УДК 343.3; 343.9
DOI: https://doi.org/10.31359/1993-0909-2025-32-4-291

Михайло Валерійович Шепітько

Національна академія правових наук України
Харків, Україна

Науково-дослідний інститут вивчення проблем злочинності імені академіка В. В. Сташиса
Національної академії правових наук України
Харків, Україна

Богдан Володимирович Щур

Національна академія правових наук України
Харків, Україна

Кафедра кримінального права та процесу
Львівський торговельно-економічний університет
Київ, Україна

КРИМІНАЛЬНО-ПРАВОВА ПОЛІТИКА ТА КРИМІНАЛІСТИЧНА СТРАТЕГІЯ В ПРОТИДІЇ КІБЕРДИВЕРСІЯМ ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Анотація. *Стаття присвячена кримінально-правовому та криміналістичному дослідженню кібердиверсій, що стали активно вчинятися агресором під час російсько-української війни в Україні. Кібервійна як форма її активної фази стала серйозно впливати на критичну інфраструктуру України, впливаючи на самі основи національної безпеки через руйнацію обороноздатності, економіки, інвестиційного клімату та життєдіяльності в цілому. Важливою частиною дослідження стало наведення прикладів здійснених кібератак, які вплинули на приватні, корпоративні та державницькі процеси в Україні (кібератаки на банківську систему України, енергетичний сектор економіки, на підприємства «Київстар», Укрзалізницю» та ін.). У цьому контексті автори здійснили аналіз кримінально-правової політики та криміналістичної стратегії в протидії кібердиверсіям під час російсько-української війни. З цією метою було проаналізовано цілу низку нормативно-правових актів у законодавстві України: 1) Закон України «Про критичну інфраструктуру»; 2) Стратегія кібербезпеки України; 3) план заходів на 2025 рік з реалізації Стратегії кібербезпеки України. Також у законодавстві інших держав було виявлено Кримінальні (Карні) кодекси Німеччини, Франції та Киргизької Республіки, які вже увібрали в себе та визначили кібердиверсію (кіберсаботаж або комп'ютерний саботаж) як окремий злочин. У результаті цього дослідження автори здійснили спробу формулювання пропозиції визначення кібердиверсії в Україні як окремого злочину проти основ національної безпеки. Відповідно до реалізації стратегії кібербезпеки України в межах виконання плану на 2025 р. було виявлено окремі заходи, які можуть бути*

віднесені до реалізації криміналістичної стратегії в протидії кіберзлочинам, включаючи кібердиверсію. Також було встановлено, що криміналістична стратегія у протидії кібердиверсіям може бути досягнута шляхом: 1) взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (кіберзахисту); 2) здійснення спільних із державами-членами ЄС і НАТО заходів у протидії кіберзагрозам; 3) проведення міжвідомчих тренінгів та навчань у протидії кібератакам; 4) створення та застосування на практиці стандартів розслідуваня кібердиверсій; 5) підвищення взаємодії між правоохоронними органами та органами кібероборони (кіберзахисту) в розслідуванні кібердиверсій; 6) підвищення спроможностей та взаємодії між правоохоронними та судово-експертними органами.

Ключові слова: *кібердиверсія; кримінальні правопорушення проти основ національної безпеки; кримінально-правова політика; криміналістична стратегія; протидія злочинності; кіберзахист.*

Mykhaylo V. Shepitko

National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine

Academician Stashis Scientific Research Institute for the Study of Crime Problems
National Academy of Law Sciences of Ukraine
Kharkiv, Ukraine

Bogdan V. Schur

National Academy of Legal Sciences of Ukraine
Kharkiv, Ukraine

Criminal Law and Procedure Department
Lviv University of Trade and Economics
Lviv, Ukraine

