DOI: 10.33270/05267303.3
УДК 343.3:340.5

ЗАГИНЕЙ-ЗАБОЛОТЕНКО Зоя*
доктор юридичних наук, професор, завідувач відділу проблем кримінальної юстиції та кримінології Інституту держави і права імені В. М. Корецького НАН України
01601, вул. Трьохсвятительська, 4, м. Київ, Україна
ORCID: https://orcid.org/0000-0002-8679-124X;
ВИЧІКОВ Володимир
аспірант Інституту держави і права імені В. М. Корецького НАН України
01601, вул. Трьохсвятительська, 4, м. Київ, Україна
ORCID: https://orcid.org/0009-0004-7885-1195

Від диверсії до саботажу: моделі криміналізації в Україні та зарубіжних правопорядках

Анотація. Статтю присвячено порівняльно-правовому дослідженню сучасних підходів до криміналізації диверсійно-саботажної діяльності та визначенню можливих напрямів удосконалення кримінально-правової охорони національної безпеки України. Метою статті є встановлення закономірностей нормативного конструювання таких кримінально-правових заборон у зарубіжному законодавстві та визначення місця української моделі диверсії в системі сучасних порівняльно-правових підходів. Матеріалами дослідження стали положення кримінального законодавства Великої Британії, Канади, Австралії, Франції, Федеративної Республіки Німеччина, Польщі, Швеції, Фінляндії, Норвегії, Чехії, Латвії, Естонії та України. Застосовано формально-юридичний, порівняльно-правовий, системний, функціональний методи й метод типологізації. Обґрунтовано, що зарубіжні аналоги диверсії не можна визначати лише за термінологічною схожістю назв відповідних кримінальних правопорушень. Запропоновано розрізняти номінативну, структурну та функціональну еквівалентність кримінально-правових заборон, визнавши функціональну еквівалентність вихідним критерієм їх порівняння. Встановлено, що національні моделі формуються через різні комбінації цільового, іноземно-агентурного, інтересоцентричного та функціонально-інфраструктурного механізмів криміналізації, а за способом законодавчого оформлення можуть мати автономну, диференційовану комплексну або децентралізовану архітектуру. Виявлено зміну функціональної парадигми кримінально-правової охорони, що полягає в перенесенні акценту з матеріальної цілісності стратегічно значущого об’єкта на забезпечення його операційної спроможності, доступності, надійності, ефективності та безперервності виконання критично важливих суспільних або державних функцій. Окреслено тенденцію до поглиблення превентивної криміналізації, яка в окремих правопорядках охоплює не лише готування і замах, а й створення засобів саботажу, розвідку об’єктів, агентурну підготовку, формування технічних і програмних вразливостей та планування майбутнього посягання. Українську конструкцію диверсії визначено як автономну цільову модель казуїстично-об’єктного типу. Обґрунтовано, що перспективним напрямом її модернізації є функціоналізація об’єктивної сторони шляхом надання самостійного кримінально-правового значення виведенню з ладу, істотному припиненню, порушенню або дезорганізації функціонування систем, об’єктів і мереж, від яких залежить безпека, обороноздатність і стійкість держави. Практичне значення результатів полягає в можливості їх використання під час подальшого вдосконалення статті 113 Кримінального кодексу України та формування підходів до кримінально-правової оцінки сучасних форм диверсійно-саботажної діяльності.

Ключові слова: диверсійно-саботажна діяльність; національна безпека; критична інфраструктура; кримінальна відповідальність; зарубіжне кримінальне законодавство; функціональний підхід.

Історія статті:
Отримано: 15.07.2026
Прийнято: 03.09.2026
Опубліковано: 01.10.2026

Рекомендоване посилання:
Загиней-Заболотенко З., Вичіков В. Від диверсії до саботажу: моделі криміналізації в Україні та зарубіжних правопорядках. *Наука і правоохорона.* 2026. Вип. 3 (73). С. 25–42. DOI: 10.33270/05267303.3

*Відповідальний автор

© Загиней-Заболотенко З., Вичіков В., 2026. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/)

Вступ

Диверсійно-саботажна діяльність упродовж останніх років набула якісно нових форм, що актуалізувало питання про відповідність традиційних кримінально-правових конструкцій характеру сучасних загроз національній безпеці. Якщо класичне уявлення про диверсію або саботаж безпосередньо формувалося навколо фізичного знищення чи пошкодження стратегічно важливих об'єктів, то сучасні посягання дедалі частіше спрямовані на порушення функціонування енергетичних, транспортних, інформаційно-комунікаційних, фінансових та інших систем без обов'язкового фізичного знищення їх матеріальних компонентів. Одночасно змінився організаційний механізм відповідної діяльності: поряд із професійно підготовленими виконавцями використовують дистанційно завербованих осіб, цифрові засоби координації, посередників і виконавців окремих локальних завдань, які можуть не володіти повною інформацією про характер і кінцеву мету операції. D. Richterova, E. Grossfeld, M. Long і P. Bury (2024), досліджуючи сучасну російську саботажну діяльність у Європі, характеризують цю трансформацію через модель «гіг-економіки» (*gig economy*), за якої організація операцій дедалі більше спирається на децентралізоване залучення виконавців і цифрову комунікацію.

Зазначені зміни відбуваються в контексті трансформації гібридних загроз, для яких характерними є поєднання різних форм державного й недержавного впливу, діяльність у просторі між миром і відкритим збройним конфліктом та ускладнена атрибуція відповідних дій. S. Sanz-Caballero (2023) зосереджено увагу на понятт'євій невизначеності гібридних загроз і складності застосування до них традиційних правових механізмів. S. G. Jones (2025), характеризуючи сучасну російську саботажну діяльність у Європі, демонструє різноманітність використовуваних засобів – від підпалів, вибухів і пошкодження критичної інфраструктури до електронних і кібернетичних операцій. Це підтверджує, що сучасну диверсійно-саботажну діяльність не можна розглядати виключно крізь призму фізичного руйнування матеріальних об'єктів.

Складність кримінально-правового реагування посилюється тим, що поняття саботажу не має універсального змісту навіть у сучасному безпековому дискурсі. J. Rovner, R. Cormac і L. Maschmeyer (2025) акцентують на фрагментарності наукових підходів до розуміння саботажу й відмежовують його від суміжних форм прихованої державної діяльності та підривного впливу. Запропоноване ними концептуальне розуміння пов'язує саботаж насамперед зі зниженням ефективності функціонування різноманітних систем. Для кримінально-правового аналізу це має принципове значення: у центрі відповідного феномену опиняється не обов'язково фізичне знищення об'єкта, а погіршення спроможності певної системи виконувати покладену на неї функцію.

Посилення уваги до функціонального виміру саботажу безпосередньо пов'язане з посиленням залежності держав і суспільств від критичної інфраструктури. Сучасні дослідження засвідчують, що енергетичні мережі, підводні кабелі, трубопроводи, транспортні системи, електронні комунікації та інформаційні системи одночасно є умовою нормального функціонування суспільства й потенційними об'єктами гібридного впливу. F. Billing і B. Feldtmann (2024), аналізуючи можливості кримінального права в протидії гібридним атакам, окремо розглядають посягання на критичну інфраструктуру, навігаційні системи, підводні кабелі й трубопроводи, аргументують складність застосування традиційних кримінально-правових механізмів до дій, які одночасно можуть мати ознаки звичайного кримінального правопорушення, гібридної операції або елементу ширшого міждержавного протиборства. Значення має не лише протидія безпосередньому пошкодженню таких об'єктів, а й забезпечення їх стійкості як систем. M. J. Alexopoulos, A. Niemi, B. Skobiej та F. Sill Torres (2025), аналізуючи Директиву ЄС про стійкість критичних суб'єктів, доводять, що навіть у межах єдиного європейського регуляторного простору визначення критичних суб'єктів і необхідних заходів їх захисту допускає істотну національну варіативність. G. Pestana та S. Sofou (2024) своєю чергою розглядають управління даними як складову протидії гібридним загрозам критичній інфраструктурі, що додатково підтверджує неможливість зводити сучасне інфраструктурне ураження лише до фізичного пошкодження матеріального об'єкта.

Схожий процес простежується і стосовно цифрової інфраструктури. S. Haataja (2022) досліджує операції проти критичної інфраструктури в кіберпросторі крізь призму не лише її пошкодження, а й порушення можливості використання або функціонування. Така постановка питання відображає можливість заподіяння істотної шкоди системі без її фізичного руйнування. T. J. Holt і співавтори (2023) додатково засвідчують специфіку підтримуваних державами кібератак, які відрізняються від діяльності недержавних суб'єктів, зокрема за характером завдань і способами впливу.

Особливого значення ця проблематика набула в Європі після початку повномасштабної російсько-української війни та серії інцидентів із критичною інфраструктурою. M. Piekarski (2025), аналізуючи український досвід, характеризує критичну інфраструктуру як об'єкт гібридних і конвенційних атак. O. L. Larsson (2024) на матеріалі морського середовища демонструє, що саботаж критичної інфраструктури стає одним із виявів діяльності в «сірій зоні», здатним спричиняти істотні порушення глобальних комунікацій, економічних процесів і безпеки держав.

H. Ringbom (2025) на матеріалі пошкоджень підводних кабелів і трубопроводів у Балтійському морі розглядає юридичні складнощі реагування на ймовірні саботажні операції, насамперед щодо юрисдикції та атрибуції. A. Castrogiovanni (2026) показує, що сучасний гібридний примус у Балтійському морі поєднує матеріальне порушення інфраструктури з правовою та атрибуційною невизначеністю, а ефективність реагування залежить також від стійкості, спостереження, швидкості відновлення та правової координації. A.W. Neal (2026) своєю чергою аналізує системні безпекові дилеми захисту критичної морської інфраструктури.

Зміна характеру загроз супроводжується трансформацією нормативних підходів до захисту критично важливих систем. M. Becker (2025), досліджуючи імплементацію законодавства ЄС у сфері захисту критичної інфраструктури в державах Балтійського регіону, виявляє істотні відмінності між національними моделями навіть за наявності спільних європейських нормативних орієнтирів. Це дає підстави припускати, що й кримінально-правова охорона відповідних систем не може бути зведена до єдиної універсальної конструкції.

Новітні законодавчі реформи в окремих державах безпосередньо змінюють традиційне кримінально-правове розуміння диверсійно-саботажної діяльності. Показовою є польська реформа 2023 року, після якої в ст. 130 КК Польщі використовують одночасно поняття «диверсія» (*dywersja*) та «саботаж» (*sabotaż*) у контексті діяльності іноземної розвідки. L. Rosicki та R. Rosicki (2025) зосереджують увагу на проблемах визначеності змісту цих категорій та меж криміналізації відповідної протиправної поведінки. Співіснування цих двох понять у межах однієї кримінально-правової норми є важливим для порівняльного дослідження, оскільки засвідчує, що «диверсія» і «саботаж» не можна апріорі розглядати як повні юридичні синоніми.

