умовах геополітичної нестабільності.

Практична цінність дослідження. Отримані результати можуть бути використані під час удосконалення державної політики у сфері протидії тероризму, розвитку міжнародного безпекового співробітництва, гармонізації законодавства України з правом Європейського Союзу, а також підготовки пропозицій щодо зміцнення кібербезпеки, міжвідомчої координації та інформаційного обміну між компетентними органами.

Тип статті. Теоретико-аналітична.

Ключові слова:. тероризм; Європейський Союз; безпека; гібридні загрози; кібербезпека; міжнародна співпраця.

Purpose. To conduct a comprehensive study of counter-terrorism systems in the European Union by analysing their institutional, legal, and organisational mechanisms, assessing the effectiveness of existing approaches, and identifying the key challenges and issues in the field of security.

Method. The study employs systemic, institutional, comparative-legal, and structural-functional approaches. The research applies methods of analysis and synthesis of scientific literature, content analysis of EU legal acts and strategic documents, comparative analysis of the activities of security institutions, statistical analysis of data from Europol, ENISA, and other European organisations, as well as elements of scenario analysis to assess the prospects for the development of the EU counter-terrorism system.

Findings. The study analyses the contemporary architecture of the European Union's counter-terrorism system and identifies the roles of Europol, Eurojust, Frontex, the Schengen Information System, and other institutions in ensuring security. The main trends in the transformation of terrorist threats are identified, including the spread of digital radicalisation, cyberterrorism, and hybrid forms of confrontation. The study substantiates directions for improving interstate coordination, information sharing, the use of digital technologies, and the development of predictive response mechanisms to address contemporary security challenges.

Theoretical Implications. The research advances the scientific understanding of the functioning of the contemporary counter-terrorism architecture of the European Union, the patterns of transformation of terrorist threats, and the role of digital technologies in ensuring security under conditions of geopolitical instability.

Practical Implications. The findings may be used to improve public policy in the field of counter-terrorism, strengthen international security cooperation, harmonise Ukrainian legislation with European Union law, and develop proposals for enhancing cybersecurity, interagency coordination, and information exchange among competent authorities.

Paper Type. Theoretical and analytical.

Keywords: Terrorism; European Union; Security; Hybrid Threats; Cybersecurity; International Cooperation.

Вступ

Сучасне безпекове середовище Європейського Союзу характеризується зростанням геополітичної нестабільності та трансформацією терористичних загроз, які дедалі частіше поєднують традиційні форми насильства з елементами гібридного впливу, кіберзлочинності та інформаційно-психологічних операцій. За таких умов системи протидії тероризму в ЄС стикаються з низкою складних викликів, пов'язаних із необхідністю посилення координації між державами-членами, удосконалення механізмів обміну розвідувальною інформацією та підвищення оперативності реагування на новітні загрози.

Водночас чинні інституційні та правові механізми не завжди забезпечують належний рівень узгодженості дій між суб'єктами безпекової політики, що знижує ефективність протидії сучасним терористичним викликам. У зв'язку з цим особливої актуальності набуває дослідження ефективності систем протидії тероризму в Європейському Союзі, виявлення їхніх сильних і слабких сторін, а також обґрунтування напрямів подальшого вдосконалення в умовах динамічних змін міжнародного безпекового середовища.

Метою статті є комплексне дослідження систем протидії тероризму в Європейському Союзі шляхом аналізу їхніх інституційних, правових та організаційних механізмів, оцінки ефективності наявних підходів і виявлення ключових проблем та викликів у сфері забезпечення безпеки. Для досягнення поставленої мети здійснено аналіз сучасних тенденцій розвитку терористичних загроз, особливостей функціонування антитерористичної архітектури ЄС та ролі міждержавної співпраці у протидії тероризму. Особливу увагу приділено обґрунтуванню напрямів удосконалення координації між державами-членами, підвищення ефективності реагування на терористичні загрози, а також розширення використання сучасних інформаційних технологій та цифрових інструментів у сфері забезпечення безпеки.

Огляд літератури

Сучасний науковий дискурс щодо протидії тероризму в Європейському Союзі характеризується багатовекторністю підходів до нейтралізації безпекових загроз. Зокрема, І. А. Білан [1] досліджує превентивні заходи та інституційні аспекти міжвідомчої координації у сфері боротьби з тероризмом, тоді як Т. О. Чернадчук і В. О. Березовська [2] аналізують нормативно-правові засади формування та реалізації антитерористичної політики Європейського Союзу. М. Красій [3] акцентує увагу на кримінально-правових механізмах реагування на терористичні прояви, а В. А. Ліпкан [4] розкриває теоретико-правові засади тероризму та основні тенденції його розвитку в сучасних умовах.

Водночас стрімка еволюція терористичних загроз під впливом цифровізації, міжнародних конфліктів і гібридних форм протиборства зумовлює необхідність врахування результатів сучасних зарубіжних досліджень. Значний внесок у вивчення технологічного виміру терористичної діяльності зробив П. Нойманн (P. Neumann) [5], який досліджує механізми онлайн-радикалізації, цифрового екстремізму та особливості функціонування мережевих терористичних спільнот. Інституційний та операційний вимір безпекової архітектури Європейського Союзу ґрунтовно аналізує О. Буреш (O. Bures) [6], який обґрунтовує значення інтеграції інформаційних систем та сумісності баз даних, зокрема Шенгенської інформаційної системи (SIS II), для підвищення ефективності транскордонної взаємодії правоохоронних органів.

Окрему увагу впливу зовнішніх геополітичних чинників на трансформацію безпекової політики ЄС приділяє Ф. Траунер (F. Trauner) [7]. Науковець доводить, що масштабні безпекові кризи, зокрема повномасштабна агресія Російської Федерації проти України, суттєво впливають на реформування європейських інституцій безпеки, діяльність Frontex і Europol та розвиток механізмів реагування на гібридні загрози.

Попри наявність вагомих наукових напрацювань, недостатньо дослідженими залишаються питання комплексної оцінки ефективності сучасної антитерористичної архітектури Європейського Союзу в умовах зростання гібридних загроз, цифровізації терористичної діяльності та майбутнього розширення ЄС. Окремого наукового осмислення потребує визначення потенційного внеску України у розвиток європейської системи безпеки та протидії тероризму з урахуванням набутого досвіду протидії гібридній агресії.

