

ПрАТ «ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ»
Навчально-науковий інститут права та безпеки ім. Володимира Великого

ЗБІРНИК МАТЕРІАЛІВ

XI Міжнародної науково-практичної конференції

**«Розвиток української держави
в умовах активізації євроінтеграційних процесів»**

08 травня 2026 р.

м. Київ

Керімова Д.

*Здобувачка першого (бакалаврського) рівня вищої освіти
Навчально-наукового інституту права та безпеки
імені князя Володимира Великого ПрАТ “ВНЗ” МАУП”*

Науковий керівник:

Талах А.М.,

*кандидат юридичних наук,
доцент кафедри теорії держави і права та конституційного права,
Навчально-науковий інститут права та безпеки
Імені князя Володимира Великого ПрАТ “ВНЗ МАУП”*

Даркнет як середовище злочинності: проблеми правового регулювання

В сучасному цифровому віці, коли технології швидко розвиваються, а Інтернет стає невід’ємною частиною нашого повсякденного життя, питання забезпечення кібербезпеки та боротьби зі злочинністю в

он-лайн середовищі набувають надзвичайної актуальності. Організовані злочинні угруповання у своїй діяльності часто використовують мережу “Даркнет” (англ. DarkNet) [1].

Таємний сегмент Інтернету, відомий як Даркнет, став осередком різноманітних злочинних дій – від незаконної торгівлі наркотиками та зброєю до обміну конфіденційною інформацією й замовлення кримінальних послуг. Проблема набуває особливої ваги, адже Даркнет постає як зручна платформа для зловживань та порушень закону, тоді як наявні методи боротьби часто виявляються недостатньо ефективними в умовах кіберпростору. У цьому світлі важливо приділяти увагу не лише технічним засобам протидії злочинності в Даркнеті, але й створенню ефективних стратегій.

Метою дослідження є аналіз Даркнету як середовища вчинення кіберзлочинів, визначення основних проблем правового регулювання діяльності у тіньовому сегменті Інтернету, а також дослідження сучасних механізмів протидії кіберзлочинності в Україні та на міжнародному рівні.

Предметом дослідження є специфіка функціонування Даркнету як платформи для реалізації протиправної діяльності у кіберпросторі, а також дослідження правового інструментарію регулювання та запобігання злочинній активності у межах даного сегменту віртуального простору.

Об’єктом дослідження є суспільні відносини, що виникають у сфері забезпечення кібербезпеки та протидії кіберзлочинності у тіньовому сегменті мережі Інтернет.

Поставленим завданням було охарактеризувати поняття та особливості функціонування Даркнету; визначити основні види злочинної діяльності, що здійснюються у Даркнеті; дослідити способи забезпечення анонімності користувачів у тіньовому сегменті мережі; проаналізувати проблеми правового регулювання та протидії кіберзлочинності; охарактеризувати міжнародний досвід боротьби зі злочинністю у Даркнеті; визначити перспектививдосконалення системи кібербезпеки та діяльності правоохоронних органів України.

Законом України «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року, визначено, що кіберзлочин (комп’ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, а кіберзлочинність – сукупність кіберзлочинів [2].

Необхідно відзначити тенденцію до постійного зростання рівня організованості суб'єктів кіберзлочинності. Згідно з оцінками окремих дослідників, якщо приблизно сім років тому до 80% кіберзлочинців діяли індивідуально, то наразі аналогічний відсоток інтегрований у кримінальні угруповання, які переважно характеризуються транснаціональним виміром.

У своїй протиправній діяльності ці угруповання активно застосовують криптографічні засоби для забезпечення мережевої анонімності та здійснення електронних транзакцій. Це сприяло формуванню тіньових онлайн-ринків, де здійснюється збут та придбання нелегальних субстанцій, викрадених та контрафактних виробів, матеріалів із експлуатацією дітей, озброєння тощо. Цей сегмент електронного ринку в Інтернеті відомий як "Даркнет". Примітно, що сам термін виник ще до широкого поширення глобальної мережі та позначав високий рівень анонімності у комп'ютерних мережах, що досягався шляхом застосування нестандартних протоколів та портів.

Крім того, злочинні елементи широко використовують "Глибоку мережу" (Deep Web) – сукупність вебресурсів, які не індексуються традиційними пошуковими системами. Термін «Даркнет» стосується підмножини інтернет-сайтів і сторінок, які не індексуються пошуковими системами.