В українській кримінально-правовій науці новітні дослідження диверсії зосереджені передусім на проблемах кваліфікації, відмежування від державної зради й терористичного акту, визначенні предметних ознак кримінального правопорушення та вдосконаленні законодавчої характеристики об’єктів, які мають важливе народногосподарське чи оборонне значення. Зокрема, О. О. Почка (2025) дослідив проблеми законодавчого забезпечення та правозастосування ст. 113 КК України й використав окремі елементи зарубіжного досвіду для формулювання пропозицій щодо її вдосконалення. В. І. Павликівський та В. Б. Селевко (2024) обґрунтовують необхідність перегляду категорії об’єктів «важливого народногосподарського чи оборонного значення» з огляду на сучасне законодавство про критичну інфраструктуру.

Водночас порівняння окремих кримінально-правових норм не дає відповіді на питання про закономірності сучасної криміналізації диверсійно-саботажної діяльності. Пошук у зарубіжному законодавстві норми, яка за назвою або набором зовнішніх ознак найбільше нагадує ст. 113 КК України, може призводити до методологічно хибних результатів. Однойменні склади саботажу в різних правопорядках істотно відрізняються за охоронюваними інтересами, суб’єктивними ознаками, значенням зв’язку з іноземною державою, характером кримінально значущої шкоди й моментом, з якого застосовують кримінально-правове реагування. Водночас функціонально близькі до саботажу заборони можуть мати іншу назву або бути розподіленими між кількома кримінально-правовими нормами.

Тому метою статті є встановлення та характеристика сучасних порівняльно-правових моделей криміналізації диверсійно-саботажних посягань на основі функціонального аналізу кримінального законодавства зарубіжних держав, виявлення закономірностей їх нормативного конструювання та визначення місця ст. 113 КК України в системі таких моделей.

Для досягнення цієї мети поставлено такі завдання: визначити критерії функціональної еквівалентності кримінально-правових заборон, які в різних правопорядках охоплюють диверсійно-саботажну діяльність; встановити механізми, за допомогою яких відповідним діянням надають спеціальну антидержавну або суспільнобезпекову спрямованість; дослідити значення фізичного пошкодження та функціонального порушення системи для конструювання об’єктивної сторони; порівняти роль зв’язку з іноземною державою або розвідкою; встановити глибину поширення криміналізації на підготовчі й інші «передсаботажні» форми поведінки; схарактеризувати способи диференціації кримінальної відповідальності й архітектуру відповідних кримінально-правових заборон.

Наукова новизна дослідження полягає в застосуванні багатовимірного підходу до порівняння диверсійно-саботажних кримінально-правових заборон. На відміну від їх групування лише за назвою кримінального правопорушення або за державами, запропоновано аналізувати національні моделі за сукупністю відносно самостійних координат: способом формування антидержавної спрямованості посягання; роллю зв’язку з іноземною державою; співвідношенням матеріального пошкодження та функціонального ураження; характеристиками охоронюваної інфраструктури чи суспільної функції; глибиною превентивної криміналізації; способом диференціації відповідальності; архітектурою кримінально-правової охорони. Такий підхід дає змогу встановити не формальну подібність законодавчих конструкцій, а механізми, комбінація яких формує конкретну національну модель криміналізації.

Огляд літератури

Сучасні дослідження проблематики саботажу умовно можна об'єднати в кілька взаємопов'язаних напрямів. Перший напрям становлять праці, присвячені концептуалізації гібридних загроз і саботажу як форм міждержавного протиборства. S. Sanz-Caballero (2023), що акцентують на понятєвій невизначеності гібридних загроз, їх функціонуванні в просторі між миром і відкритим збройним конфліктом та складності застосування до них традиційних правових механізмів. J. C. Bergaust і S. R. Sellevåg (2024) втручання нижче від порогу збройного конфлікту виокремлюють саботаж серед самостійних форм такого впливу та пропонують типологічний підхід до їх систематизації. D. Richterova, E. Grossfeld, M. Long і P. Bury (2024) досліджують трансформацію організації сучасних саботажних операцій, насамперед використання децентралізованого вербування та залучення виконавців до окремих завдань. J. Rovner, R. Cormac і L. Maschmeyer (2025) безпосередньо ставлять питання про межі поняття саботажу, його співвідношення з прихованими операціями та підривною діяльністю.

Другий напрям утворюють дослідження критичної інфраструктури як об'єкта сучасних гібридних, фізичних і кібернетичних посягань. S. Haataja (2022) аналізує правове значення пошкодження та функціонального порушення критичної інфраструктури внаслідок кібератак; F. Billing і B. Feldtmann (2024) – можливості кримінально-правового реагування на гібридні атаки; G. Pestana та S. Sofou (2024) – значення управління даними для стійкості критичної інфраструктури в умовах гібридних загроз; M. J. Alexopoulos і співавтори (2025) – особливості нормативного забезпечення стійкості критичних суб'єктів, зокрема в морському секторі. O. L. Larsson (2024), H. Ringbom (2025), A. W. Neal (2026) та A. Castrogiovanni (2026) висвітлюють різні аспекти вразливості морської та підводної інфраструктури в умовах діяльності в «сірій зоні», проблем атрибуції та забезпечення стійкості. G. Pestana та S. Sofou (2024) досліджують стійкість критичної інфраструктури до гібридних загроз крізь призму управління даними й інформаційними потоками, акцентуючи на тому, що забезпечення її захищеності не обмежується фізичною охороною об'єктів, а охоплює збереження спроможності відповідних систем до належного функціонування. Спільним для цих досліджень є зміщення аналітичного фокусу з власне матеріального об'єкта на його стійкість, доступність, відновлюваність і безперервність виконуваної ним функції.

Третій напрям має безпосередньо кримінально-правовий зміст і стосується аналізу окремих національних моделей. Показовою є польська дискусія, активізована реформою 2023 року. L. Rosicki та R. Rosicki (2025) досліджують криміналізацію пов'язаних зі шпигунством диверсії та саботажу, акцентуючи на невизначеності цих понять і складності встановлення меж нових кримінально-правових заборон. P. Burczaniuk (2024) аналізує зміни польського законодавства про шпигунство в ширшому контексті протидії діяльності іноземних розвідувальних служб, а P. Chlebowicz (2026) уже розглядає проблеми практичного застосування нових конструкцій, пов'язаних із диверсійною та саботажною діяльністю. Польський досвід у цьому аспекті демонструє не лише можливість швидкого оновлення кримінального законодавства у відповідь на сучасні загрози, а й ризик використання понять, нормативний зміст яких залишається недостатньо конкретизованим. Окреме значення для розуміння сучасної моделі кримінально-правової протидії саботажу має британська реформа 2023 року. R. Ward (2024), аналізуючи нову систему кримінальних правопорушень, пов'язаних із загрозами державі, досліджує роль зв'язку з іноземною державою, конструкцію саботажу та криміналізацію підготовчої поведінки. Такий підхід дає змогу розглядати британський склад саботажу не ізольовано, а як елемент ширшої системи кримінально-правового реагування на діяльність, пов'язану з іноземним впливом.

В українській кримінально-правовій літературі сучасний етап дослідження ст. 113 КК України характеризується увагою до її застосування в умовах війни, відмежування диверсії від суміжних кримінальних правопорушень та модернізації предметних ознак складу. О. О. Почка (2025) аналізує законодавчі та правозастосовні проблеми зі зверненням до зарубіжного досвіду; В. І. Павліківський і В. Б. Селевко (2024) спеціально досліджують співвідношення передбачених ст. 113 КК об'єктів важливого народногосподарського або оборонного значення із сучасною категорією критичної інфраструктури. О. М. Герасименко (2024) розглядає критичну інфраструктуру України як самостійний предмет наукового пізнання, а К. О. Черевко та Д. В. Пашнєв (2024) акцентують на специфіці кібератак на об'єкти критичної інфраструктури в умовах війни. Р. Бундз і Д. Яровик (2024) аналізують кримінальну відповідальність за державну зраду та диверсію в умовах воєнного стану.

Отже, у сучасній літературі достатньо ґрунтовно представлені аспекти феномену саботажу, захисту критичної інфраструктури, гібридних загроз і національного кримінально-правового регулювання. Водночас порівняльно-правова типологізація саме механізмів криміналізації відповідних посягань залишається недостатньо розробленою. Наявні дослідження не дають системної відповіді на питання, чому функціонально схоже діяння в одному правопорядку набуває спеціального кримінально-правового значення через антидержавну мету, в іншому – через зв'язок з іноземною державою, у третьому – через характер охоронюваної системи, а в четвертому – через

масштаб порушення суспільно важливої функції. Саме заповнення цієї прогалини визначає спрямованість подальшого дослідження.

Матеріали та методи

Матеріалами дослідження стали чинні положення кримінального законодавства таких держав: Великої Британії, Канади, Австралії, Франції, Федеративної Республіки Німеччина, Польщі, Швеції, Фінляндії, Норвегії, Чехії, Латвії та Естонії, а також ст. 113 КК України. Нормативні положення досліджено за актуальними редакціями, розміщеними в офіційних національних базах законодавства. Для з'ясування передумов і змісту окремих новітніх законодавчих рішень додатково використовували офіційні пояснювальні й аналітичні матеріали.

Вибір держав здійснено цілеспрямовано з огляду на кілька критеріїв. По-перше, до вибірки включено правопорядки, у яких протягом останніх років відбулося істотне оновлення законодавства про саботаж або кримінальні правопорушення, пов'язані із загрозами державі, – Велику Британію, Канаду, Австралію та Польщу. По-друге, досліджено правопорядки з усталеними автономними або системними конструкціями саботажу – Францію, ФРН, Швецію і Фінляндію. По-третє, до вибірки включено держави, які використовують функціонально орієнтовані конструкції охорони інфраструктури або життєво важливих систем без обов'язкового використання поняття «саботаж», – Норвегію та Естонію. По-четверте, Чехія і Латвія обрані як особливо релевантні для порівняння з Україною правопорядки, у яких спеціальна антидержавна спрямованість поєднується із функціональним описом об'єктивної сторони.

Під час формування нормативної вибірки застосовано функціональний, а не термінологічний критерій еквівалентності. До предмета порівняння включено кримінально-правові заборони, спрямовані на протидію умисному порушенню національної безпеки, оборонного потенціалу держави, інституційної спроможності або функціонування життєво важливих суспільних систем, незалежно від того, чи використовує національний законодавець поняття «саботаж» (*sabotage*), «диверсія» (*dywersja*), «підривна діяльність» (*subversion*), «напад на інфраструктуру» (*attack on infrastructure*) або інше поняття. Натомість загальні склади пошкодження майна, комп'ютерних кримінальних правопорушень чи порушень правил експлуатації систем до вибірки не включали, якщо спеціальна антидержавна, інфраструктурна або системно-функціональна спрямованість не була закладена в конструкцію відповідної кримінально-правової заборони.