Методологія дослідження

Методологічну основу дослідження становить комплекс загальнонаукових і спеціальних методів, застосування яких забезпечило всебічний аналіз систем протидії тероризму в Європейському Союзі. Інституційний та системно-структурний методи використано для дослідження організаційної побудови безпекових інституцій ЄС, механізмів їхньої взаємодії та виявлення наявних функціональних і координаційних проблем. Компаративно-правовий метод застосовано для аналізу рівня гармонізації антитерористичного законодавства держав-членів ЄС та оцінки його відповідності сучасним викликам у сфері безпеки, зокрема щодо збору та використання цифрових доказів в умовах дотримання вимог захисту персональних даних.

Емпіричну основу дослідження сформовано шляхом використання статистичного методу, зокрема прийомів групування, узагальнення, порівняльного та дескриптивного аналізу. Це дозволило систематизувати дані офіційної звітності Європолу, ENISA та інших профільних безпекових інституцій, виявити основні тенденції розвитку терористичних загроз, зміни у структурі радикалізації та особливості трансформації підходів до протидії тероризму в ЄС.

Для оцінювання перспектив розвитку безпекової архітектури Європейського Союзу використано прогностичний метод і елементи сценарного аналізу, що дало змогу окреслити можливі напрями вдосконалення системи протидії тероризму в умовах поширення гібридних загроз, цифровізації терористичної діяльності та майбутнього розширення Європейського Союзу.

Результати дослідження

У сучасній науковій парадигмі під тероризмом розуміють суспільно небезпечну діяльність, що виражається у свідомому та цілеспрямованому застосуванні насильства через захоплення заручників, підпали, убивства, тортури, залякування населення й органів влади або вчинення інших посягань на життя чи здоров’я невинуватих осіб, а також у погрозах здійснення таких дій задля досягнення злочинних цілей [8]. В умовах сучасної геополітичної нестабільності цей феномен зазнає фундаментальної трансформації, перетворюючись із локального радикалізму на інструмент стратегічного впливу недержавних суб'єктів та проксі-сил у межах гібридних протистоянь. Концептуальною основою безпекової архітектури Європейського Союзу є принцип солідарності, закріплений у ст. 222 Договору про функціонування ЄС, який зобов’язує держави-членів мобілізувати всі наявні ресурси для допомоги партнеру, що став об’єктом атаки. Цей принцип знаходить свою практичну реалізацію через Контртерористичну стратегію ЄС, яка базується на чотирьох фундаментальних «стовпах», що охоплюють повний цикл протидії загрозам. Перший сегмент — запобігання (Prevent) — спрямований на боротьбу з радикалізацією через усунення її глибинних соціальних причин та моніторинг екстремістського контенту. Другий напрям — захист (Protect) — передбачає зменшення вразливості критичної інфраструктури, енергомереж та транспортних вузлів, а також посилення контролю на зовнішніх кордонах Шенгенської зони. Третій складник — переслідування (Pursue) — фокусується на активному руйнуванні логістичних ланцюгів терористів, припиненні каналів фінансування (AML/CFT) та проведенні спільних транскордонних розслідувань. Завершальний етап — реагування (Respond) — полягає у підготовці систем цивільного захисту до мінімізації наслідків можливих атак, наданні допомоги жертвам та швидкому відновленні стабільності суспільних інститутів [9]. Важливим

елементом правової архітектури в цьому контексті є Директива (ЄС) 2017/541, яка уніфікує криміналізацію терористичних злочинів у національних законодавствах 27 країн та встановлює суворі правові механізми для протидії діяльності "іноземних бойовиків-терористів", що передбачають кримінальну відповідальність за виїзд за кордон, навчання та фінансування з терористичною метою [10].

Інституційна система протидії тероризму в ЄС функціонує як модель багаторівневого мережевого управління, де ключову оперативну роль відіграє Європол (Europol). Це агентство ЄС у сфері правоохоронної діяльності було офіційно засноване 1 липня 1999 року після тривалого етапу еволюції з Відділу боротьби з наркотиками, створеного ще у 1994 році. На сучасному етапі Європол виступає центральним координаційно-аналітичним центром обміну кримінальною розвідувальною інформацією, координує масштабні операції проти терористичних осередків та здійснює стратегічний аналіз загроз через Європейський центр боротьби з тероризмом (ECTC). На прокурорському та судовому рівнях цю систему органічно доповнює Євроюст (Eurojust) — Агентство ЄС з питань співробітництва у сфері кримінального правосуддя, яке було офіційно засноване 28 лютого 2002 року з метою посилення координації розслідувань після терактів 11 вересня. Євроюст забезпечує процесуальну взаємодію між суддями та прокурорами різних держав, надає юридичну підтримку Спільним слідчим групам (JITs) та долає колізії національних правових систем, гарантуючи невідворотність покарання за терористичну діяльність. Важливим елементом сучасних підходів до протидії тероризму є концепція соціальної стійкості (resilience), яка розглядається як здатність суспільства та державних інституцій ефективно реагувати на кризові явища та мінімізувати наслідки терористичних загроз.

Сучасне терористичне середовище в Європейському Союзі характеризується високим рівнем динамічності, фрагментації та адаптивності до змін у міжнародному безпековому середовищі. Еволюція терористичного ландшафту в ЄС відбувається у напрямі децентралізації, що виявляється у підвищенні ролі індивідуальних виконавців та малих автономних груп, діяльність яких часто не пов'язана безпосередньо з організованими терористичними структурами.

Терористичні загрози в Європейському Союзі залишаються ідеологічно різноманітними та охоплюють джихадистський, праворадикальний, ліворадикальний і сепаратистський екстремізм. При цьому, попри кількісне переважання окремих типів атак, найбільшу небезпеку з точки зору летальності та суспільного резонансу продовжує становити джихадистський тероризм. Водночас кількісні показники терористичної активності демонструють нестабільну динаміку, що свідчить не про зменшення загрози, а про її трансформацію та ускладнення форм прояву. Статистичні дані щодо кількості терористичних атак у державах — членах ЄС за 2015–2024 рр., узагальнені на основі щорічних звітів Європолу TE-SAT[11], наведено на рисунку 1.