CRIMINAL LAW POLICY AND CRIMINALISTIC STRATEGY IN COUNTERACTION TO CYBER SABOTAGE DURING RUSSIAN-UKRAINIAN WAR

Abstract. *The article is devoted to the criminal-legal and forensic investigation of cyber sabotage, which began to be actively committed by the aggressor during the Russian-Ukrainian war in Ukraine. Cyberwarfare as a form of the active phase of the war began to seriously affect the critical infrastructure of Ukraine, affecting the very foundations of national security through the destruction of defense capabilities, economy, and investment climate. An important part of the study was to provide examples of cyberattacks that affected private, corporate, and state processes in Ukraine (cyberattacks on the banking system of Ukraine, the energy sector of the economy, «Kyivstar», «Ukrzaliznytsia», etc.). In this context, the authors analyzed the criminal law policy and forensic strategy in countering cyber sabotage during the Russian-Ukrainian*

war. For this purpose, a number of regulatory legal acts in the legislation of Ukraine were analyzed: 1) The Law of Ukraine «On Critical Infrastructure»; 2) the Cybersecurity Strategy of Ukraine; 3) the Action Plan for 2025 for the Implementation of the Cybersecurity Strategy of Ukraine. Also, in the legislation of other states, the Criminal (Penal) Codes of Germany, France, and the Kyrgyz Republic were identified, which have already incorporated and defined cyber sabotage (cyber sabotage or computer sabotage) as a separate crime. As a result of this study, the authors attempted to formulate a proposal to define cyber sabotage in Ukraine as a separate crime against the foundations of national security. In accordance with the implementation of the Cybersecurity Strategy of Ukraine within the framework of the implementation of the 2025 plan, certain measures were identified that can be attributed to the implementation of the forensic strategy in countering cybercrimes, including cyber sabotage. It was also established that the forensic strategy in countering cyber sabotage can be achieved through: 1) interaction of the main subjects of the national cybersecurity system and the defense forces in terms of joint implementation of cyber defense tasks (cyber defense); 2) implementation of joint measures with EU and NATO member states in countering cyber threats; 3) conducting interagency trainings and exercises in countering cyber-attacks; 4) creation and practical application of standards for investigating cyber sabotage; 5) increasing interaction between law enforcement agencies and cyber defense agencies (cyber defense) in investigating cyber sabotage; 6) increasing the capabilities and interaction between law enforcement and forensic agencies.

Ключові слова: *cyber sabotage; criminal offenses against basis of national security; criminal law policy; criminalistic strategy; crime counteraction; cyber defense.*

ВСТУП

Російська-українська війна проходить різні стадії та форми, що пов'язують із інформаційним, психологічним, економічним і збройним впливом. Такі прояви російсько-української війни в своїй єдності часто відносять до гібридної війни, яка в цілому спрямована на знищення України, а окремо на досягнення проміжних цілей – зменшення економічного потенціалу, погіршення інвестиційного клімату, унеможливлення поставок зброї, зменшення людського ресурсу, створення обстановки остраху в Україні та поза її межами.

Однією із форм російсько-української війни, яка здійснює серйозний руйнівний ефект від її застосування, є кібервійна. Вона реалізовується через кібератаки на різні сфери – від індивідуальних (персональних) до корпоративних, державних і міжнародних. Такі посягання можуть також мати різні цілі – від психологічного впливу та психічного насильства до цілком фізичних наслідків, що пов'язуються із зупиненням, руйнацією або знищенням транспортного сполучення, зв'язку, платіжних систем чи енергетики. Такі об'єкти прийнято йменувати об'єктами критичної інфраструктури, які є «важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам» [1].

Дослідження кіберзагроз із урахуванням уже здійснених кібератак проти України дозволяє вказати на те, що в цілому такі діяння становлять окрему форму

війни проти України. Це передбачає застосування комплексу заходів, що дозволити мінімізувати, нейтралізувати наслідки від їх вчинення, а також убезпечити від майбутніх кібератак. Окрему небезпеку для Україну становить достатньо нове діяння, яке посягає на основи національної безпеки, – це кібердиверсія. На нашу думку, протидія цьому явищу має передбачати формування й оновлення кримінально-правової політики та криміналістичної стратегії.