Дослідження проведено в декілька етапів. На першому було ідентифіковано функціонально релевантні кримінально-правові заборони та встановлено їх місце в системі кримінального законодавства відповідної держави. На другому – кожну заборону проаналізовано за єдиною системою критеріїв. На третьому результати порівняння зіставлено з чинною конструкцією ст. 113 КК України. На завершальному етапі на основі повторюваних нормативних закономірностей сформовано типологію механізмів криміналізації та визначено особливості української моделі.

Для забезпечення порівнюваності нормативного матеріалу використано сім аналітичних осей. Перша – ***антидержавна***, яка дала змогу встановити, чи залежить спеціальний характер діяння від мети суб'єкта, об'єктивної здатності заподіяти шкоду державним інтересам або взагалі не передбачає спеціальної антидержавної спрямованості. Друга – ***іноземно-агентурна***, за якою з'ясовували значення зв'язку діяння з іноземною державою, її розвідкою, органом, організацією або іншим іноземним суб'єктом. Такий зв'язок оцінювали залежно від його законодавчої функції як конструктивний, кваліфікуючий, диференціюючий або юридично незначущий для відповідного складу. Третю – ***функціональну – вісь*** використовували для встановлення співвідношення фізичного пошкодження та порушення операційної спроможності об'єкта або системи. Аналізували, чи вимагає закон знищення або пошкодження матеріального носія, чи визнає самостійно кримінально значущими втрату функціональності, обмеження доступу, зниження ефективності, надійності або працездатності, припинення чи істотне порушення функціонування. Четверта – ***інфраструктурна – вісь*** стосувалася способу визначення спеціальної значущості охоронюваного об'єкта. З'ясовували, чи встановлюється вона через закритий або відкритий перелік матеріальних об'єктів, належність до критичної або життєво важливої інфраструктури, характер послуги, що забезпечує система, або через суспільну чи державну функцію, виконання якої поставлено під загрозу. П'яту – ***превентивну – вісь*** використовували для визначення того, наскільки кримінально-правова заборона поширюється на поведінку, що передує безпосередньому функціональному ураженню системи. Порівнювали караність замаху, готування, змови, розвідки об'єктів, виготовлення чи придбання спеціальних засобів, створення технічних або програмних вразливостей, агентурної підготовки та планування майбутнього саботажного посягання. Ступінь віддалення самостійно криміналізованої поведінки від моменту фактичного ураження охоронюваного об'єкта або функції використано для характеристики превентивної глибини криміналізації. Шоста – ***диференціююча – вісь*** дала змогу встановити критерії зміни ступеня кримінальної відповідальності: тяжкість наслідків, масштаб функціонального порушення, форму вини, зв'язок з іноземною державою, особливий статус об'єкта, вчинення діяння під час війни або в інших надзвичайних умовах. Сьому –

архітектурну – вісь використовували для визначення способу системного розміщення відповідних заборон: автономного складу, диференційованого комплексу спеціальних складів або децентралізованої моделі, за якої різні вияви функціонально спорідненої діяльності криміналізують кількома нормами.

Формально-юридичний метод застосовано для встановлення змісту та меж відповідних кримінально-правових заборон; порівняльно-правовий – для їх зіставлення за визначеними критеріями; системний – для з'ясування місця відповідних складів у структурі кримінального законодавства та їх взаємозв'язку із суміжними нормами. Функціональний метод став основним для виявлення нормативно різних, але функціонально еквівалентних способів кримінально-правової охорони. Типологізацію використано на завершальному етапі для встановлення повторюваних механізмів криміналізації та їх комбінацій у конкретних національних моделях.

Результати й обговорення

1. Від диверсії до саботажу: межі функціональної еквівалентності кримінально-правових заборон. Порівняльно-правове дослідження кримінальної відповідальності за диверсійно-саботажну діяльність ускладнюється відсутністю універсальної термінології для позначення відповідних кримінальних правопорушень, прийнятної в різних державах. Уже на рівні їх найменувань простежуються істотні відмінності. Законодавство Франції, Швеції, Фінляндії, Великої Британії та Австралії оперує поняттям «саботаж» (*sabotage*)[1]; КК Чехії – поняттям «саботаж» (*sabotáž*)[2]; польський законодавець одночасно використовує поняття «диверсія» (*dywersja*) та «саботаж» (*sabotaż*)[3]. Латвійське поняття *kaitniecība* в актуальному офіційному англомовному перекладі також перекладається як «саботаж» (*sabotage*), хоча в попередніх перекладах використовували поняття «підривна діяльність» (*subversion*)[4]. Водночас у Норвегії функціонально близьке посягання визначено як «напад на інфраструктуру» (*attack on infrastructure*)[5], а в Естонії – як «втручання в життєво важливі системи суспільного забезпечення або їх пошкодження» (*interference with or damaging vital public utilities systems*)[6]. У ФРН поняття саботажу використовують для позначення кількох різних за змістом кримінально-правових заборон, а не одного універсального складу кримінального правопорушення[7].

Особливо показовою є польська законодавча модель. У ст. 130 §7 КК Польщі поряд названо диверсію (*dywersja*) і саботаж (*sabotaż*), що вчиняють у межах діяльності іноземної розвідки або на її користь[8]. Отже, законодавець не ототожнює ці поняття на рівні термінології, водночас не відображає їх зміст безпосередньо в диспозиції. Саме ця обставина стала одним із предметів сучасної польської наукової дискусії. L. Rosicki та R. Rosicki (2025) акцентують на складності визначення меж нових кримінально-правових заборон, а P. Burczaniuk (2024) і P. Chlebowicz (2026) – на проблемності їх включення до оновленої системи протидії діяльності іноземних розвідок.

Цей приклад має ширше методологічне значення. Він засвідчує помилковість підходу, за якого іншомовне поняття *sabotage* автоматично визнають точним юридичним відповідником української «диверсії», а *dywersja* – лише її мовним еквівалентом. Однакові або близькі за звучанням назви можуть приховувати істотно різні конструкції складів кримінальних правопорушень. І, навпаки, норми з різними назвами можуть виконувати близьку кримінально-правову функцію.

Про концептуальну неоднорідність поняття саботажу зазначають й J. Rovner, R. Cormac і L. Maschmeyer (2025). Вони пов'язують його насамперед із погіршенням функціонування певної системи, а не виключно з її фізичним знищенням. Для кримінально-правового порівняння це вкрай важливо, оскільки дає змогу змістити фокус із зовнішньої форми діяння на характер того деструктивного результату, до якого воно спрямоване.

Водночас функціональний підхід не дає підстав відносити до диверсійно-саботажних будь-

[1] Code pénal, art. 410-1, 411-9. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418361?utm_source=chatgpt.com; Brottsbalk (1962:700), 13 kap. 4, 5, 12 §§. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700-s/?utm_source=chatgpt.com; Rikoslaki (39/1889), 34 luku, 1–3, 9 §. URL: https://www.finlex.fi/en/legislation/1889/39-001/amendment-history/20250250?utm_source=chatgpt.com; National Security Act 2023, c. 32, ss. 12, 18. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents?utm_source=chatgpt.com; Criminal Code Act 1995 (Cth), Criminal Code, Division 82. URL: https://www.legislation.gov.au/C2004A04868/latest/text?utm_source=chatgpt.com

[2] Zákon č. 40/2009 Sb., trestní zákoník, § 314. URL: https://mze.gov.cz/public/portal/mze/legislativa/vap68040-88168?utm_source=chatgpt.com

[3] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 130, 140. URL: https://eli.gov.pl/api/acts/DU/2024/17/text.html?utm_source=chatgpt.com

[4] Krimināllikums, 89. pants. URL: https://likumi.lv/ta/en/en/id/88966?utm_source=chatgpt.com

[5] Lov om straff (straffeloven), *LOV-2005-05-20-28*, §§ 192–193, 196. URL: https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL_2-5#%C2%A7196

[6] Karistusseadustik (Penal Code), §§ 232–233, 406. URL: https://www.riigiteataja.ee/en/akt/506032020002?leiaKehtiv

[7] Strafgesetzbuch (StGB), §§ 87, 88, 109e. URL: https://www.gesetze-im-internet.de/stgb/__87.html?utm_source=chatgpt.com

[8] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 130, 140. URL: https://eli.gov.pl/api/acts/DU/2024/17/text.html?utm_source=chatgpt.com

які посягання на інфраструктуру, транспортні мережі або інформаційні системи. За такого надмірно широкого розуміння до порівнюваної групи потрапили б звичайне умисне пошкодження майна, транспортні й комп'ютерні кримінальні правопорушення, які не мають спеціальної антидержавної або системно-суспільної спрямованості. F. Billing і B. Feldtmann (2024), аналізуючи можливості кримінального права в протидії гібридним атакам, також акцентують на необхідності відмежування звичайної злочинної поведінки від посягань, що використовують уразливості держави та її критично важливих систем у ширшому безпековому контексті.

З огляду на це, у порівняльно-правовому аналізі доцільно розрізняти номінативну, структурну та функціональну еквівалентність кримінально-правових заборон. Номінативна еквівалентність ґрунтується на подібності їх назв і має найменше пізнавальне значення. Структурна характеризує подібність окремих ознак складу кримінального правопорушення – предмета, діяння, мети, наслідків чи обстановки. Функціональна еквівалентність означає, що різні за назвою та юридичною конструкцією заборони спрямовані на протидію умисному ураженню спроможності держави, її оборонного потенціалу, інституцій або життєво важливих суспільних систем виконувати покладені на них функції.

Саме функціональна еквівалентність має бути вихідним критерієм порівняння. Зокрема, це пояснює включення до досліджуваної групи Кримінального кодексу Норвегії, у якому §192 не використовує терміна «саботаж», але криміналізує спричинення масштабного порушення функціонування публічного управління або суспільства шляхом знищення, пошкодження чи виведення з ладу інформаційних масивів, енергетичних, мовленнєвих, електронно-комунікаційних і транспортних систем[1]. Схожою є й відповідна норма в Кримінальному кодексі Естонії. § 406 цього Кодексу охоплює порушення або припинення функціонування життєво важливої системи, якщо це становить небезпеку, зокрема безпеці, незалежності або територіальній цілісності держави[2].

Отже, зарубіжні аналоги диверсії не можна визначати лише за лексичною відповідністю назви кримінального правопорушення. Порівнянню мають підлягати функціонально споріднені кримінально-правові заборони незалежно від того, чи називає їх законодавець диверсією, саботажем, підривною діяльністю, нападом на інфраструктуру, втручанням у життєво важливі системи або розподіляє відповідну охорону між кількома самостійними нормами. Водночас функціональний критерій встановлює й межі такого порівняння, не допускаючи механічного включення всіх правопорушень, предметом яких є інфраструктурний або інформаційний об'єкти.