Глибокий ретроспективний аналіз представлених статистичних даних дозволяє диференціювати досліджуваний десятирічний цикл на три ключові етапи, кожен з яких детермінований унікальними геополітичними та технологічними факторами:

- Перший етап (2015–2017 рр.) — "Пікова криза летального тероризму": Максимальні показники терористичної активності цього періоду безпосередньо пов'язані з військовою експансією та піком операційної спроможності ІДІЛ (Даїш) на Близькому Сході. Централізована координація, масовий приплив "іноземних бойовиків-терористів" (FTF) європейського походження, які повертались із зон конфліктів, а також слабка на той час синхронізація національних баз даних держав-членів ЄС зумовили хвилю масштабних скоординованих атак (Париж, Брюссель, Ніцца, Берлін).

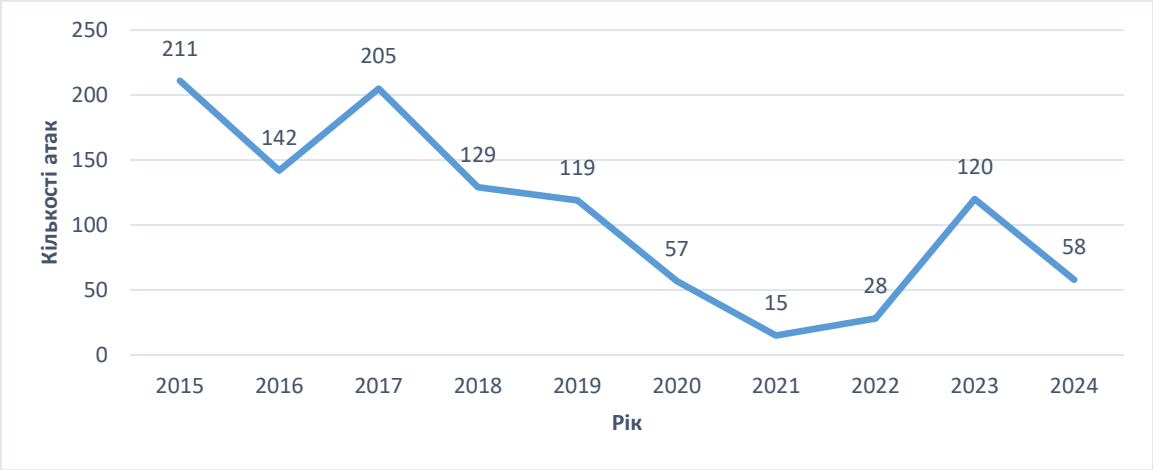

Рисунок 1: Динаміка кількості терористичних атак у державах — членах ЄС за 2015–2024 рр.
Джерело: складено автором за даними Europol TE-SAT 2022–2024.

- Другий етап (2018–2020 рр.) — "Етап тактичної адаптації та пандемічного затишшя": Стрімке зниження кількості атак стало наслідком розгрому територіального ядра ІДІЛ та запровадження в ЄС Плану дій щодо боротьби з тероризмом (Counter-Terrorism Agenda). Проте ключовим фактором аномального зниження інцидентів у 2020 році стали жорсткі карантинні обмеження під час пандемії COVID-19. Закриття кордонів, обмеження масових заходів, скорочення кількості потенційних "м'яких цілей" та посилений поліцейський контроль на вулицях європейських міст суттєво ускладнили діяльність і логістичне забезпечення терористичних груп.
- Третій етап (2021–2024 рр.) — "Асиметричне відновлення та децентралізація": Стабілізація показників на відносно низькому рівні порівняно з 2015 роком є оманливою, оскільки відбулася якісна трансформація загрози. Зазначені тенденції значною мірою зумовлені переходом від ієрархічних терористичних мереж до децентралізованих форм терористичної діяльності саморадикалізованих осіб. Водночас новий сплеск у 2023–2024 рр. чітко корелює із загостренням конфлікту на Близькому Сході (Газа), що виступило потужним тригером для ідеологічної поляризації всередині мусульманських громад ЄС, а також із різким зростанням праворадикального та антисемітського екстремізму в цифровому просторі Співтовариства.

Суттєвих змін зазнає і соціально-демографічний профіль осіб, причетних до терористичної діяльності, зокрема спостерігається тенденція до зниження віку радикалізованих осіб. Важливу роль у цьому процесі відіграє цифрове середовище, оскільки інтернет і соціальні мережі виступають ключовими каналами пропаганди, вербування та координації терористичної діяльності, що значно ускладнює виявлення загроз на ранніх етапах.

Цифрове середовище відіграє визначальну роль у сучасних процесах радикалізації в Європейському Союзі, трансформуючи їх у більш приховані, швидкі та децентралізовані форми. Інтернет-платформи не лише забезпечують поширення екстремістського контенту, але й створюють умови для цілеспрямованого психологічного впливу, формування радикальної ідентичності та індивідуалізованого вербування. Алгоритми рекомендацій сприяють поступовому зануренню користувачів у радикалізовані інформаційні середовища, посилюючи ефект "інформаційних бульбашок" і нормалізацію насильства. Особливого значення набуває феномен саморадикалізації, за якого індивід проходить весь шлях залучення до екстремістської ідеології виключно онлайн, без прямого контакту з терористичними мережами. Водночас використання закритих спільнот, зашифрованих каналів комунікації та

мультимедійного контенту підвищує ефективність впливу, особливо на молодіжну аудиторію, та ускладнює діяльність правоохоронних органів щодо своєчасного виявлення загроз.

Крім того, сучасне терористичне середовище в ЄС формується під впливом зовнішніх геополітичних чинників, включаючи міжнародні конфлікти, міграційні процеси та поширення гібридних загроз.

Архітектура протидії тероризму в Європейському Союзі є комплексною багаторівневою системою управління безпекою, що поєднує стратегічне політичне керівництво, оперативно-правоохоронну взаємодію, судово-правову координацію та розвинуті інформаційно-аналітичні механізми. На стратегічному рівні формування політики здійснюється Європейською комісією, Радою ЄС та Координатором ЄС з питань боротьби з тероризмом, які визначають спільні пріоритети безпеки, гармонізують законодавчі підходи держав-членів і забезпечують узгодженість дій у межах простору свободи, безпеки та правосуддя. Оперативний рівень реалізується через ключові агенції ЄС, зокрема Europol, який виконує функції аналітичного центру та платформи обміну оперативною інформацією між державами-членами, Frontex, що забезпечує контроль зовнішніх кордонів та моніторинг ризиків у контексті міграційних потоків, а також Eurojust, який координує судове переслідування терористичних злочинів і сприяє взаємодії національних прокуратур.