1. ОГЛЯД ЛІТЕРАТУРИ

До проблеми визначення та протидії кібердиверсії як окремого явища зверталися в своїх спеціальних дослідженнях Д. Агінг [2], Д. С. Мельник [3], О. Р. Пелещак [4], А. Д. Пратіві [2] та О. В. Шамсутдінов [3]. Цікаво, що вони визначили це явище як саботаж або кіберсаботаж (кібердиверсію) та запропонували кримінально-правові засоби протидії. Це корелюється із тенденцією встановлення кримінальної відповідальності за такі та подібні явища (комп'ютерний саботаж) у КК Німеччини [5], Франції [6] та Киргизької Республіки [7].

У своїй єдності аналіз зазначених джерел у поєднанні з комплексом нормативно-правових актів, які формують та реалізують кримінальну політику в Україні, дають змогу запропонувати нові підходи в протидії кібердиверсіям на кримінально-правовому та криміналістичному рівні.

2. МАТЕРІАЛИ ТА МЕТОДИ

Об'єктом аналізу цього дослідження є кримінально-правова політика та криміналістична стратегія в протидії кібердиверсіям під час російсько-української війни.

Авторами було використано комплекс методів – діалектичний (під час дослідження розвитку законодавства та наукових досліджень, спрямованого в протидії кіберзагрозам і кібердиверсіям), логічний (під час викладу матеріалу та співвідношення суміжних кримінально-правових і криміналістичних понять у сфері протидії кримінальним правопорушенням проти основ національної безпеки), порівняльно-правовий (при порівнянні кримінальних та карних законодавств України, Німеччини, Франції та Киргизької Республіки) та формально-юридичний (під час виявлення специфіки такого явища як кібердиверсія з виявленням необхідних ознак і заходів протидії кримінально-правовими та криміналістичними засобами).

3. РЕЗУЛЬТАТИ ТА ОБГОВОРЕННЯ

Кримінальна політика України в протидії кіберзлочинам реалізується через Стратегію кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 №447/2021. У ній визначено, що загрозами кібербезпеці України є: 1) гібридна агресія Російської Федерації проти України в кіберпросторі; 2) кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат; 3) організовані та спонсоровані

урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності; 4) використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової й іншої підтримки терористичної діяльності.

Кабінет Міністрів України своїм розпорядженням від 07.03.2025 № 204-р затвердив плани заходів на 2025 рік, включивши до нього окремі заходи, що можна віднести до форми реалізації криміналістичної стратегії в протидії кіберзлочинам, включаючи кібердиверсії, зокрема: 1) запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони; 2) запровадження практики проведення загальнонаціональної інформаційної роз'яснювальної кампанії щодо дій громадян у разі, коли вони стикаються із кібершахрайством та іншими кіберзлочинами, а також роз'яснення процедур щодо звернення до правоохоронних органів; 3) здійснення спільних із державами – членами ЄС і НАТО заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність і реагувати на кіберзагрози; 4) застосовування всіх доступних інструментів дипломатії та міжнародного права для протидії зловмисній діяльності проти України в кіберпросторі [8].

Органами, які здійснюють задіяні в розслідуванні кібератак в Україні є кіберполіція та департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України. При цьому вони вимушені діяти у взаємодії з іншими державними органами – Державною службою спеціального зв'язку та захисту інформації України та іншими органами та підприємствами, які регулюють діяльність критичної інфраструктури та які здійснюють власні заходи з кіберзахисту (Міністерство розвитку громад та територій України, АТ «Укрзалізниця», ПрАТ «Київстар», тощо).