Даркнет часто асоціюється з доменом верхнього рівня ".onion", сайти якого називаються «Onion-сайтами» (від англ. onion – цибуля) і доступні через спеціальний браузер, наприклад Tor. [3]

Для доступу в темну мережу, особі, по суті, потрібно лише отримати доступ до правильних .onion-посилань або знати відповідні облікові дані. Однак додатково для доступу до даркнету потрібно встановити спеціальний клієнт, такий як Tor Browser, який приховує доступ і анонімізує користувача.[4]

У контексті використання для протиправної діяльності, темна мережа (Darknet) виявляє низку специфічних характеристик: забезпечення анонімності фінансових операцій, зокрема через використання криптовалют для маскування походження та призначення коштів; високий рівень шифрування комунікацій, що унеможливує доступ до змісту обміну інформацією; функціонування прихованих сервісів (Hidden Services), представлених веб-ресурсами зі специфічними доменами (.onion), які не індексуються традиційними пошуковими системами та недоступні через стандартні веб-браузери; розробка та застосування специфічної термінології, включно з жаргоном і кодовими словами, для ускладнення зовнішнього розуміння; наявність динамічних торго-

вих майданчиків, які регулярно змінюють свої мережеві ідентифікатори (адреси) для уникнення виявлення існування внутрішніх систем репутації та

довіри, призначених для оцінки доброчесності та надійності користувачів; використання складних логістичних схем для маскуванню фізичної передачі товарів та послуг; функціонування посередницьких послуг, включаючи ескроу-сервіси або "гарантів", для забезпечення безпеки транзакцій між сторонами; широке застосування засобів для запобігання відстеженню, таких як маскуванню IP-адрес та інших цифрових ідентифікаторів користувачів; обмежений доступ до окремих сегментів, що реалізується через закриті спільноти та форуми з жорсткими вимогами до членства.

З огляду на вищевикладене, темна мережа (Darknet) у криміногенному контексті може бути визначена як спеціалізована цифрова інфраструктура в глобальній мережі Інтернет, що слугує інструментом для реалізації протиправних діянь. Її функціонал передбачає забезпечення підвищеного рівня анонімності суб'єктів, криптографічного захисту обміну інформацією та фінансових операцій, а також надання доступу до нелегальних віртуальних торговельних майданчиків. Це суттєво ускладнює процеси ідентифікації правопорушників та їхнього переслідування з боку правоохоронних органів.

Кіберзлочинність спричиняє значні економічні втрати не лише фізичним особам, а й масштабним суб'єктам господарювання. Яскравим ілюстративним прикладом є широкомасштабний кіберінцидент у червні 2017 року, спровокований шкідливим програмним забезпеченням "Petya.A", який паралізував діяльність численних критично важливих українських державних і приватних установ, включаючи Міжнародний аеропорт "Бориспіль", ПАТ "Укртелеком", Чорнобильську атомну електростанцію, АТ "Укрзалізниця", а також Кабінет Міністрів України та інші подібні структури. Фахівці Міжнародного валютного фонду здійснили оцінку, згідно з якою сукупні економічні збитки від атаки вірусу "NotPetya" сягнули 850 мільйонів доларів США.[5]

Перед правоохоронними структурами постає актуальна проблематика протидії багатогранним викликам, що їх створює кримінальна діяльність у тіньовому сегменті інтернету. Характерні для цього середовища анонімність користувачів та використання криптографічних методів істотно ускладнюють процеси виявлення та ідентифікації правопорушників. Це зумовлює необхідність впровадження інноваційних технологічних рішень та стратегічних підходів задля ефективної нейтралізації цих бар'єрів. Транснаціональний вимір злочинних проявів у

Даркнеті актуалізує потребу в інтенсивній міжнародній взаємодії та оперативному обміні розвідувальною інформацією між компетентними органами України та їхніми іноземними партнерами.