Важливим елементом функціонування системи є судово-правові та координаційні механізми, що забезпечують практичну реалізацію принципу взаємного визнання рішень у кримінально-правовій сфері. До них належить Європейський ордер на арешт (European Arrest Warrant), який суттєво спростив процедури екстрадиції між державами-членами та підвищив оперативність реагування на підозрюваних у терористичній діяльності. Не менш значущими є Спільні слідчі групи (Joint Investigation Teams, JITs), які дозволяють правоохоронним органам різних держав-членів проводити спільні розслідування в режимі реального часу, забезпечуючи безпосередній обмін доказами та координацію слідчих дій без традиційних бюрократичних бар'єрів. Ці механізми суттєво підвищують ефективність транскордонного переслідування терористичних мереж і є ключовим інструментом практичної інтеграції кримінальної юстиції в ЄС.

Окреме системоутворююче значення має інформаційно-аналітична складова, яка базується на постійному обміні даними між державами-членами через захищені канали та загальноєвропейські бази даних. Центральну роль відіграє Шенгенська інформаційна система (SIS), що забезпечує оперативне інформування про підозрюваних осіб, об'єкти та ризики, а також аналітичні платформи Europol, які агрегують дані на рівні ЄС. Обмін інформацією між державами-членами відбувається на основі принципів взаємної довіри та солідарності, однак на практиці залишається залежним від рівня готовності держав передавати чутливі розвідувальні дані, що створює певні асиметрії в ефективності системи.

Динаміка кількості арештів за терористичну діяльність у Європейському Союзі за період 2015–2024 рр. відображає загальну еволюцію контртерористичної політики ЄС, що характеризується переходом від масових затримань у період пікової джихадистської загрози до більш вибіркових і превентивних правоохоронних заходів у подальші роки. Як свідчать узагальнені дані Europol у межах щорічних звітів TE-SAT [8], після максимальних значень у 2015–2017 рр. спостерігається поступове зниження показників із подальшою стабілізацією в межах 380–449 арештів у 2021–2024 рр., що вказує на зміну характеру терористичних загроз та посилення аналітично-орієнтованих механізмів реагування. Узагальнена візуалізація цієї динаміки представлена на рис. 2, який ілюструє тенденції арештів за тероризм у ЄС.

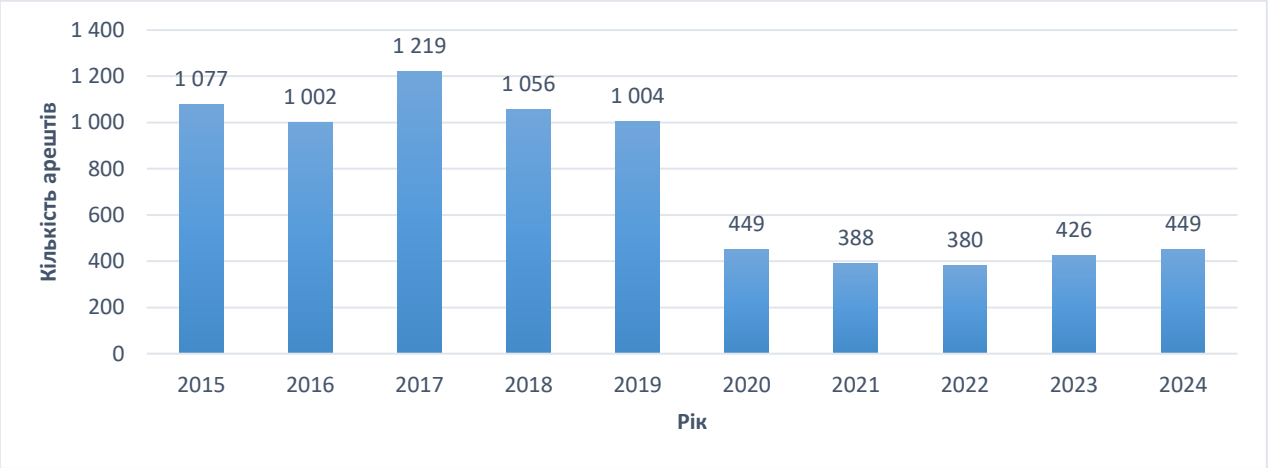

Рисунок 2: Кількість арештів за тероризм у державах Європейського Союзу за 2015–2024 рр. (за даними Europol / TE-SAT).
Джерело: складено автором за даними Europol TE-SAT 2022–2024.

Інтерпретація динаміки правоохоронної діяльності, відображеної на Рисунку 2, демонструє чітку зміну філософії безпекових органів ЄС — від реактивного правосуддя до проактивної превенції. Надзвичайно високий рівень арештів у 2015–2017 роках пояснюється проведенням масштабних контртерористичних операцій правоохоронних органів Франції, Бельгії та Німеччини. Реакція систем кримінальної юстиції у цей період мала характер "наздоганяючого регулювання", коли затримання відбувалися переважно за фактом скоєння злочину або в процесі ліквідації вже сформованих логістичних осередків.

Натомість тенденція до зниження та подальшої стабілізації кількості арештів у межах 380–449 осіб у період 2021–2024 років свідчить не про послаблення уваги спецслужб, а про суттєве підвищення точності та вибірковості контртерористичних заходів. Головним чинником такої стабілізації виступає докорінна модернізація інформаційного обміну, зокрема повноцінний запуск оновленої Шенгенської інформаційної системи (SIS II) та розширення у 2022 році аналітичного мандату Європолу, що дозволило виявляти радикалізованих осіб та канали фінансування (AML/CFT) на етапі задуму чи транскордонного переміщення, усуваючи потребу в масових затриманнях. Важливу роль відіграє також посилений законодавчий тиск на цифрове середовище через імплементацію Регламенту (EU) 2021/784 щодо видалення терористичного контенту протягом однієї години, який дозволяє правоохоронцям руйнувати вербувальні ланцюги в інтернеті до моменту переходу потенційних виконавців до практичних дій. Крім того, посилення превентивної складової діяльності відображає переорієнтацію ресурсів Євроюсту та національних прокуратур на складні, тривалі розслідування із використанням штучного інтелекту для аналізу Big Data, що дозволяє ізолювати ключових організаторів та фінансових донорів, а не лише дезорієнтованих одноосібних виконавців.