2. Базові механізми криміналізації диверсійно-саботажних посягань. Зіставлення засвідчило, що національні підходи недоцільно розподіляти на взаємовиключні «диверсійні», «саботажні» чи «інфраструктурні» моделі. У межах однієї нормативної конструкції можуть одночасно поєднуватися декілька юридичних механізмів, за допомогою яких поведінка набуває спеціальної кримінально-правової якості. Тому продуктивнішим є виокремлення базових механізмів криміналізації, різні комбінації яких формують конкретні національні моделі.

Першим із них є *цільовий механізм*, за якого спеціальний характер посягання визначають його суб'єктивною антидержавною спрямованістю. Саме така логіка є основою ст. 113 КК України, що пов'язує всі передбачені нею форми диверсії з метою ослаблення держави. Такий підхід використовують Чехія та Латвія, хоча їх законодавчі конструкції істотно відрізняються від української за способом опису об'єктивної сторони.

Зокрема, §314 КК Чехії вимагає наміру зашкодити конституційному устрою або обороноздатності Чеської Республіки чи міжнародної організації. Водночас відповідне діяння описано не через перелік конкретних руйнівних способів, а через зрив або ускладнення виконання важливого завдання, порушення чи інше серйозне заподіяння шкоди діяльності органу влади, збройних сил, органу безпеки, економічної організації або іншої установи[3].

Латвійська законодавча конструкція також пов'язує саботаж з метою завдати шкоди Латвійській Республіці. Проте його об'єктивна сторона може полягати в дії або бездіяльності, спрямованій на підрив фінансової системи, промислового, транспортного, сільськогосподарського, торговельного чи іншого сектору економіки або діяльності установ й організацій[4].

Отже, спеціальна антидержавна мета не зумовлює необхідності казуїстичного опису об'єктивної сторони. Цільовий механізм цілком сумісний із функціонально сформульованим діянням. Це має важливе значення для оцінки можливих напрямів модернізації ст. 113 КК України, оскільки спростовує припущення, ніби посилення функціонального компонента норми обов'язково потребує відмови від мети ослаблення держави.

Другим є *іноземно-агентурний механізм*, у якому спеціальна кримінально-правова якість діяння пов'язана з його належністю до діяльності

[1] Lov om straff (straffeloven), LOV-2005-05-20-28, §§ 192–193, 196. URL: https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL_2-5#%C2%A7196

[2] Karistusseadustik (Penal Code), §§ 232–233, 406. URL: https://www.riigiteataja.ee/en/akt/506032020002?leiaKehtiv

[3] Zákon č. 40/2009 Sb., trestní zákoník, § 314. URL: https://mze.gov.cz/public/portal/mze/legislativa/vap68040-88168?utm_source=chatgpt.com

[4] Krimināllikums, 89. pants. URL: https://likumi.lv/ta/en/en/id/88966?utm_source=chatgpt.com

іноземної держави, її розвідки або іншого іноземного суб'єкта.

Найбільш послідовно такий механізм реалізовано у Великій Британії. За ст. 12 Закону про національну безпеку 2023 року (*National Security Act 2023*) склад саботажу передбачає, крім відповідної шкоди активу та спрямованості проти безпеки чи інтересів держави, умову зв'язку з іноземною державою (*foreign power condition*)[1]. Отже, такий зв'язок є конструктивною ознакою саме цього складу. Такий спосіб конструювання відповідає загальній логіці британської реформи 2023 року, у межах якої зв'язок з іноземною державою набув системоутворюючого значення для кримінально-правового реагування на низку загроз національній безпеці. R. Ward (2024), аналізуючи нову систему відповідних кримінально-правових заборон, розглядає саботаж у взаємозв'язку з іншими посяганнями, для яких такий іноземний компонент має вирішальне значення.

У Польщі ст. 130 § 7 Кримінального кодексу встановлює ще вужчий зв'язок: диверсію або саботаж повинна вчиняти особа, яка бере участь у діяльності іноземної розвідки або діє на її користь[2]. У цьому випадку іноземно-агентурний компонент також є конститутивною ознакою складу кримінального правопорушення.

Інший підхід використано в КК Австралії. Зв'язок з іноземним суб'єктом (*foreign principal*) не є необхідним для всіх складів саботажу, але впливає на диференціацію кримінальної відповідальності та суворість санкції[3].

У Франції такий зв'язок має ще іншу функцію. Базовий склад саботажу не потребує доведення іноземної участі, однак мета служити інтересам іноземної держави, іноземної організації чи іншої відповідної структури утворює більш тяжкий різновид посягання[4]. Тобто такий зв'язок має диференціююче значення.

Отже, одна й та сама ознака – зв'язок з іноземною державою чи іншим іноземним суб'єктом – може виконувати різні функції: конструктивну, кваліфікуючу або диференціюючу. В інших правопорядках, зокрема Канаді, Швеції, Фінляндії, Чехії та Латвії, такий зв'язок взагалі не є необхідною ознакою відповідних складів кримінальних правопорушень.

Третім є *інтересоцентричний механізм*, який послідовно представлений у кримінальному законодавстві Франції. Стаття 411-9 КК Франції не вимагає спеціальної мети, аналогічної українській меті ослаблення держави. Спеціальну якість саботажу визначають тим, що відповідні дії за своїм характером здатні завдати шкоди фундаментальним інтересам нації (*intérêts fondamentaux de la nation*)[5].

Антидержавний характер відповідного посягання може бути нормативно сконструйований двома принципово різними способами. У першому випадку він суб'єктивується через спеціальну антидержавну мету особи; у другому – об'єктивується через характер охоронюваного державного інтересу та здатність діяння створити для нього небезпеку. Саме це розмежування дає змогу пояснити, чому зовні схожі акти пошкодження або втручання набувають спеціальної кримінально-правової якості в різних правопорядках за різними юридичними підставами.

Четвертим є *функціонально-інфраструктурний механізм*. Його визначальною рисою є перенесення нормативного акценту з матеріальної цілісності конкретної речі на здатність об'єкта, системи, мережі або установи виконувати суспільно чи державно значущу функцію. У різних формах цей механізм використовують Канада, Австралія, Швеція, Фінляндія, Норвегія та Естонія; істотні його елементи наявні також у ФРН, Чехії та Латвії.

Виокремлені механізми не є взаємовиключними. Британська модель поєднує іноземно-агентурний і функціональний механізми; чеська та латвійська – цільовий і функціональний; французька – інтересоцентричний механізм із кваліфікуючим значенням зв'язку з іноземною державою; австралійська – функціонально-інфраструктурний механізм із диференціюючим значенням іноземного компонента та розвиненою превентивною складовою. Тому національна модель криміналізації не є одиницею лінійної класифікації, а являє собою певну конфігурацію різних механізмів. Саме їх співвідношення визначає, чому законодавець надає конкретному діянню підвищеного кримінально-правового значення, який вид шкоди визнає визначальним і наскільки широко поширює кримінально-правову заборону.

3. Від пошкодження об'єкта до порушення функції: функціональний поворот у криміналізації саботажу. Найвиразнішою закономірністю, виявленою під час аналізу досліджених правопорядків, є зміна самого способу нормативного опису кримінально значущої шкоди. Традиційний підхід пов'язує її насамперед із фізичним впливом на матеріальний об'єкт – його знищенням, пошкодженням або приведенням у непридатний стан. У сучасних конструкціях дедалі більшого значення набуває інший критерій: не те, що

[1] National Security Act 2023, c. 32, ss. 12, 18. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents?utm_source=chatgpt.com

[2] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, art. 130, 140. URL: https://eli.gov.pl/api/acts/DU/2024/17/text.html?utm_source=chatgpt.com

[3] Criminal Code Act 1995 (Cth), Criminal Code, Division 82. URL: https://www.legislation.gov.au/C2004A04868/latest/text?utm_source=chatgpt.com

[4] Code pénal, art. 410-1, 411-9. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418361?utm_source=chatgpt.com

[5] Code pénal, art. 410-1, 411-9. URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418361?utm_source=chatgpt.com

фізично сталося з річчю, а те, чи зберегла відповідна система здатність виконувати своє призначення.

Виразно такий підхід реалізовано в законодавстві Великої Британії. Стаття 12 Закону про національну безпеку 2023 року широко визначає поняття шкоди (*damage*). Воно охоплює не лише знищення чи фізичну зміну активу, а й втручання в нього, втрату або зменшення доступності, втрату чи зниження функціональності, корисності або надійності. Шкода може бути як постійною, так і тимчасовою, а поняття активу поширюється не лише на матеріальні речі, а й на електронні системи та інформацію[1].

Канадська модель демонструє функціоналізацію ще виразніше. Загальний склад саботажу охоплює не тільки пошкодження речі, а й дію чи бездіяльність, яка знижує ефективність або перешкоджає нормальній роботі відповідного об'єкта. Спеціальний склад саботажу щодо життєво важливої інфраструктури (*essential infrastructure*), запроваджений 2024 року, охоплює, зокрема, перешкоджання доступу до такої інфраструктури, її втрату, приведення в непрацездатний, небезпечний або не придатний для використання стан[2]. Важливо, що канадський законодавець визначає спеціальне значення інфраструктури через послуги, які вона забезпечує: транспортні, інформаційно-комунікаційні, водні, енергетичні, медичні, продовольчі, урядові, фінансові тощо. Отже, цінність відповідного об'єкта визначають не лише його фізичними властивостями, а й функцією, від безперервного виконання якої залежить життєдіяльність суспільства.

Австралійське законодавство також виходить далеко за межі фізичного пошкодження. У розділі 82 (*Division 82*) Кримінального кодексу шкода публічній інфраструктурі охоплює її знищення, втрату, приведення в непридатний стан, втрату функціональності чи доступу, істотне погіршення, а щодо електронних систем – серйозне порушення їх роботи. Тож фізичне пошкодження є лише одним із можливих виявів кримінально значущого ураження[3].

Схожу тенденцію демонструє кримінальне законодавство ФРН. § 88 КК ФРН пов'язує відповідальність, зокрема з повним або частковим припиненням діяльності підприємств, установок і систем або позбавленням можливості використовувати їх відповідно до призначення. §87 так само охоплює поведінку, якою перешкоджають або істотно порушують роботу підприємств, важливих для оборони, цивільного захисту чи економіки[4].

У Швеції склад саботажу також не зводиться до знищення або пошкодження матеріального предмета. Кримінально значущим є серйозне порушення або перешкоджання використанню об'єктів і засобів, важливих для оборони, продовольчого забезпечення, правосуддя, державного управління, громадського порядку, транспорту, зв'язку, водо-, тепло- й енергопостачання[5].

Фінський КК поряд із матеріально-деструктивними діями охоплює неправомірне втручання у функціонування виробничої, розподільчої або інформаційної системи, якщо це спричиняє серйозну небезпеку енергопостачанню, охороні здоров'я, обороні, правосуддю чи іншій співмірній за значенням суспільній функції[6]. Тут нормативний акцент уже прямо перенесено з речі на суспільно значущу функцію.