Під час реалізації криміналістичної стратегії в розслідуванні кіберінцидентів слід звернути увагу, що такі події зазвичай мають масований характер, що дозволяє застосовувати стратегічне планування й організацію заходів розслідування щодо таких суспільно небезпечних діянь. У межах діяльності Державної служби спеціального зв'язку та захисту інформації України діє CERT-UA як урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України [9]. Так, до завдань CERT-UA можна віднести окремі, які можуть мати криміналістичний зміст: 1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів; 2) надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення й усунення наслідків кіберінцидентів щодо цих об'єктів; 3) організація та проведення практичних семінарів із питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; 4) підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак

і кіберзагроз; 5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки; 6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі в Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків; 7) взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами й організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору; 8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту; 9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Слід звернути увагу, що Адміністрація Державної служби спеціального зв'язку та захисту інформації України прийняла Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі від 03.07.2023 № 570. Зокрема, у цих методичних рекомендаціях сформовано типовий перелік заходів із реагування на кіберінциденти/кібератаки для одночасного відстеження заходів до їх завершення (дод. 4). При чому *окремі заходи є повторюваними й можуть виконуватися та змінюватися безперервно*, доки підозріла поведінка не буде усунена, наслідки кіберінциденту/кібератаки не будуть ліквідовані, *електронні докази, необхідні для проведення розслідування та аналізу процесу реагування на кіберінциденти/кібератаки, не будуть зібрані* (п. 9 розд. І).

Не дивлячись на зростаючу потребу в протидії таким кіберзагрозам, кримінально-правове законодавства України не можна назвати досконалим в цій частині [10, с. 115–122; 11, с. 88–92]. До таких суспільно небезпечних діянь прийнято відносити ті, які охоплюються розділом XVI Особливої частини КК України «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (статті 361–363-1).

До найбільш відомих і масованих російських кібератак, які були здійснені проти України в період російсько-української війни, зазвичай відносять ті, які здійснили посягання на критичну інфраструктуру, зокрема: 1) кібератака на енергетичні компанії, що дозволили вивести енергосистеми з ладу на певний час (23.12.2015) [12]; 2) кібератака NotPetya, яка порушила роботу державних і приватних установ, фінансового й енергетичного секторів економіки, включаючи аеропорти, метрополітен, поліцію, банків, мобільних операторів, медичних компаній, тощо (27.06.2017) [13]; 3) DDoS-атака на державні сайти банків, сайтів уряду та Міністерства оборони України, що призвело до створення обстановки паніки напередодні початку широкомасштабного вторгнення (15.02.2022) [14]; 4) кібератака на «Київстар», що призвела до знищення майже половини інфраструк-

тури мобільного оператора та відсутності стільникового зв'язку в 24 млн населення України (12.12.2023) [15]; 5) кібератака на державні реєстри та сайт Міністерства юстиції України, що призвело до порушення архітектури 25 реєстрів? їх внутрішні зв'язки, через що було унеможливлено на значний час доступ до банківських послуг, реєстрацію нерухомого майна, народження, шлюбу, смерті, зміни прізвища, реєстрацію юридичних осіб, тощо (19.12.2024) [16]; 6) таргетована кібератака на Укрзалізницю, що призвела до збоїв у роботі онлайн сервісів, включаючи продаж квитків та надання послуг вантажовідправникам (23.03.2025) [17].

У цілому названі кібератаки не досягли цілей повного знищення критичної інфраструктури, однак суттєво вплинули на життєдіяльність. Очевидно, що російські кібератаки ставили своєю метою не тільки ускладнення корпоративних і державних процесів в Україні, але й ослабити Україну в цілому, чим полегшити її захоплення, а також зруйнувати або пошкодити об'єкти, які мають важливе народногосподарське чи оборонне значення (об'єкти критичної інфраструктури).

Це наближає визначення цих кібератак у контексті диверсії, сформульованої в ст. 113 КК України. Такий висновок випливає з того, що першочерговим об'єктом посягання стають на комп'ютерні мережі або системи зв'язку, а самі основи національної безпеки України, що відсилає правозастосувача до розділу I Особливої частини КК України в пошуку відповідного кримінального правопорушення для захисту держави як такої.

Зрозуміло, що законодавець при визначенні диверсії (починаючи з 2001 р.) не передбачав можливість кібервпливу на подібні об'єкти та не міг знати про можливий ефект на об'єкти критичної інфраструктури, що можуть дорівнювати фізичному впливу на них шляхом вибухів, підпалів або інших дій. Це дозволяє виокремити з-поміж інших діянь, які посягають на кіберсферу – кібердиверсію *(«cyber sabotage»)* як особливий вид диверсії та специфічний «комп'ютерний» або кіберзлочин.