Трансформація сучасного терористичного середовища в Європейському Союзі відбувається на тлі безпрецедентної геополітичної нестабільності, детермінованої повномасштабною агресією проти України та загостренням конфлікту на Близькому Сході. За даними Global Terrorism Index [12], цей вплив виражається у відчутному зростанні кількості інцидентів у західних країнах та суттєвому збільшенні числа атак безпосередньо в європейському регіоні, що супроводжується стрімким підвищенням рівня смертності від таких нападів.

Науковий аналіз поточної ситуації підтверджує остаточне зміщення парадигми від ієрархічних структур до децентралізованої мережевої активності автономних суб'єктів, на яких наразі припадає абсолютна більшість усіх летальних випадків у країнах Заходу. Ключовим дестабілізуючим чинником стає ідеологічна поляризація суспільства: кількість політично

мотивованих нападів помітно перевищила кількість релігійних, а рівень антисемітських інцидентів стрімко зріс, що безпосередньо корелює з міжнародними конфліктами.

Особливої гостроти для безпекових інституцій ЄС, зокрема Європолу та Євроюсту, набуває проблема цифрової радикалізації неповнолітніх, які становлять значну частку серед підозрюваних у ЄС, а також використання зловмисниками новітніх технологій, таких як безпілотні літальні апарати та штучний інтелект. Така динаміка вимагає переходу від реактивного правосуддя до проактивної стратегії моніторингу інформаційних потоків та зміцнення інтегрованого управління кордонами в умовах гібридної агресії, що є логічним продовженням еволюції контртерористичної архітектури Євросоюзу.

Водночас сучасна еволюція тероризму характеризується докорінною зміною методів впливу внаслідок диджиталізації конфліктів, де онлайн-радикалізація постає не просто допоміжним інструментом, а повноцінним автономним фронтом ідеологічного протистояння. Використання соціальних медіа як платформ для первинного рекрутингу в поєднанні з переходом у месенджери з наскрізним шифруванням (encrypted apps) створює феномен "цифрових ехо-камер", у яких екстремістський наратив ізолюється від правоохоронного нагляду. Особливу загрозу становить інтеграція штучного інтелекту, що дозволяє автоматизувати виробництво пропаганди та створювати дипфейки, які радикально знижують поріг довіри до офіційних джерел інформації. Аналіз свідчить, що використання сучасних цифрових технологій у терористичній діяльності сприяє децентралізації загроз, перетворюючи її на мережеву структуру, де алгоритми рекомендацій сприяють радикалізації користувачів на основі їхніх психологічних вразливостей.

Паралельно з децентралізацією мережевих структур, сучасний кібертероризм пройшов шлях від поверхневого візуального спотворення веб-ресурсів до складних багатовекторних операцій, спрямованих на руйнацію критичної інфраструктури держав-членів ЄС. Згідно з даними ENISA (Агентства ЄС з кібербезпеки) [13], у період з 2020 по 2025 рік спостерігається стрімка ідеологізація кіберпростору. Аналіз структури загроз у межах Євросоюзу за цей п'ятирічний цикл демонструє чітку спеціалізацію атак, яку доцільно представити у вигляді статистичного розподілу (див. рис. 3):

- DDoS-атаки (48 %): головний інструмент "цифрового тиску", що використовується для блокування урядових порталів, банківських сервісів та транспортних вузлів країн ЄС.
- Програми-вимагачі (Ransomware) (22 %): метод фінансового виснаження та паралізації критичних установ (зокрема, масштабні атаки на сектор охорони здоров'я та муніципалітети).
- Шпигунство та компрометація даних (18 %): цілеспрямовані операції проти оборонних підприємств та державних інституцій ЄС.
- Деструктивні атаки на промислові системи (ICS) (8 %): спроби втручання в роботу енергомереж та систем водопостачання.
- Інші операції (4 %): маніпуляція інформаційним простором через злам ефірного мовлення чи офіційних сторінок.

Практика останніх років підтверджує, що територія ЄС стала ключовим полігоном для апробації методів "цифрового терору". Серед найбільш резонансних подій у регіоні слід виділити:

- Атака на Службу здоров'я Ірландії (HSE, 2021): наймасштабніша кібератака на державну систему охорони здоров'я в ЄС, що призвела до повного відключення ІТ-мереж лікарень на кілька тижнів, поставивши під загрозу тисячі життів.
- Кібердиверсія проти уряду Албанії (2022): серія деструктивних атак, що призвела до паралічу державних цифрових послуг і стала першим випадком в історії регіону, коли кіберінцидент спричинив розрив дипломатичних відносин.