Так наприклад, Європейський центр боротьби зі злочинністю Європолу щорічно готує звіт “Оцінка загрози організованої злочинності в Інтернеті” – ІЮСТА. Аналітичні матеріали для ІЮСТА готуються на основі роботи експертів Європолу, правоохоронних органів, партнерів з приватного сектору та наукового середовища. На жаль, в Україні такі дослідження ще не проводилися, хоча актуальність цієї проблеми вкрай висока, адже українські хакери постійно розшуковуються правоохоронними органами різних країн по всьому світу, починаючи від міжнародного злочинного угруповання “CarderPlanet”, яка діяла на початку 2000-х рр. Затримані в різних країнах громадяни України через завдані іноземним компаніям мільйонні збитки отримують великі (30 – 40 років) терміни позбавлення волі.[6]

Враховуючи транснаціональний характер організованої злочинності та її здатність до ефективної координації на глобальному рівні, результативна протидія цій загрозі можлива виключно шляхом консолідованих міжнародних зусиль. Стрімкий технологічний прогрес та динамічна еволюція кіберпростору обумовлюють необхідність безперервного професійного вдосконалення компетенцій суб’єктів правоохоронної діяльності. Одночасно критично важливою є імплементація інноваційних інструментів для комплексного моніторингу та розширеного аналізу операцій у тіньовому сегменті інтернету (Даркнеті). Отже, вироблення адаптивних стратегічних підходів та застосування передових технологічних рішень становлять фундаментальний аспект успішної боротьби з кіберзлочинністю в умовах багатовимірного цифрового середовища.

В Україні після потужних кібератак, які були спрямовані на об’єкти критичної інфраструктури, було прийнято низку заходів щодо посилення кібербезпеки та протидії кіберзлочинності. Зокрема це прийняття Стратегії кібербезпеки України, створення Департаменту кіберполіції, посилення спроможності нових структур завдяки західним партнерам, навчання кіберполіцейських та слідчих виявленню та розслідуванню кіберзлочинів [7].

Таким чином, Даркнет являє собою багатогранну та специфічну складову цифрової екосистеми, що, окрім надання можливостей для анонімної взаємодії, активно експлуатується для реалізації протизаконних діянь широкого спектра. Застосування криптографічних методів, архітектури прихованих сервісів та децентралізованих фінансових

інструментів (криптовалют) значно ускладнює процедури виявлення, встановлення особи та притягнення до правової відповідальності суб'єктів, що вчиняють девіантні дії. Ця обставина генерує суттєві перешкоди для діяльності правоохоронних структур та всієї архітектури кібербезпеки.

Проведене дослідження демонструє транскордонний характер кіберзлочинності в сегментах Даркнету, що зумовлює необхідність ефективної протидії шляхом інтенсифікації міжнародної кооперації, реформування національного правового поля та імплементації передових технологічних рішень для моніторингу та аналізу потенційних кібернетичних загроз. Ключовим аспектом також є формування спеціалізованих підрозділів кіберполіції та системне підвищення кваліфікації експертів у галузі інформаційної безпеки.

Відтак, в контексті прискореної цифровізації соціуму, проблематика правового регламентування Даркнету та протидії кібернетичній злочинності вимагає подальшого емпіричного та теоретичного осмислення, а також всебічного оптимізування механізмів державної та транснаціональної координації у площині кібернетичної безпеки.

Список використаних джерел

1. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі “Даркнет”. Інформація і право. № 3(26)/2018. С. 102-108.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-VIII. – (База даних “Законодавство України” / ВР України). – Режим доступу : <http://zakon.rada.gov.ua/laws/show/2163-19>
3. Deep web vs. dark web: What's the difference? URL:<https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web-vs-deep-web/>
4. Гринюк Р. Особливості функціонування Даркнету та проблеми протидії кіберзлочинності // Dictum Factum. URL: <https://df.duit.in.ua/index.php/dictum/article/view/364/327> (дата звернення: 13.05.2026).
5. Збитки від глобальних кібератак у світі сягнули \$ 53 мільярдів – МВФ. UKRINFORM. 11.10.2017. URL: <https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-milardivmvf.html>
6. Кравчук В. М. Проблеми протидії кіберзлочинності у мережі Даркнет. URL: https://ippi.org.ua/sites/default/files/13_9.pdf (дата звернення: 13.05.2026).
7. DR Mykhaylo Gutsalyuk. Ukraine's Cybersecurity strategy and ways to implement it // European Cybersecurity journal. – Volume 2 (2016). – P. 65-69. – (The Kosciuszko Institute. Poland). URL: <https://twitter.com/i/moments/781827366100140032>