Найпослідовніше така логіка простежується в Норвегії. §192 КК Норвегії ґрунтується навколо масштабного порушення функціонування публічного управління або суспільства загалом, чого досягають через вплив на інформаційні масиви, енергетичні, мовленнєві, електронно-комунікаційні або транспортні системи. Визначальним стає не матеріальний стан окремого об'єкта, а масштаб функціонального результату[7] .

Схожий підхід використано й в Естонії, де §406 КК поряд з пошкодженням або знищенням елементів життєво важливої системи самостійно називає порушення або припинення її функціонування, якщо це становить небезпеку життю чи здоров'ю людей або безпеці, незалежності чи територіальній цілісності держави[8].

Ця тенденція вкрай важлива в умовах цифровізації. S. Haataja (2022) акцентує, що ураження критичної інфраструктури в кіберпросторі може полягати не лише у фізичному пошкодженні, а й в порушенні можливості її використання або роботи. У цифрових й автоматизованих системах бажаного для правопорушника деструктивного результату нерідко досягають без фізичного знищення сервера, мережевого обладнання чи іншого матеріального носія.

---

[1] National Security Act 2023, c. 32, ss. 12, 18. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents?utm_source=chatgpt.com

[2] Criminal Code, R.S.C. 1985, c. C-46, ss. 52–52.2. URL: https://laws-lois.justice.gc.ca/eng/acts/C-46/section-52.html?utm_source=chatgpt.com

[3] Independent National Security Legislation Monitor. Review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences in Division 82 and Part 5.2 of the Criminal Code Act 1995. 2026. URL: https://www.inslm.gov.au/reviews/review-australias-espionage-foreign-interference-sabotage-and-theft-trade-secrets-offences-division-82-and-part-52-criminal-code-act-1995?utm_source=chatgpt.com

[4] Strafgesetzbuch (StGB), §§ 87, 88, 109e. URL: https://www.gesetze-im-internet.de/stgb/__87.html?utm_source=chatgpt.com

[5] Brottsbalk (1962:700), 13 kap. 4, 5, 12 §§. URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700-s/?utm_source=chatgpt.com

[6] Rikoslaki (39/1889), 34 luku, 1–3, 9 §. URL: https://www.finlex.fi/en/legislation/1889/39-001/amendment-history/20250250?utm_source=chatgpt.com

[7] Lov om straff (straffeloven), LOV-2005-05-20-28, §§ 192–193, 196. URL: https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL_2-5#%C2%A7196

[8] Karistusseadustik (Penal Code), §§ 232–233, 406. URL: https://www.riigiteataja.ee/en/akt/506032020002?leiaKehtiv

Практика сучасної саботажної діяльності додатково підтверджує таку трансформацію характеру деструктивного впливу. S. G. Jones (2025), аналізуючи російську саботажну кампанію в Європі, зауважує, що поряд із підпалами, вибухами та фізичними посяганнями на інфраструктуру застосовують електронні й кібернетичні засоби впливу. Це підтверджує, що фізичне пошкодження матеріального об'єкта вже не можна розглядати як універсальний спосіб опису сучасної диверсійно-саботажної діяльності.

На підставі цього може йтися про зміну функціональної парадигми криміналізації диверсійно-саботажних посягань. Її сутність полягає в зміщенні центру кримінально-правової охорони від матеріальної цілісності стратегічно важливого об'єкта до його операційної спроможності – доступності, надійності, ефективності функціонування, можливості використання за призначенням і безперервності забезпечення критично важливої суспільної або державної функції. Така зміна не означає відмови від охорони матеріального об'єкта. У більшості досліджених законодавств знищення або пошкодження залишається типовою формою саботажного впливу. Змінюється інше: матеріальна шкода перестає бути єдиною нормативною формою опису деструктивного результату. Поряд з нею самостійного значення набувають втрата функціональності, обмеження доступу, зниження ефективності чи надійності, припинення роботи, істотне порушення функціонування або дезорганізація відповідної системи. Умовно цей розвиток можна представити як послідовність: «знищення» → «пошкодження» → «приведення у непридатний стан» → «обмеження доступу» → «зниження працездатності або надійності» → «припинення чи істотне порушення функціонування» → «дезорганізація важливої суспільної або державної функції». Ідеться не про стадії одного кримінального правопорушення, а про різні способи нормативного осмислення шкоди.

У цьому контексті конструкція ст. 113 КК України має виразну специфіку. У частині посягань на важливі об'єкти законодавець пов'язує диверсію з діями, спрямованими на їх зруйнування або пошкодження. Окремого функціонального відповідника – виведення з ладу, припинення чи істотного порушення функціонування – диспозиція не містить. Це не означає, що будь-який функціональний вплив автоматично знаходиться поза межами ст. 113 КК, однак буквальна конструкція норми не надає функціональному ураженню самостійного нормативного значення.

Саме тому перспективи модернізації ст. 113 КК не слід зводити до заміни словосполучення «об'єкти, які мають важливе народногосподарське чи оборонне значення» поняттям «об'єкти критичної інфраструктури». Така зміна осучаснила б предметну термінологію, але зберегла б ту саму об'єктно-матеріальну логіку. Порівняльний матеріал засвідчує, що важливішим є нормативне визнання кримінально-правового значення самого порушення критично важливої функції, незалежно від того, супроводжується воно фізичним знищенням відповідного матеріального носія чи ні.

4. Від заподіяння шкоди до створення здатності її заподіяти: превентивна глибина криміналізації. Паралельно із функціональним зміщенням у досліджених правопорядках простежується інша тенденція – перенесення кримінально-правового реагування на ранні етапи формування саботажної загрози. У традиційній моделі відповідальність за поведінку, що передує закінченому кримінальному правопорушенню, переважно забезпечують загальними положеннями про готування та замах. Частина сучасних законодавств прямує далі, створюючи спеціальні склади підготовчої поведінки, пристосовані саме до особливостей саботажної діяльності.

Найрозгорнутіший підхід демонструє Австралія. Розділ 82 Кримінального кодексу цієї держави поряд із закінченими формами саботажу передбачає окрему відповідальність за створення вразливості (*introducing vulnerability*), а також підготовку або планування саботажу (*preparing for or planning sabotage offence*)[1]. Причому караність планування не залежить від фактичного вчинення майбутнього саботажу чи навіть остаточної індивідуалізації конкретного майбутнього діяння.

Це має принципове значення. Кримінально значущим стає не лише підготовлення особи до майбутнього посягання, а й формування всередині системи технічної або програмної вразливості, яку може бути використано згодом. Отже, превентивне кримінально-правове реагування переноситься на етап створення здатності до майбутнього функціонального ураження.

У Великій Британії окремо криміналізовано підготовчу поведінку (*preparatory conduct*) щодо низки кримінальних правопорушень, пов'язаних із загрозами державі, серед яких і саботаж [2]. Особливість такої конструкції полягає в тому, що майбутнє основне посягання не повинно бути вже вчинене або повністю конкретизоване.

Канада використовує предметно орієнтований спосіб превентивної криміналізації. Кримінальний кодекс передбачає окрему відповідальність за виготовлення, володіння, продаж чи поширення засобу, призначеного для саботажу, причому поняття такого засобу безпосередньо охоплює комп'ютерну програму. Це дає змогу

[1] Independent National Security Legislation Monitor. Review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences in Division 82 and Part 5.2 of the Criminal Code Act 1995. 2026. URL: https://www.inslm.gov.au/reviews/review-australias-espionage-foreign-interference-sabotage-and-theft-trade-secrets-offences-division-82-and-part-52-criminal-code-act-1995?utm_source=chatgpt.com

[2] National Security Act 2023, c. 32, ss. 12, 18. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents?utm_source=chatgpt.com

адаптувати превентивну криміналізацію до цифрових способів ураження систем.

У ФРН §87 КК фактично містить розгорнутий перелік агентурно-підготовчої поведінки: розвідку потенційних об'єктів, виготовлення, придбання, зберігання або передачу відповідних засобів, створення баз, підготовку чи навчання осіб, встановлення та підтримання необхідних зв'язків[1]. У Польщі ст. 130 §8 окремо криміналізує готування до передбачених попереднім параграфом диверсії чи саботажу. Норвезький КК передбачає спеціальну відповідальність за змову щодо нападу на інфраструктуру[2], а §314 КК Чехії прямо встановлює караність готування до саботажу[3].

Ці відмінності дають змогу запропонувати для порівняльно-правового аналізу категорію «превентивна глибина криміналізації» – ступінь часової та причинової віддаленості самостійно криміналізованої поведінки від фактичного функціонального ураження охоронюваної системи чи державного інтересу. Умовно її можна представити як послідовність: «замах» → «загальне готування» → «спеціальна змова» → «створення або придбання засобів саботажу» → «розвідка майбутнього об'єкта» → «агентурна підготовка» → «створення технічної чи програмної вразливості» → «планування ще не конкретизованого майбутнього посягання».

Однак збільшення превентивної глибини криміналізації не свідчить про досконалість відповідної законодавчої моделі. Навпаки, що далі межа кримінальної відповідальності відсувається від безпосереднього заподіяння шкоди, то гостріше постають вимоги юридичної визначеності, пропорційності й необхідності використання кримінального права як крайнього засобу (*ultima ratio*). Важливе значення має також доведення достатньо конкретного зв'язку між підготовчою поведінкою та майбутнім саботажним посяганням.

У цьому аспекті показовим є перегляд австралійського законодавства незалежним монітором законодавства у сфері національної безпеки (*Independent National Security Legislation Monitor*), під час якого оцінювали, зокрема, спеціальні склади створення вразливості й підготовки саботажу. Факт такої оцінки демонструє, що розширення превентивних можливостей кримінального закону потребує одночасного встановлення меж його експансії.

Для України цей результат не означає необхідності механічного запозичення спеціальних переддиверсійних складів. Сучасні способи дистанційного вербування виконавців, цифрової координації, розподілу завдань і попереднього створення технічних умов для майбутнього ураження справді підвищують значення раннього кримінально-правового реагування (Richterova et al., 2024). Однак необхідність спеціальної криміналізації конкретних форм такої поведінки слід оцінювати з огляду на можливості чинних інститутів незакінченого кримінального правопорушення та суміжних складів. Інакше постає ризик переходу від відповідальності за суспільно небезпечне діяння до відповідальності за абстрактну небезпечність особи або її наміри.

5. Архітектура кримінально-правової охорони та місце України серед порівнюваних моделей. Поряд із відмінностями в змісті конкретних заборон порівняльне дослідження виявило різні способи їх системного розміщення в кримінальному законодавстві. Цей параметр слід відокремлювати від базових механізмів криміналізації, оскільки він характеризує не джерело спеціальної суспільної небезпечності посягання, а архітектуру кримінально-правової охорони.

Першою є *автономна архітектура*, за якої основний зміст заборони концентрується в одному спеціальному складі. Такий підхід використовують, зокрема, Велика Британія, Франція, Чехія та Латвія. Водночас автономність не означає змістової однорідності: британська конструкція тяжіє до іноземно-агентурної моделі, французька – до інтересоцентричної, чеська й латвійська – до поєднання цільового та функціонального механізмів.