При визначенні кібердиверсії О. Р. Пелещак наполягає, що «у випадку вчинення кібердиверсії з метою знищення інформації або цілеспрямованого атакування певних вузлів управління зазначений механізм характеризується використанням однієї комп'ютерної інформації (знаряддя – вірус) для здійснення впливу на іншу комп'ютерну інформацію (предмет – критична інформаційна структура)». Також він уточнює, що цей злочин відноситься до «геополітичних» та може призвести до людських жертв [4, с. 31, 32]. Кібердиверсія також досліджується окремими дослідниками, які визначають її як «серія заходів для знищення, пошкодження або порушення роботи мережевих систем та комп'ютерних програм, підключених до Інтернету» [2, с. 54, 55].

О. В. Шамсутдінов і Д. С. Мельник під час аналізу диверсії дійшли до висновку щодо необхідності створення окремої норми «Саботаж» (ст. 113–1 КК України) на підставі порівняльного дослідження кримінальних законодавств різних держав. На нашу думку, з цією позицію можна погодитися тільки частково. По-перше, кримінально-правове використання терміну «саботаж» в Україні заанга-

жоване тоталітарним минулим, коли в КК УРСР 1927 р. це «контрреволюційний саботаж» визначався як свідоме невиконання певних обов'язків або навмисне недбале їх виконання із спеціальною метою послабити владу уряду й діяльність державного апарату [18]. По-друге, «саботаж» на сьогодні є певним іноземним відповідником такого злочину як диверсія, що в перекладі на англійську або французьку мови має саме таку назву. По-третє, за своїм змістом включає посягання на «системи автоматизованої обробки інформації або внесення неполадок в їх роботу, якщо це діяння здатне завдати шкоди основоположним інтересам нації» («саботаж»/«sabotage» [6], ст. 411–9 КК Франції) [3, с. 180, 182]. По-четверте, наявність синонімічних конструкцій у КК України здатне захарастити кримінальне законодавство.

За ст. 303b Карного кодексу Німеччини встановлюється кримінальна відповідальність за «комп'ютерний саботаж» / «комп'ютерну диверсію» *(«computer sabotage»)*, що включає в себе «втручання в операції з обробки даних, які мають істотне значення для іншого у вигляді вчинення злочину» відповідно до ст. 303a (1) («Маніпуляція даними»), «введення або передачі даних (ст. 202a (2)) з наміром негативно вплинути на іншого, або знищення, пошкодження, видалення або зміна системи обробки даних або носія даних». За умови, що ставиться під загрозу постачання населенню життєво важливих товарів або послуг, або відбувається посягання на безпеку Німеччини, то такі справи відносяться до серйозних (п. 3 ч. 4 ст. 303b) [5].

Також серед злочинів проти кібербезпеки (розд. 40) у КК Киргизької Республіки передбачено «кіберсаботаж» як окреме діяння – «навмисна зміна, знищення, блокування, надання непридатної для використання інформації, що зберігається на електронному носії, що міститься в інформаційній системі або передається через телекомунікаційні мережі або програми без права перешкоджати роботі комп'ютерних систем, з наміром перешкодити функціонуванню програмних продуктів або телекомунікаційних систем, а також відключення програмних продуктів, обладнання» (ст. 321) [7].

ВИСНОВКИ

Таким чином, видається можливим виокремлення спеціального виду диверсії в окремий склад «кібердиверсію» як поліоб'єктного злочину, що посягає на самі основи національної безпеки, кіберсферу та є таким, що є більш небезпечним через використання інформаційних та кіберспособів. Також слід мати на увазі, що сам факт використання інформаційних мереж, месенджерів, електронних (цифрових) засобів і способів автоматично не робить таке діяння кібердиверсією. Аналіз окремих вироків за ст. 113 КК України демонструють використання таких засобів для втягнення громадян України для здійснення підпалів та вибухів на об'єктах критичної інфраструктури [19].