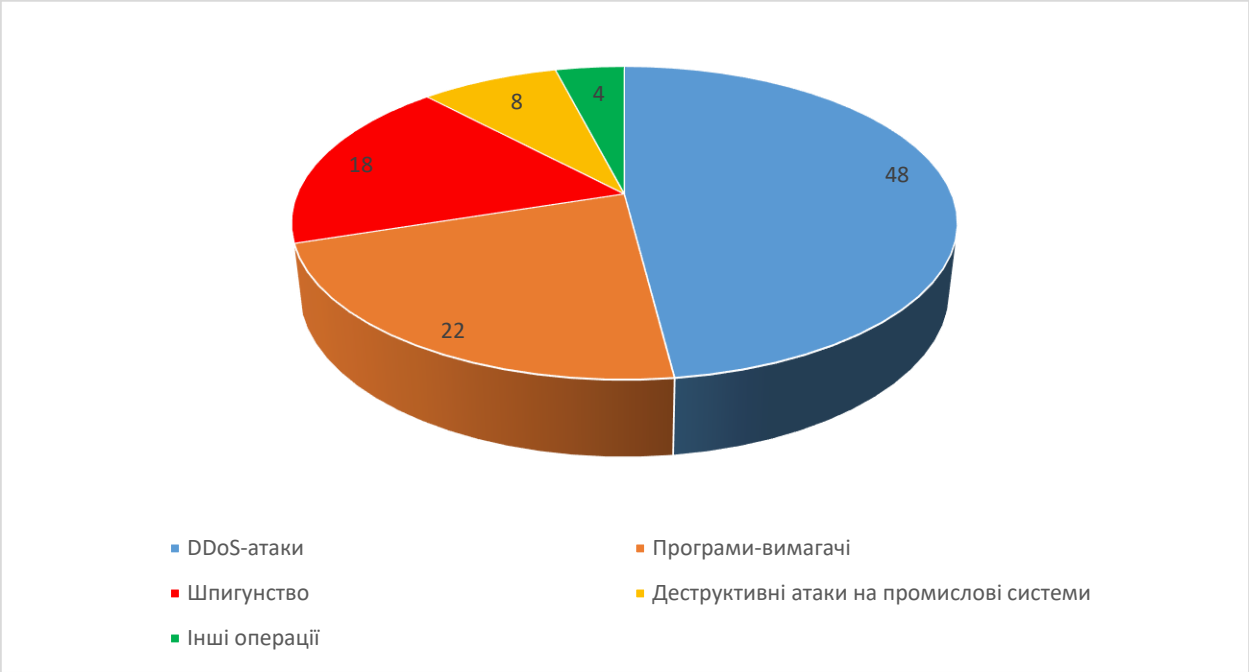

Рисунок 3: Структура кібертерористичних загроз у Європейському Союзі (2020–2025 рр.)
Джерело: складено автором за даними ENISA Threat Landscape 2024

- Кібердиверсія проти уряду Албанії (2022): серія деструктивних атак, що призвела до паралічу державних цифрових послуг і стала першим випадком в історії регіону, коли кіберінцидент спричинив розрив дипломатичних відносин.
- Злам мережі супутникового зв'язку KA-SAT (2022): атака, що відбулася в день початку повномасштабного вторгнення в Україну, але мала транскордонний ефект, вивівши з ладу тисячі вітрогенераторів у Німеччині та термінали зв’язку по всьому ЄС.
- Параліч банківського сектору Литви (2022–2023): тривалі DDoS-атаки з боку ідеологічно мотивованих угруповань, що на певний час заблокували доступ громадян до фінансових операцій та державних реєстрів у відповідь на політичні рішення Вільнюса.
- Втручання в інфраструктуру німецької залізниці (Deutsche Bahn, 2022): акти саботажу на лініях зв’язку, які експерти з безпеки кваліфікували як гібридну терористичну атаку на транспортну логістику ЄС.

Така динаміка підкреслює, що кіберпростір став асиметричною зброєю, де використання ШІ-інструментів дозволяє зловмисникам проводити сканування вразливостей європейської інфраструктури в рази швидше, ніж на початку 2020-х. Це призводить до поступового зниження стійкості цифрової інфраструктури та підриває довіру громадян до спроможності інституцій ЄС забезпечувати належний рівень безпеки.

У контексті вищезазначених детермінант, ефективність системи протидії тероризму в Європейському Союзі ґрунтується на реалізації стратегічного порядку денного (Counter-Terrorism Agenda 2020), результативність якого підтверджується конкретними операційними успіхами інституцій ЄС. Згідно зі звітами Europol [11], ключовим індикатором успіху є високий рівень превенції: попри складну геополітичну ситуацію, більшість терористичних актів на стадії підготовки було вчасно нейтралізовано завдяки транскордонному обміну даними через Європейський антитерористичний центр (ECTC). Важливим практичним заходом стало впровадження Регламенту (EU) 2021/784 [14], який зобов’язує хостинг-провайдерів видаляти терористичний контент протягом однієї години; це дозволило суттєво обмежити цифрову радикалізацію та онлайн-рекрутинг. У юридичній площині ефективність демонструє діяльність

Eurojust, яка забезпечила координацію сотень спільних розслідувань, що призвело до понад 400 обвинувальних вироків щорічно у 2023–2024 роках, підтверджуючи здатність правових систем держав-членів до результативного переслідування злочинців.

Значний внесок у цей процес зробила масштабна модернізація Шенгенської інформаційної системи (SIS II), яка з 2023 року отримала розширений функціонал для превентивного виявлення загроз. Оновлення системи дозволило впровадити нові категорії попереджень, зокрема "превентивні алерти" щодо осіб, схильних до терористичної діяльності, а також розширило використання біометричних даних (відбитків долонь та зображень обличчя) для точної ідентифікації підозрюваних. Паралельно з цим, посилення мандату Europol у 2022 році надало агентству право безпосередньо взаємодіяти з приватними компаніями для отримання великих масивів даних (Big Data), що критично важливо для аналізу цифрових слідів терористів. Оновлений статус також дозволив Europol ініціювати кримінальні розслідування в державах-членах навіть у випадках, коли злочин стосується лише однієї країни, але має значний вплив на інтереси всього Союзу, та надавати посилену підтримку національним органам через використання штучного інтелекту для обробки оперативної інформації.

Незважаючи на вагомі здобутки у зміцненні безпекового контуру, сучасна архітектура протидії тероризму в Європейському Союзі стикається з низкою критичних інституційних та технологічних бар'єрів, що зумовлюють необхідність радикальної трансформації стратегічних підходів. Системний аналіз існуючих проблем вказує на те, що ключовою перешкодою залишається глибока технологічна асиметрія та фрагментація між національними спецслужбами: держави-члени володіють різним рівнем ресурсів для кіберрозвідки, що створює зони безпекової вразливості всередині Шенгенської зони, якими терористичні угруповання користуються для транскордонної логістики та фінансових операцій. Ситуація ускладнюється розмиванням меж між класичним тероризмом та гібридними атаками, де іноземні актори можуть використовувати радикальні осередки як інструмент дестабілізації, що критично ускладнює процеси атрибуції та оперативного реагування. Крім того, інтеграція штучного інтелекту для моніторингу потенційних загроз постійно входить у клінч з етико-правовими стандартами Хартії основних прав ЄС та регламентом GDPR, що подекуди уповільнює впровадження автоматизованих систем розпізнавання облич та предиктивної аналітики.