Другою є *диференційована комплексна архітектура*, за якої різні вияви саботажної діяльності розподіляються між кількома взаємопов'язаними спеціальними складами. У Канаді поряд із загальним складом саботажу передбачено окремий склад саботажу щодо життєво важливої інфраструктури й відповідальність за дії із засобами, призначеними для саботажу[4]. В Австралії розділ 82 Кримінального кодексу утворює розгалужену систему, що диференціює відповідальність залежно від форми психічного ставлення, зв'язку з іноземним суб'єктом, створення вразливості та підготовки чи планування майбутнього посягання[5].

Третьою є *децентралізована архітектура*, за якої законодавець не прагне охопити всі функціонально споріднені вияви одним універсальним складом. Показовим є КК ФРН, у якому окремо передбачено агентурну діяльність із саботажною метою, антиконституційний саботаж і

[1] Strafgesetzbuch (StGB), §§ 87, 88, 109e. URL: https://www.gesetze-im-internet.de/stgb/__87.html?utm_source=chatgpt.com

[2] Lov om straff (straffeloven), LOV-2005-05-20-28, §§ 192–193, 196. URL: https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL_2-5#%C2%A7196

[3] Zákon č. 40/2009 Sb., trestní zákoník, § 314. URL: https://mze.gov.cz/public/portal/mze/legislativa/vap68040-88168?utm_source=chatgpt.com

[4] Criminal Code, R.S.C. 1985, c. C-46, ss. 52–52.2. URL: https://laws-lois.justice.gc.ca/eng/acts/C-46/section-52.html?utm_source=chatgpt.com

[5] Independent National Security Legislation Monitor. Review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences in Division 82 and Part 5.2 of the Criminal Code Act 1995. 2026. URL: https://www.inslm.gov.au/reviews/review-australias-espionage-foreign-interference-sabotage-and-theft-trade-secrets-offences-division-82-and-part-52-criminal-code-act-1995?utm_source=chatgpt.com

саботаж щодо засобів оборони[1]. В Естонії функціональне ураження життєво важливих систем також відокремлено від кримінальних правопорушень, пов'язаних із наданням допомоги іноземній державі в діяльності проти незалежності, суверенітету або територіальної цілісності країни[2].

Отже, децентралізація не означає неповноту кримінально-правової охорони. Вона може бути результатом свідомого законодавчого рішення не об'єднувати в одному складі посягання, що істотно різняться за охоронюваним інтересом, механізмом заподіяння шкоди або характером спеціальної спрямованості.

На цьому тлі українська конструкція має виразну специфіку. Стаття 113 КК поєднує в одній нормі дії, спрямовані на масове знищення людей чи заподіяння шкоди їх здоров'ю; зруйнування або пошкодження об'єктів, які мають важливе народногосподарське чи оборонне значення; радіоактивне забруднення; масове отруєння; поширення епідемій, епізоотій та епіфітотій. Спільною ознакою всіх цих різнорідних форм є мета ослаблення держави.

За результатами здійсненого дослідження українську конструкцію можна визначити як *автономну цільову модель диверсії казуїстично-об'єктного типу*. Її антидержавний характер формується спеціальною метою ослаблення держави; об'єктивна сторона – через перелік різнорідних напрямів і способів деструктивного впливу; зв'язок з іноземною державою не є конструктивною ознакою; а диференціація відповідальності в ч. 2 ст. 113 КК здійснюється за ознакою вчинення тих самих діянь в умовах воєнного стану або в період збройного конфлікту. Таку характеристику не слід сприймати як автоматичну оцінку української конструкції як застарілої лише через її відмінність від зарубіжних підходів. Порівняльне право не створює ієрархії національних моделей. Британська, канадська, австралійська, французька й інші конструкції також істотно різняться між собою. Наприклад, Велика Британія вимагає обов'язкового зв'язку з іноземною державою, Канада не надає такому зв'язку конструктивного значення, а Австралія використовує його для диференціації кримінальної відповідальності.

Тому значення зарубіжного досвіду полягає не в пошуку готового зразка для запозичення, а у виявленні порівняльних розривів, які дають змогу перевірити здатність ст. 113 КК України реагувати на сучасні форми диверсійної діяльності.

Першим є матеріально-функціональний розрив. Українська норма в частині посягань на важливі об'єкти описує деструктивний результат через їх зруйнування або пошкодження, натомість у значній частині досліджених законодавств самостійного значення набувають виведення із функціонування, обмеження доступу, зниження ефективності або надійності, перешкоджання використанню чи істотна дезорганізація системи.

Другим є об'єктно-системний розрив. Українське законодавство оперує категорією об'єктів важливого народногосподарського чи оборонного значення, натомість низка зарубіжних конструкцій визначає спеціальну значущість через систему, мережу, послугу або суспільну функцію. Показовою є Канада, де життєво важливу інфраструктуру визначають через послуги, необхідні для здоров'я, безпеки, захищеності чи економічного добробуту населення[3]. У Фінляндії значення має створення серйозної небезпеки енергопостачанню, охороні здоров'я, обороні, правосуддю чи іншій важливій суспільній функції[4] , а в Норвегії – масштабне порушення функціонування суспільства або публічного управління[5].

Третім є цифрово-функціональний розрив. У цифровому середовищі припинення чи істотного порушення функціонування системи може бути досягнуто без фізичного пошкодження її матеріального носія. Британське законодавство безпосередньо охоплює електронні системи й інформацію[6]; канадське – комп'ютерні програми як можливі засоби саботажу[7]; австралійське – серйозне порушення роботи електронних систем і створення їх уразливості[8]; фінське – втручання у функціонування інформаційної системи[9]. Це підтверджує, що функціональна конструкція має самостійне значення, а не є лише новою назвою традиційного фізичного пошкодження.

Четвертим є превентивний розрив. Стаття 113 КК України функціонує разом із загаль-

---

[1] Strafgesetzbuch (StGB), §§ 87, 88, 109e. URL: https://www.gesetze-im-internet.de/stgb/__87.html?utm_source=chatgpt.com

[2] Karistusseadustik (Penal Code), §§ 232–233, 406. URL: https://www.riigiteataja.ee/en/akt/506032020002?leiaKehtiv

[3] Criminal Code, R.S.C. 1985, c. C-46, ss. 52–52.2. URL: https://laws-lois.justice.gc.ca/eng/acts/C-46/section-52.html?utm_source=chatgpt.com

[4] Rikoslaki (39/1889), 34 luku, 1–3, 9 §. URL: https://www.finlex.fi/en/legislation/1889/39-001/amendment-history/20250250?utm_source=chatgpt.com

[5] Lov om straff (straffeloven), LOV-2005-05-20-28, §§ 192–193, 196. URL: https://lovdata.no/dokument/NLE/lov/2005-05-20-28/KAPITTEL_2-5#%C2%A7196

[6] National Security Act 2023, c. 32, ss. 12, 18. URL: https://www.legislation.gov.uk/ukpga/2023/32/contents?utm_source=chatgpt.com

[7] Criminal Code, R.S.C. 1985, c. C-46, ss. 52–52.2. URL: https://laws-lois.justice.gc.ca/eng/acts/C-46/section-52.html?utm_source=chatgpt.com

[8] Independent National Security Legislation Monitor. Review of Australia's espionage, foreign interference, sabotage and theft of trade secrets offences in Division 82 and Part 5.2 of the Criminal Code Act 1995. 2026. URL: https://www.inslm.gov.au/reviews/review-australias-espionage-foreign-interference-sabotage-and-theft-trade-secrets-offences-division-82-and-part-52-criminal-code-act-1995?utm_source=chatgpt.com

[9] Rikoslaki (39/1889), 34 luku, 1–3, 9 §. URL: https://www.finlex.fi/en/legislation/1889/39-001/amendment-history/20250250?utm_source=chatgpt.com

ними положеннями про незакінчене кримінальне правопорушення, натомість окремі зарубіжні законодавства спеціально типізують певні форми поведінки, що передують саботажу. Водночас цей розрив найменше виправдовує пряме запозичення, оскільки спеціальна превентивна кримналізація потребує окремого обґрунтування її необхідності, пропорційності та співвідношення з уже чинними заборонами.

Окремим напрямом порівняння є диференціація відповідальності залежно від особливої обстановки. Частина 2 ст. 113 КК України пов'язує більш сувору відповідальність із вчиненням тих самих діянь в умовах воєнного стану або в період збройного конфлікту. Схожий підхід використано в Чехії, де відповідна особлива обстановка безпосередньо впливає на кваліфікацію саботажу[1]. Натомість у Фінляндії війна чи інші надзвичайні умови є лише одним із критеріїв тяжкого саботажу й повинні поєднуватися з оцінкою всього посягання як тяжкого[2]. Це свідчить про відсутність єдиного порівняльно-правового вирішення питання щодо значення воєнної обстановки.

Порівняльний матеріал також не підтверджує доцільності перетворення зв'язку з іноземною державою на обов'язкову ознаку української диверсії. Британська та польська моделі справді дають змогу чітко виокремити саботаж, організований або підтримуваний іноземною державою. Однак досвід Канади, Швеції, Фінляндії, Чехії та Латвії засвідчує, що спеціальна небезпечність такого посягання може бути нормативно сформована й без обов'язкового іноземного компонента. Його включення до ст. 113 КК України як конструктивної ознаки необґрунтовано звузило б сферу її застосування.

Так само дослідження не підтверджує необхідності перейменування «диверсії» на «саботаж». Навпаки, відмінність змісту однойменних складів у Великій Британії, Франції, Швеції, Фінляндії та інших державах демонструє обмеженість суто термінологічної модернізації. Функціонально близькі моделі Норвегії та Естонії взагалі не потребують використання поняття «саботаж».

Перспективнішим видається функціональний напрям модернізації ст. 113 КК України. Його сутність полягає не в механічному запозиченні іншомовної назви та не в простому розширенні переліку предметів, а у визнанні поряд зі зруйнуванням і пошкодженням самостійного кримінально-правового значення виведення з ладу, істотного припинення, порушення або дезорганізації функціонування систем, об'єктів чи мереж, від яких залежать безпека, обороноздатність, стійкість держави або забезпечення життєво важливих суспільних функцій. Така модернізація не потребує відмови від мети ослаблення держави. Навпаки, чеський і латвійський досвід підтверджує сумісність цільового механізму із функціонально сформульованою об'єктивною стороною. Це надає можливість зберегти кримінально-правову ідентичність диверсії як спеціального антидержавного посягання, водночас адаптувати її конструкцію до способів ураження сучасних фізичних, цифрових і мережевих систем.

У підсумку трансформацію сучасної криміналізації диверсійно-саботажної діяльності доцільно характеризувати не як лінійний рух від одного поняття до іншого, а як значно глибшу зміну нормативної парадигми: від матеріального об'єкта – до функціонально значущої системи; від фізичного пошкодження – до втрати операційної спроможності; від реагування на завершене ураження – до диференційованого запобігання його підготовці; від пошуку єдиного універсального складу – до поєднання різних механізмів криміналізації.