На нашу думку, тільки використання спеціальних способів, спрямованих на знищення, пошкодження, видалення, блокування або зміну носія даних чи їх

систем, що посягають, таким чином, на об'єкти критичної інфраструктури та самі основи національної безпеки, можуть бути віднесені до кібердиверсії. При цьому визначення конкретного місця «Кібердиверсії» в Особливій частин КК України може залежати від особливостей її складу, необхідних (обов'язкових) ознак та цілей законодавця, які він прагне досягти від появи такого злочину в КК України. Вже на сьогодні ефект від вчинення таких кібердиверсій під час російсько-української війни є відчутним для населення України. Заповнення даної прогалини в кримінальному законодавстві дозволить індивідуалізувати та посилити покарання осіб, які їх здійснюють проти України. Також формування такого окремого злочину проти основ національної безпеки України дозволяє більше ефективно реалізовувати кримінально-правову політику в протидії кіберзагрозам та кіберзлочинності.

Також реалізація криміналістичної стратегії в протидії кібердиверсіям може бути досягнута наступним шляхом: 1) запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони (кіберзахисту); 2) здійснення спільних із державами-членами ЄС і НАТО заходів, спрямованих на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність і реагувати на кіберзагрози; 3) проведення міжвідомчих тренінгів та навчань у протидії кібератакам, що посягають на критичну інфраструктуру, включаючи на безпеки від вчинення кібердиверсій; 4) створення та застосування на практиці міжнародних і національних стандартів розслідування кібердиверсій; 5) підвищення взаємодії між правоохоронними органами та органами кібероборони (кіберзахисту) в розслідуванні кібердиверсій; 6) підвищення спроможностей та взаємодії між правоохоронними й судово-експертними органами під час розслідування кібердиверсій.

Результати дослідження можуть бути використані як основа для подальших досліджень щодо кримінально-правової та криміналістичної протидії кримінальним правопорушенням проти основ національної безпеки України в цілому, та кібердиверсіям зокрема.

Подальші дослідження можуть бути сконцентровані на формуванні кримінальної політики в сфері протидії кібердиверсіям в Україні та інших держав.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Про критичну інфраструктуру : Закон України від 16.11.2021 №1882-IX. *Верховна Ради України*. URL: https://zakon.rada.gov.ua/laws/show/1882–20#Text

[2] Aging D., Pratiwi A. D. Cyber-Sabotage from The Perspective of Information and Electronic Transactions Regulation. *Alauddin Law Development Journal.* 2024. Iss. 6(1). P. 52–61.