Перспективним вектором подолання цих викликів вбачається перехід від реактивної моделі безпеки до парадигми предиктивної оборони, що вимагає впровадження низки дієвих кроків. По-перше, критично необхідним є створення Єдиного безпекового хмарового середовища (Security Cloud), яке дозволить забезпечити миттєву синхронізацію між національними базами даних та аналітичними потужностями Europol, усуваючи затримки в обміні інформацією. По-друге, розв'язання проблеми цифрових доказів потребує остаточної уніфікації регламентів щодо транскордонного доступу до електронних даних (e-evidence), що дасть змогу правоохоронцям вилучати критичну інформацію безпосередньо у провайдерів в інших юрисдикціях за лічені години. Стратегічні завдання на майбутнє також мають фокусуватися на розбудові мережі спеціалізованих кіберцентрів колективного захисту на базі Європейського центру кіберзлочинності (EC3), які будуть орієнтовані на захист критичної інфраструктури від терористичних кібердиверсій. Нарешті, розвиток системи має базуватися на принципі "безпеки за дизайном" (Security by Design), що передбачає впровадження антитерористичних алгоритмів безпосередньо у розробку нових фінансових та комунікаційних платформ, забезпечуючи солідарну, високотехнологічну та правомірно збалансовану відповідь Союзу на терористичні експансії в умовах тривалої геополітичної турбулентності.

Окремим вектором трансформації безпекової архітектури, що заслуговує на прискіпливу увагу, є вплив майбутнього розширення Європейського Союзу на його антитерористичний контур. Перспектива включення України та країн Західних Балкан ставить

перед інституціями ЄС завдання з масштабної реконфігурації оборонного ландшафту. Зокрема, вступ України, яка володіє унікальним практичним досвідом протидії гібридній агресії та проявам державного тероризму, здатен кардинально посилити інтелектуальний і оперативний потенціал Europol та ECTC, трансформуючи їх з координаційних хабів на центри активного випереджального реагування. Реконфігурація безпекової ролі ЄС внаслідок агресії РФ проти України розглядається в академічному середовищі як "тектонічний зсув" (Yearbook of European Law, 2025) [15], що вимагає переходу від виключно економічної солідарності до військово-технологічної інтеграції нових членів у контртерористичні мережі. Водночас перенесення зовнішнього кордону Співтовариства на схід вимагає розгортання оновленої системи інтегрованого управління кордонами (IBM) під егідою Frontex, що базуватиметься на предиктивній ідентифікації ризиків та впровадженні інтелектуальних засобів спостереження.

Для регіону Західних Балкан пріоритетним викликом залишається подолання наслідків минулих конфліктів, що потребує інтенсифікації контролю за незаконним обігом вогнепальної зброї через спільні платформи, такі як EMPACT. Загалом розширення Союзу детермінує перехід до "інклюзивної моделі безпеки", де нові держави-члени переходять від ролі отримувачів безпекової підтримки до активних учасників формування спільного безпекового простору Європейського Союзу. Такий процес вимагатиме прискореної технологічної конвергенції національних баз даних із Шенгенською інформаційною системою (SIS) та створення розгалуженої мережі регіональних центрів кіберзахисту для ефективного нівелювання транскордонних терористичних ланцюгів на нових рубежах Співтовариства.

Обговорення

Проведений аналіз еволюції системи протидії тероризму в Європейському Союзі свідчить, що забезпечення безпеки Співтовариства в умовах геополітичної нестабільності поступово зміщується від переважного використання традиційних правоохоронних механізмів до розвитку превентивних цифрових та інформаційно-аналітичних інструментів. Результати дослідження підтверджують, що посилення кібербезпекового та інформаційного компонентів сприяє підвищенню адаптивності контртерористичної системи до асиметричних загроз і розширює можливості їх своєчасного виявлення та нейтралізації.

Отримані результати розвивають положення концепції онлайн-екстремізму П. Нойманна [5], а також доповнюють наукові підходи до оцінювання ефективності сучасних систем безпеки. Запропонований у дослідженні підхід, заснований на принципі Security by Design та концепції предиктивної солідарності, спрямований на підвищення ефективності обміну інформацією між безпековими інституціями ЄС за одночасного дотримання вимог щодо захисту персональних даних. Крім того, на відміну від підходів, у межах яких повномасштабна агресія Російської Федерації проти України розглядається переважно як джерело нових безпекових ризиків для Європи, результати дослідження дають підстави розглядати Україну як важливого партнера у розвитку європейської системи безпеки. Набутий Україною практичний досвід протидії гібридним загрозам, кібератакам і проявам державного тероризму може бути використаний для вдосконалення діяльності європейських безпекових інституцій у процесі подальшого розширення Європейського Союзу.

Практичне значення отриманих результатів полягає у можливості використання запропонованих підходів під час оцінювання ефективності контртерористичних механізмів, виявлення проблемних аспектів міжвідомчого інформаційного обміну та підтримки управлінських рішень у сфері безпеки. Окремі положення дослідження можуть бути використані під час формування державної політики у сфері європейської інтеграції та безпекового співробітництва України з Європейським Союзом.

Висновки

Проведене дослідження засвідчило, що сучасна система протидії тероризму в Європейському Союзі являє собою складну багаторівневу архітектуру безпеки, яка поєднує інституційні, правові, інформаційно-аналітичні та технологічні механізми реагування на терористичні загрози. Встановлено, що в умовах зростання геополітичної нестабільності та поширення гібридних викликів пріоритетними напрямами розвитку контртерористичної політики ЄС стають превентивні заходи, цифровий моніторинг загроз, посилення міжвідомчої координації та вдосконалення механізмів обміну інформацією між державами-членами.

Результати аналізу засвідчили важливу роль Europol, Eurojust, Frontex та Шенгенської інформаційної системи (SIS) у забезпеченні ефективного функціонування європейської системи безпеки. Водночас виявлено низку проблем, серед яких технологічна нерівномірність розвитку держав-членів, складність протидії цифровій радикалізації, необхідність удосконалення механізмів обміну розвідувальною інформацією та забезпечення балансу між безпекою і захистом фундаментальних прав людини.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Використання штучного інтелекту

Мовне редагування, переклад, технічна перевірка тексту.