Тому для українського кримінального права актуальним є не формальний «перехід від диверсії до саботажу», а збереження диверсії як антидержавного кримінального правопорушення за функціональної модернізації її об'єктивних ознак відповідно до характеру сучасних загроз.

Висновки

Порівняльно-правовий аналіз кримінального законодавства Великої Британії, Канади, Австралії, Франції, ФРН, Польщі, Швеції, Фінляндії, Норвегії, Чехії, Латвії та Естонії засвідчив, що термінологічний критерій не є достатнім для визначення зарубіжних аналогів диверсії. Функціонально споріднені посягання можуть позначатися як диверсія, саботаж, підривна діяльність, напад на інфраструктуру, втручання в життєво важливі системи або розподілятися між кількома кримінально-правовими заборонами. У зв'язку з цим доцільно розрізняти номінативну, структурну та функціональну еквівалентність таких заборон, визнавши саме функціональну еквівалентність вихідним критерієм їх порівняння.

Встановлено, що національні підходи до криміналізації диверсійно-саботажної діяльності не утворюють системи взаємовиключних моделей. Конкретна національна модель формується через поєднання кількох базових механізмів криміналізації: цільового, за якого спеціальний характер посягання визначається антидержавною метою; іноземно-агентурного, пов'язаного з діяльністю іноземної держави, її розвідки або іншого іноземного суб'єкта; інтересоцентричного, за якого визначальною є здатність діяння заподіяти шкоду нормативно визначеним державним інтересам; функціонально-інфраструктурного, орієнтованого на збереження працездатності й

[1] Zákon č. 40/2009 Sb., trestní zákoník, § 314. URL: https://mze.gov.cz/public/portal/mze/legislativa/vap68040-88168?utm_source=chatgpt.com

[2] Rikoslaki (39/1889), 34 luku, 1–3, 9 §. URL: https://www.finlex.fi/en/legislation/1889/39-001/amendment-history/20250250?utm_source=chatgpt.com

безперервності функціонування суспільно чи державно значущих систем. За способом законодавчого оформлення відповідних заборон виокремлено автономну, диференційовану комплексну та децентралізовану архітектури кримінально-правової охорони.

Найвиразнішою закономірністю розвитку досліджених законодавств є функціональний поворот у криміналізації диверсійно-саботажних посягань. Його сутність полягає у зміщенні акценту з матеріальної цілісності стратегічно важливого об'єкта на його операційну спроможність – доступність, працездатність, надійність, можливість використання за призначенням і безперервність виконання критично важливої суспільної або державної функцій. Знищення чи пошкодження не втрачає кримінально-правового значення, однак перестає бути єдиною формою опису деструктивного результату. Самостійного значення набувають втрата функціональності, обмеження доступу, зниження ефективності, припинення роботи, істотне порушення функціонування або дезорганізація відповідної системи.

Паралельно виявлено тенденцію до поглиблення превентивної криміналізації. У низці правопорядків кримінально-правове реагування поширюється не лише на замах і загальне готування, а й на спеціально визначені форми підготовчої поведінки: змову, розвідку майбутнього об'єкта, створення чи придбання засобів саботажу, агентурну підготовку, формування технічних або програмних вразливостей, підготовку та планування майбутнього посягання. Для характеристики цього явища запропоновано поняття «превентивна глибина криміналізації» як ступінь часової та причинової віддаленості самостійно криміналізованої поведінки від фактичного функціонального ураження охоронюваної системи. Водночас збільшення такої глибини не можна оцінювати як безумовну перевагу, оскільки потребує особливо суворого дотримання вимог правової визначеності, необхідності, пропорційності та використання кримінального права як крайнього засобу.

За результатами порівняльного аналізу ст. 113 КК України доцільно характеризувати як автономну цільову модель диверсії казуїстично-об'єктного типу. Її антидержавний характер визначається спеціальною метою ослаблення держави, натомість об'єктивна сторона побудована через перелік різнорідних способів і напрямів деструктивного впливу. Порівняння із зарубіжними конструкціями дало змогу виявити насамперед матеріально-функціональний, об'єктно-системний та цифрово-функціональний розриви української моделі. Вони виявляються в недостатній нормативній самостійності функціонального ураження системи, орієнтованості переважно на матеріальний об'єкт, а не на виконувану ним критично важливу функцію, а також в обмеженій пристосованості буквального змісту норми до випадків, коли деструктивного результату досягають без фізичного пошкодження матеріального носія.

Здійснене дослідження не підтверджує доцільності ні механічного перейменування диверсії на саботаж, ні перетворення зв'язку з іноземною державою на обов'язкову ознаку ст. 113 КК України. Перспективним напрямом її модернізації є функціоналізація об'єктивної сторони – надання поряд зі зруйнуванням і пошкодженням самостійного кримінально-правового значення виведенню з ладу, істотному припиненню, порушенню або дезорганізації функціонування систем, об'єктів чи мереж, від яких залежать безпека, обороноздатність, стійкість держави або забезпечення життєво важливих суспільних функцій. Такий підхід суміщений зі збереженням мети ослаблення держави, що надає можливість зберегти кримінально-правову ідентичність диверсії як спеціального антидержавного посягання та водночас адаптувати її конструкцію до сучасних фізичних, цифрових і мережевих способів ураження.

Перспективи подальших досліджень пов'язані з визначенням оптимальної законодавчої форми функціоналізації ст. 113 КК України, встановленням меж спеціальної криміналізації поведінки, що передує диверсійному посяганню, а також окремим аналізом ч. 2 ст. 113 КК щодо значення воєнного стану та збройного конфлікту для диференціації кримінальної відповідальності.

Подяки

Немає.

Фінансування

Дослідження не фінансувалося.

Конфлікт інтересів

Немає.

References

[1] Alexopoulos, M.J., Niemi, A., Skobiej, B., & Sill Torres, F. (2025). Examination of the Critical Infrastructure Resilience Directive from the maritime point of view. *JCMS: Journal of Common Market Studies,* 63(2), 667-678. DOI: 10.1111/jcms.13681

[2] Becker, M. (2025). Transposing EU-legislation on critical infrastructure protection: Legal implementation performance in the Baltic Sea region. *International Journal of Critical Infrastructure Protection,* 50. DOI: 10.1016/j.ijcip.2025.100781

[3] Bergaust, J.C., & Sellevåg, S.R. (2024). Improved conceptualising of hybrid interference below the threshold of armed conflict. *European Security,* 33(2), 169-195. DOI: 10.1080/09662839.2023.2267478

[4] Billing, F., & Feldtmann, B. (2024). The role of criminal law approaches against hybrid attacks. *Bergen Journal of Criminal Law & Criminal Justice,* 12(2), 1-30. DOI: 10.15845/bjclcj.v12i2.4440

[5] Bundz, R., & Yarovyk, D. (2024). Treason and sabotage: Criminal liability under martial law. *Bulletin of Lviv Polytechnic National University. Series "Legal Sciences",* 11(2/42), 12-18. DOI: 10.23939/law2024.42.012

[6] Burczaniuk, P. (2024). Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku. *Przegląd Bezpieczeństwa Wewnętrznego,* 16(30), 49-78. DOI: 10.4467/20801335PBW.24.002.19604

[7] Castrogiovanni, A. (2026). Hybrid coercion and maritime deterrence in the Baltic Sea: Critical undersea infrastructure and narrative contestation. *Security and Defence Quarterly,* 54(2), 73-90. DOI: 10.35467/sdq/221580

[8] Cherevko, K.O., & Pashniev, D.V. (2024). Cyberattacks on critical infrastructure facilities in wartime: Key concepts. *Bulletin of Criminological Association of Ukraine,* 31(1), 209-219. DOI: 10.32631/vca.2024.1.15

[9] Chlebowicz, P. (2026). Udział w zorganizowanej grupie przestępczej mającej na celu działalność dywersyjną i sabotażową. Glosa krytyczna do wyroku Sądu Okręgowego we Wrocławiu z 21 lutego 2025 r., sygn. akt III K 339/24, Lex nr 3843269. *Studia Prawnoustrojowe,* 71, 534-543. DOI: 10.31648/sp.12377

[10] Haataja, S. (2023). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. *International Journal of Law and Information Technology,* 30(4), 423-443. DOI: 10.1093/ijlit/eaad006

[11] Herasymenko, O.M. (2024). Critical infrastructure of Ukraine as a subject of scientific knowledge: Theoretical aspect. *Uzhhorod National University Herald. Series "Law",* 85(4), 42-49. DOI: 10.24144/2307-3322.2024.85.4.6

[12] Holt, T.J., Griffith, M., Turner, N., Greene-Colozzi, E., Chermak, S., & Freilich, J.D. (2023). Assessing nation-state-sponsored cyberattacks using aspects of situational crime prevention. *Criminology & Public Policy,* 22(4), 825-848. DOI: 10.1111/1745-9133.12646

[13] Jones, S.G. (2025). Russia's sabotage campaign in Europe. *Survival,* 67(6), 129-148. DOI: 10.1080/00396338.2025.2588963

[14] Larsson, O.L. (2024). Sea blindness in grey zone preparations. *Defence Studies,* 24(3), 399-420. DOI: 10.1080/14702436.2024.2359913

[15] Neal, A.W. (2026). After Nord Stream: Four security dilemmas in critical maritime infrastructure protection. *International Affairs,* 102(1), 207-225. DOI: 10.1093/ia/iiaf229

[16] Pavlykivskyi, V.I., & Selevko, V.B. (2024). Objects of important national economic or defence significance as a mandatory element of sabotage: Problems of improving current legislation. *Bulletin of the Penitentiary Association of Ukraine,* 1, 77-84. DOI: 10.34015/2523-4552.2024.1.09

[17] Pestana, G., & Sofou, S. (2024). Data governance to counter hybrid threats against critical infrastructures. *Smart Cities,* 7(4), 1857-1877. DOI: 10.3390/smartcities7040072

[18] Piekarski, M. (2025). Critical infrastructure as a target of hybrid and conventional attacks. Lessons from the Ukrainian experience. *Terroryzm – studia, analizy, prewencja*, Special Issue, 113-132. DOI: 10.4467/27204383TER.25.016.21519

[19] Pochka, O.O. (2025). Countering sabotage in Ukraine by criminal law means: Problems of legislation and law enforcement. *Bulletin of Criminological Association of Ukraine,* 36(3), 92-105. DOI: 10.32631/vca.2025.3.07

[20] Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024). Russian sabotage in the gig-economy era. *The RUSI Journal,* 169(5), 10-21. DOI: 10.1080/03071847.2024.2401232

[21] Ringbom, H. (2025). New threats–old rules: Law of the sea issues raised by suspected attacks on submarine infrastructure in the Baltic Sea. *Ocean Development & International Law,* 56(3), 390-414. DOI: 10.1080/00908320.2025.2534621