[3] Шамсутдінов О. В., Мельник Д. С. Кримінально-правова охорона критичної інфраструктури від підривних посягань. *Вісник Харківського національного університету внутрішніх справ.* 2020. № 3(98). С. 170–183.
[4] Пелещак О. Р. Деякі аспекти кримінально-правової характеристики кібердиверсії. *Соціально-правові студії.* 2020. Вип. 3(9). С. 26–33.
[5] German Criminal Code. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
[6] Penal Code of France. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/
[7] The Criminal Code of the Kyrgyz Republic. URL: https://www.refworld.org/legal/legislation/natlegbod/2021/ru/150130
[8] Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Каб. Міністрів України від 07.03.2025 № 204-р. *Верховна Ради України*. URL: https://zakon.rada.gov.ua/laws/show/204–2025-p#Text
[9] CERT-UA. URL: https://cert.gov.ua/about-us
[10] Кулешов М. В. Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України. *Інформація і право.* 2019. № 2 (29). С. 115–122.
[11] Дришлюк І. А. Невидима зброя з реальними наслідками: правова кваліфікація кібератак у контексті російсько-української війни. *Правовий вимір конституційної та кримінальної юрисдикції в Україні та світі. Восьмі юридичні читання*: збірник тез Всеукр. щорічн. наук.-практ. дист. конф. (м. Одеса, 18 квіт. 2024 р.). Одеса, 2024. С. 88–92.
[12] Чи була кібератака на обленерго? *DDC News Україна*. 06.01.2016. URL: https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc
[13] США також звинуватили у вірусі NotPetya Росію. *BBC News Україїна*. 16.02.2018. URL: https://www.bbc.com/ukrainian/news-43082212.amp
[14] Нова кібератака на банки була «найбільшою в історії України» й досі триває. *BBC News Україна*. 16.02.2022. URL: https://www.bbc.com/ukrainian/news-60401775.amp
[15] Коваль О. Якою була атака хакерів на «Київстар» та як відновлювалась компанія. *DOU*. 19.03.2024. URL: https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/
[16] Сєров І. Кібератака на державні реєстри України: які дані постраждали і що загрожує мільйонам громадян. *TCH*. 20.12.2024. URL: https://tsn.ua/amp/exclusive/kiberataka-na-derzhavni-reyestri-ukrayini-yaki-dani-postrazhdali-i-scho-zagrozhuye-milyonam-gromadyan-2728092.html
[17] Кібератака на Укрзалізницю: у Держспецзв'язку кажуть, що були використані тактики спецслужб РФ. *Укрінформ*. 01.04.2025. URL: https://www.ukrinform.ua/amp/rubric-society/3977123-kiberataka-na-ukrzaliznicu-u-derzspeczvazku-kazut-so-buli-vikoristani-taktiki-specsluzb-rf.html
[18] Кримінальний кодекс УРСР 1927 р. URL: https://coollib.net/b/669494-kollektiv-avtorov-yurisprudentsiya-kriminalniy-kodeks-ursr-1927-roku-v-redaktsiyi-1949-roku/readp?p=2&cnt=9000
[19] Вирок Інгульського районного суду м. Миколаєва від 25.09.2025 (справа № 489/4360/25, провадження № 1-кп/489/733/2).

REFERENCES

[1] On Critical Infrastructure: Law of Ukraine (2021, November). Retrieved from https://zakon.rada.gov.ua/laws/show/1882–20#Text

[2] Aging, D., & Pratiwi, A. D. (2024). Cyber-Sabotage from The Perspective of Information and Electronic Transactions Regulation. *Alauddin Law Development Journal*, 6(1), 52–61.
[3] Shamsutdinov, O. V., & Melnyk, D. S. (2020). Criminal-legal protection of critical infrastructure from subversive attacks. *Bulletin of the KhNUVS*, 3(98), 170–183.
[4] Peleshchak, O. R. (2020). Some aspects of the criminal-legal characteristics of cyber sabotage. *Socio-legal studies*, 3(9), 26–33.
[5] German Criminal Code. Retrieved from https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html
[6] Penal Code of France. Retrieved from https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/
[7] The Criminal Code of the Kyrgyz Republic. Retrieved from https://www.refworld.org/legal/legislation/natlegbod/2021/ru/150130
[8] On approval of the action plan for 2025 for the implementation of the Cybersecurity Strategy of Ukraine: Resolution of the Cabinet of Ministers of Ukraine (2025, March, No. 204-r). Retrieved from https://zakon.rada.gov.ua/laws/show/204–2025-p#Text
[9] CERT-UA. Retrieved from https://cert.gov.ua/about-us
[10] Kuleshov, M. V. (2019). The essence and content of the investigation of cyber incidents and cyber attacks by the subdivisions of the Security Service of Ukraine. *Information and Law*, 2(29),115–122.
[11] Dryshlyuk, I. A. (2024, April 18) Invisible weapons with real consequences: legal qualification of cyberattacks in the context of the Russian-Ukrainian war. *Legal dimension of constitutional and criminal jurisdiction in Ukraine and the world. Eighth legal readings: collection of theses of the All-Ukrainian annual scientific-practical dist. conference.* (pp. 88–92). Odessa.
[12] Was there a cyberattack on the regional energy company? (2016). *DDC News Ukraine*. Retrieved from https://www.bbc.com/ukrainian/society/2016/01/160106_cyber_attacks_electricity_ukraine_vc
[13] The US also blamed Russia for the NotPetya virus. (2018). *BBC News Ukraine*. Retrieved from https://www.bbc.com/ukrainian/news-43082212.amp
[14] New cyberattack on banks was 'largest in Ukrainian history' and still ongoing. (2022). *BBC News Ukraine.* Retrieved from https://www.bbc.com/ukrainian/news-60401775.amp
[15] Koval, O. (2024). What was the hacker attack on Kyivstar and how was the company restored. *DOU*. Retrieved from https://dou.ua/lenta/news/kyivstar-cyber-attack-restoration/
[16] Serov, I. (2024). Cyberattack on state registers of Ukraine: what data was affected and what threatens millions of citizens. *TSN*. Retrieved from https://tsn.ua/amp/exclusive/kiberataka-na-derzhavni-reyestri-ukrayini-yaki-dani-postrazhdali-i-scho-zagrozhuye-milyonam-gromadyan-2728092.html
[17] Cyberattack on Ukrzaliznytsia: the State Special Communications Service says that tactics of the Russian special services were used. (2025). *Ukrinform*. Retrieved from https://www.ukrinform.ua/amp/rubric-society/3977123-kiberataka-na-ukrzaliznicu-u-derzspeczvazku-kazut-so-buli-vikoristani-taktiki-specsluzb-rf.html
[18] Criminal Code of the Ukrainian SSR (1927). Retrieved from https://coollib.net/b/669494-kollektiv-avtorov-yurisprudentsiya-kriminalniy-kodeks-ursr-1927-roku-v-redaktsiyi-1949-roku/readp?p=2&cnt=9000
[19] Verdict of the Ingulsky District Court of Mykolaiv (2025, September, Case No. 489/4360/25, Proceedings No. 1-kp/489/733/2).