Список використаних джерел

1. Білан І. А. Протидія тероризму: досвід ЄС. Інформація і право. 2021. № 2 (37). С. 67–73. DOI : https://doi.org/10.37750/2616-6798.2021.2(37).238338 (дата звернення: 23.05.2026).
2. Чернадчук, Т. О., & Березовська, В. О. (2022). Політика європейського союзу щодо боротьби з тероризмом: аналіз законодавства європейського союзу та деяких національних антитерористичних програм. *Правова держава*, (48), 66–76. https://doi.org/10.18524/2411-2054.2022.48.267964 (дата звернення: 23.05.2026).
3. Красій М. О. Кримінально-правова політика ЄС у сфері боротьби з тероризмом. Слово Національної школи суддів України. 2025. № 2 (51). DOI : https://doi.org/10.37566/2707-6849-2025-2(51)-15 (дата звернення: 23.05.2026).
4. Ліпкан В. А. Тероризм і національна безпека України : монографія. Київ, 2000. 262 с. URL: https://www.lipkan.com/terorizm-i-natsionalna-bezpeka-ukrayini/ (дата звернення: 23.05.2026).
5. Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies. *International Journal of Conflict and Violence (IJCV)*, *14*, 1–20. https://doi.org/10.4119/ijcv-3809 (accessed: 23.05.2026).
6. Bures, O., & Gajo, C. (2026). Interoperability: A Paradigm Shift in EU Counterterrorism? *Studies in Conflict & Terrorism*. Advance online publication. https://doi.org/10.1080/1057610X.2026.2618982 (accessed: 23.06.2026).
7. Trauner F. The Impact of the Russian War against Ukraine on the Reform of the Common European Asylum System. European Politics and Society. 2024. Vol. 25, No. 4. P. 1–18. URL: https://www.tandfonline.com/doi/epdf/10.1080/23745118.2024.2435401 (accessed: 23.05.2026).

8. Про боротьбу з тероризмом : Закон України від 20 березня 2003 р. № 638-IV. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 23.06.2026).
9. The EU Counter-Terrorism Strategy. Council of the European Union. Brussels, 2005. URL: https://data.consilium.europa.eu/doc/document/ST-14469-2005-REV-4/en/pdf (accessed: 23.05.2026).
10. On Combating Terrorism : Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017. Official Journal of the European Union. 2017. URL: https://eur-lex.europa.eu/eli/dir/2017/541/oj/eng (accessed: 23.05.2026).
11. EU Terrorism Situation and Trend Report (TE-SAT) 2022–2024. Europol. Luxembourg : Publications Office of the European Union, 2022–2024. URL: https://www.europol.europa.eu/publications-events/main-reports/tesat-report (accessed: 23.05.2026).
12. Global Terrorism Index 2025: Measuring the Impact of Terrorism. Institute for Economics & Peace. Sydney, 2025. 94 p. URL: https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf (accessed: 23.05.2026).
13. ENISA Threat Landscape 2024: July 2023 to June 2024. European Union Agency for Cybersecurity. Athens : ENISA, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed: 23.05.2026).
14. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content Online. Official Journal of the European Union. 2021. L 172. P. 79–109. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0784 (accessed: 23.05.2026).
15. How the War in Ukraine Has Transformed the EU's Common Foreign and Security Policy. Yearbook of European Law. 2025. Vol. 44. URL: https://academic.oup.com/yel/advance-article/doi/10.1093/yel/yeaf003/8112000 (accessed: 23.05.2026).

References

1. Bilan, I. A. (2021). Protydiia teroryzmu: dosvid YeS [Countering terrorism: The EU experience]. Informatsiia i pravo, 2(37), 67–73. https://doi.org/10.37750/2616-6798.2021.2(37).238338
2. Chernadchuk, T. O., & Berezovska, V. O. (2022). Polityka Yevropeiskoho Soiuzu shchodo borotby z teroryzmom: analiz zakonodavstva Yevropeiskoho Soiuzu ta deiakykh natsionalnykh antyterorystychnykh prohram [European Union policy on combating terrorism: Analysis of European Union legislation and selected national counter-terrorism programs]. Pravova derzhava, (48), 66–76. https://doi.org/10.18524/2411-2054.2022.48.267964
3. Krasii, M. O. (2025). Kryminalno-pravova polityka YeS u sferi borotby z teroryzmom [EU criminal law policy in the field of counter-terrorism]. Slovo Natsionalnoi shkoly suddiv Ukrainy, 2(51). https://doi.org/10.37566/2707-6849-2025-2(51)-15
4. Lipkan, V. A. (2000). Teroryzm i natsionalna bezpeka Ukrainy [Terrorism and national security of Ukraine]. Kyiv, Ukraine.
5. Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online extremism: Research trends in internet activism, radicalization, and counter-strategies. International Journal of Conflict and Violence, 14, 1–20. https://doi.org/10.4119/ijcv-3809
6. Bures, O., & Gajo, C. (2026). Interoperability: A paradigm shift in EU counterterrorism? Studies in Conflict & Terrorism. Advance online publication. https://doi.org/10.1080/1057610X.2026.2618982
7. Trauner, F. (2024). The impact of the Russian war against Ukraine on the reform of the common European asylum system. European Politics and Society, 25(4), 1–18. https://doi.org/10.1080/23745118.2024.2435401
8. Verkhovna Rada of Ukraine. (2003). Pro borotbu z teroryzmom: Zakon Ukrainy vid 20 bereznia 2003

roku № 638-IV [On combating terrorism: Law of Ukraine No. 638-IV of March 20, 2003]. https://zakon.rada.gov.ua/laws/show/638-15

9. Council of the European Union. (2005). The EU counter-terrorism strategy. https://data.consilium.europa.eu/doc/document/ST-14469-2005-REV-4/en/pdf
10. European Parliament & Council of the European Union. (2017). Directive (EU) 2017/541 of 15 March 2017 on combating terrorism. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2017/541/oj
11. Europol. (2022–2024). EU terrorism situation and trend report (TE-SAT) 2022–2024. Publications Office of the European Union. https://www.europol.europa.eu/publications-events/main-reports/tesat-report
12. Institute for Economics & Peace. (2025). Global terrorism index 2025: Measuring the impact of terrorism. https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf
13. European Union Agency for Cybersecurity (ENISA). (2024). ENISA threat landscape 2024: July 2023 to June 2024. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
14. European Parliament & Council of the European Union. (2021). Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online. Official Journal of the European Union, L172, 79–109. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0784
15. How the war in Ukraine has transformed the EU's common foreign and security policy. (2025). Yearbook of European Law, 44. https://doi.org/10.1093/yel/yeaf003