[22] Rosicki, L., & Rosicki, R. (2025). Penal policy as exemplified by the criminalisation of the offences of espionage-related subversion and sabotage in Poland. *Środkowoeuropejskie Studia Polityczne,* 2, 99-127. DOI: 10.14746/ssp.2025.2.6

[23] Rovner, J., Cormac, R., & Maschmeyer, L. (2025). Sand in the gears: Sabotage in world politics. *European Journal of International Security*, 1-20. DOI: 10.1017/eis.2025.10025
[24] Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications,* 10. DOI: 10.1057/s41599-023-01864-y
[25] Ward, R. (2024). State threat activity: Principal offences. R. Ward, D. Blundell, C. Stone, & K. Laird (Eds.). *National Security Law, Procedure and Practice* (2nd ed.), (pp. 650-684). Oxford: Oxford University Press. DOI: 10.1093/oso/9780198895282.003.0019

Список використаних джерел

[1] Alexopoulos M. J., Niemi A., Skobiej B., Sill Torres F. Examination of the Critical Infrastructure Resilience Directive From the Maritime Point of View. *JCMS: Journal of Common Market Studies*. 2025. Vol. 63. No. 2. P. 667–678. DOI: 10.1111/jcms.13681
[2] Becker M. Transposing EU-legislation on critical infrastructure protection: legal implementation performance in the Baltic Sea region. *International Journal of Critical Infrastructure Protection*. 2025. Vol. 50. DOI: 10.1016/j.ijcip.2025.100781
[3] Bergaust J. C., Sellevåg S. R. Improved conceptualising of hybrid interference below the threshold of armed conflict. *European Security*. 2024. Vol. 33. No. 2. P. 169–195. DOI: 10.1080/09662839.2023.2267478
[4] Billing F., Feldtmann B. The Role of Criminal Law Approaches Against Hybrid Attacks. *Bergen Journal of Criminal Law & Criminal Justice*. 2024. Vol. 12. No. 2. P. 1–30. DOI: 10.15845/bjclcj.v12i2.4440
[5] Бундз Р., Яровик Д. Державна зрада і диверсія: кримінальна відповідальність в умовах воєнного стану. *Вісник Національного університету «Львівська політехніка». Серія «Юридичні науки»*. 2024. Т. 11. № 2 (42). С. 12–18. DOI: 10.23939/law2024.42.012
[6] Burczaniuk P. Przestępstwo szpiegostwa po nowemu, czyli w świetle nowelizacji Kodeksu karnego z 17 sierpnia 2023 roku. *Przegląd Bezpieczeństwa Wewnętrznego*. 2024. Vol. 16. No. 30. P. 49–78. DOI: 10.4467/20801335PBW.24.002.19604
[7] Castrogiovanni A. Hybrid coercion and maritime deterrence in the Baltic Sea: Critical undersea infrastructure and narrative contestation. *Security and Defence Quarterly*. 2026. Vol. 54. No. 2. P. 73–90. DOI: 10.35467/sdq/221580
[8] Черевко К. О., Пашнєв Д. В. Кібератаки на об'єкти критичної інфраструктури в умовах ведення війни: ключові поняття. *Вісник Кримінологічної асоціації України*. 2024. Т. 31. № 1. С. 209–219. DOI: 10.32631/vca.2024.1.15
[9] Chlebowicz P. Udział w zorganizowanej grupie przestępczej mającej na celu działalność dywersyjną i sabotażową. Glosa krytyczna do wyroku Sądu Okręgowego we Wrocławiu z 21 lutego 2025 r., sygn. akt III K 339/24, Lex nr 3843269. *Studia Prawnoustrojowe*. 2026. Nr 71. S. 534–543. DOI: 10.31648/sp.12377
[10] Haataja S. Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. *International Journal of Law and Information Technology*. 2023. Vol. 30. No. 4. P. 423–443. DOI: 10.1093/ijlit/eaad006
[11] Герасименко О. М. Критична інфраструктура України як предмет наукового пізнання: теоретичний аспект. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2024. Вип. 85. Ч. 4. С. 42–49. DOI: 10.24144/2307-3322.2024.85.4.6
[12] Holt T. J., Griffith M., Turner N., Greene-Colozzi E., Chermak S., Freilich J. D. Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*. 2023. Vol. 22. No. 4. P. 825–848. DOI: 10.1111/1745-9133.12646
[13] Jones S. G. Russia's Sabotage Campaign in Europe. *Survival*. 2025. Vol. 67. No. 6. P. 129–148. DOI: 10.1080/00396338.2025.2588963
[14] Larsson O. L. Sea blindness in grey zone preparations. *Defence Studies*. 2024. Vol. 24. No. 3. P. 399–420. DOI: 10.1080/14702436.2024.2359913
[15] Neal A. W. After Nord Stream: Four security dilemmas in critical maritime infrastructure protection. *International Affairs*. 2026. Vol. 102. No. 1. P. 207–225. DOI: 10.1093/ia/iiaf229
[16] Павликівський В. І., Селевко В. Б. Об'єкти, які мають важливе народногосподарське чи оборонне значення як обов'язкова ознака складу диверсії (проблеми вдосконалення чинного законодавства). *Вісник Пенітенціарної асоціації України*. 2024. № 1. С. 77–84. DOI: 10.34015/2523-4552.2024.1.09
[17] Pestana G., Sofou S. Data Governance to Counter Hybrid Threats against Critical Infrastructures. *Smart Cities*. 2024. Vol. 7. No. 4. P. 1857–1877. DOI: 10.3390/smartcities7040072
[18] Piekarski M. Critical infrastructure as a target of hybrid and conventional attacks. Lessons from the Ukrainian experience. *Terroryzm – studia, analizy, prewencja*. 2025. Special Issue. P. 113–132. DOI: 10.4467/27204383TER.25.016.21519

[19] Почка О. О. Протидія диверсіям в Україні кримінально-правовими засобами: проблеми законодавства та правозастосування. *Вісник Кримінологічної асоціації України*. 2025. № 3 (36). С. 92–105. DOI: 10.32631/vca.2025.3.07
[20] Richterova D., Grossfeld E., Long M., Bury P. Russian Sabotage in the Gig-Economy Era. *The RUSI Journal*. 2024. Vol. 169. No. 5. P. 10–21. DOI: 10.1080/03071847.2024.2401232
[21] Ringbom H. New Threats–Old Rules: Law of the Sea Issues Raised by Suspected Attacks on Submarine Infrastructure in the Baltic Sea. *Ocean Development & International Law*. 2025. Vol. 56. No. 3. P. 390–414. DOI: 10.1080/00908320.2025.2534621
[22] Rosicki L., Rosicki R. Penal Policy as Exemplified by the Criminalisation of the Offences of Espionage-Related Subversion and Sabotage in Poland. *Środkowoeuropejskie Studia Polityczne*. 2025. No. 2. P. 99–127. DOI: 10.14746/ssp.2025.2.6
[23] Rovner J., Cormac R., Maschmeyer L. Sand in the gears: Sabotage in world politics. *European Journal of International Security*. 2025. P. 1–20. DOI: 10.1017/eis.2025.10025
[24] Sanz-Caballero S. The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanities and Social Sciences Communications*. 2023. Vol. 10. DOI: 10.1057/s41599-023-01864-y
[25] Ward R. State Threat Activity: Principal Offences. *National Security Law, Procedure and Practice* / ed. by R. Ward, D. Blundell, C. Stone, K. Laird. 2nd ed. Oxford : Oxford University Press, 2024. P. 650–684. DOI: 10.1093/oso/9780198895282.003.0019

ZAHYNEI-ZABOLOTENKO Zoia
Doctor of Law, Professor, Head of the Department of Criminal Justice and Criminology of the V.M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine
01601, 4 Triokhsviatytelska St., Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-8679-124X;
VYCHIKOV Volodymyr
Postgraduate Student of the V.M. Koretsky Institute of State and Law of the National Academy of Sciences of Ukraine
01601, 4 Triokhsviatytelska St., Kyiv, Ukraine
ORCID: https://orcid.org/0009-0004-7885-1195

From Diversion to Sabotage: Criminalisation Models in Ukraine and Foreign Legal Systems

Abstract. The article presents a comparative legal study of contemporary approaches to the criminalization of acts of diversion and sabotage and identifies possible directions for improving the criminal-law protection of Ukraine's national security. The relevance of the study stems from the changing nature of such offences: alongside the physical destruction of or damage to strategically significant objects, increasing importance is being attached to interference with the functioning of energy, transport, information and communication, and other systems; the creation of technical and software vulnerabilities; and conduct aimed at disrupting the continuity of critical societal and state functions. The purpose of the article is to identify patterns in the legislative construction of such criminal-law prohibitions in foreign jurisdictions and to determine the place of the Ukrainian model of diversion within contemporary comparative legal approaches. The study is based on the criminal legislation of the United Kingdom, Canada, Australia, France, the Federal Republic of Germany, Poland, Sweden, Finland, Norway, the Czech Republic, Latvia, Estonia, and Ukraine. The research employs formal legal, comparative legal, systemic, and functional methods, as well as the method of typological analysis. It is argued that foreign counterparts of diversion cannot be identified solely on the basis of the terminological similarity of the names of the relevant criminal offences. A distinction is proposed between nominative, structural, and functional equivalence of criminal-law prohibitions, with functional equivalence being regarded as the primary criterion for their comparison. It is established that national models are formed through different combinations of purpose-based, foreign-agent, interest-centred, and functional-infrastructure mechanisms of criminalisation, while their legislative architecture may be autonomous, differentiated and comprehensive, or decentralized. A shift in the functional paradigm of criminal-law protection has been identified, involving a move away from the physical integrity of a strategically significant object towards ensuring its operational capability, accessibility, reliability, effectiveness, and continuity in performing critical societal or state functions. At the same time, a tendency towards deeper preventive criminalisation has been established. In certain jurisdictions, it encompasses not only preparation and attempt, but also the creation of means for sabotage, reconnaissance of potential targets, agent-related

preparatory activities, the creation of technical and software vulnerabilities, and the planning of future offences. To characterize this phenomenon, the concept of the “preventive depth of criminalization” is proposed. The Ukrainian legal construction of diversion is characterized as an autonomous purpose-based model of a casuistic object-oriented type. It is argued that a promising direction for its modernization lies neither in terminologically replacing diversion with sabotage nor in mechanically expanding the list of protected objects, but rather in functionalizing the objective elements of the offence by recognizing the disabling, substantial interruption, disruption, or disorganization of systems, facilities, and networks on which the security, defense capability, and resilience of the state depend as independently relevant forms of criminal conduct. The practical significance of the findings lies in their potential use for the further improvement of Article 113 of the Criminal Code of Ukraine and for developing approaches to the criminal-law assessment of contemporary forms of diversion and sabotage activities.

Keywords: acts of diversion and sabotage; national security; critical infrastructure; criminal liability; foreign criminal legislation; functional approach.