Михайло Валерійович Шепітько
Доктор юридичних наук, професор
Член-кореспондент НАПрН України
Національна академія правових наук України
61024, вул. Григорія Сковороди, 70, Харків, Україна

Провідний науковий співробітник
Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса
Національної академії правових наук України
61002, вул. Григорія Сковороди, 49, Харків, Україна

Mykhaylo V. Shepitko
Doctor of Law, Professor
Corresponding Member NALS of Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Hryhoriia Skovorody St., Kharkiv, Ukraine

Leading Researcher
Academician Stashis Scientific Research Institute for the Study of Crime Problems
National Academy of Legal Sciences of Ukraine
61002, 49 Hryhoriia Skovorody Str., Kharkiv, Ukraine

Email: shepitko.michael@gmail.com
ORCID: https://orcid.org/0000-0002-7164-8037

Богдан Володимирович Щур
Доктор юридичних наук, професор
Член-кореспондент НАПрН України
Національна академія правових наук України
61024, вул. Григорія Сковороди, 70, Харків, Україна

Завідувач кафедри кримінального права та процесу
Львівський торговельно-економічний університет
79011, вул. Уласа Самчука, 9, Львів, Україна

Bogdan V. Schur
Doctor of Law, Professor
Corresponding Member NALS of Ukraine
National Academy of Legal Sciences of Ukraine
61024, 70 Hryhoriia Skovorody St., Kharkiv, Ukraine

Head of Department Criminal Law and Procedure
Lviv University of Trade and Economics,
79011, 9 Ulasa Samchuka Str., Lviv, Ukraine

Email: bogdanshchur1965@ukr.net
ORCID: https://orcid.org/0000-0003-2139-2317

Рекомендоване цитування: Шепітько М. В., Щур Б. В. Кримінально-правова політика та криміналістична стратегія в протидії кібердиверсіям під час російсько-української війни. *Вісник Національної академії правових наук України*. 2025. Т. 32. №4. С. 291–303.

Suggested Citation: Shepitko, M. V., & Schur, B. V. (2025). Criminal Law Policy and Criminalistic Strategy in Counteraction to Cyber Sabotage during Russian-Ukrainian War. *Journal of the National Academy of Legal Sciences of Ukraine,* 32(4), 291–303.

Стаття надійшла / Submitted: 16/10/2025
Доопрацьовано / Revised: 16/11/2025
Схвалено до друку / Accepted: 18/12/2025