***Яровий Кирило Васильович,***
кандидат юридичних наук, старший
викладач кафедри кримінології
та інформаційних технологій
Національної академії внутрішніх справ

## СТРАТЕГІЇ ПРОТИДІЇ СУЧАСНІЙ КІБЕРЗЛОЧИННОСТІ В МЕРЕЖІ DARKNET

Сучасний розвиток інформаційних технологій, окрім позитивного впливу, зумовлює також появу нових викликів у галузі кібербезпеки. Кіберзлочинність включає різноманітні види правопорушень, що здійснюються у цифровому середовищі з використанням мережевих технологій та методів анонімізації. Зокрема, актуальним залишається питання протидії кіберзлочинності в контексті мережі DarkNet, де тіньові онлайн-ринки та автоматизовані боти значно сприяють ескалації злочинної активності в кіберпросторі. Однак, незважаючи на актуальність досліджень у сфері кіберзлочинності зазначена проблема залишається багатогранною та вимагає комплексного підходу, що поєднує технологічні, організаційні та юридичні аспекти.

Своєю чергою тіньовий або глибинний Інтернет (Deep Web) охоплює значну частину мережі-Інтернет, який не підлягає індексації звичайними пошуковими системами. Окрім цього, глибинний Інтернет складається з веб-ресурсів, доступ до яких обмежується системами автентифікації, що унеможливлює їхній пошук за допомогою загальнодоступних пошукових механізмів. З огляду на вказане, особливу увагу слід приділити області мережі, відомій як DarkNet.

Поняття DarkNet відноситься до спеціалізованої частини Інтернету, яка гарантує анонімність користувачів та захищеність веб-сайтів від відстеження. Децентралізований характер DarkNet охоплює вебсайти, розташовані на серверах із прихованими IP-адресами, що забезпечує мінімальну можливість їх ідентифікації. Відсутність єдиного центру контролю в DarkNet створює умови для поширення нелегальної діяльності,

Зважаючи на погляди окремих дослідників, слід зазначити, що значна частина контенту мережі DarkNet містить легальний контент, однак, інша її сторона асоціюється з незаконною діяльністю, зокрема торгівлі забороненими товарами та послугами, включно торгівлею людьми [1, с. 323]. Важливою проблемою DarkNet є приховування кримінальної діяльності

через закриті форуми, які орієнтовані на експлуатацію потенційних жертв та просування незаконних послуг.

Українське законодавство не містить обмежень на використання програмного забезпечення та технічних засобів, які надають користувачам повну анонімність під час доступу до мережі DarkNet. Окрім того, існують технічні труднощі у блокуванні функціонування таких програмних продуктів і рішень. Дослідження можливостей ідентифікації осіб у мережах Інтернет та DarkNet є ключовим аспектом, що підкреслює необхідність розробки ефективних стратегій для протидії сучасній кіберзлочинності.

Доступ до мережі DarkNet можливий тільки за допомогою спеціалізованого програмного забезпечення, найпоширенішим з яких є браузер TOR (The Onion Router). TOR є спеціально налаштованим браузером, який дозволяє користувачам отримувати доступ до веб-сервісів способами, що ускладнюють або унеможливлюють їх відстеження.

TOR можуть користуватися особи для доступу до різноманітних ресурсів, до яких раніше було обмежено доступ [2, с. 98]. Варто зазначити, що не весь контент містить заборонений або аморальний характер, оскільки багато користувачів використовують зазначену технологію виключно для збереження анонімності в мережі-Інтернет.

Браузер TOR забезпечує захист даних за допомогою багаторівневого шифрування, яке передбачає передачу трафіку через три незалежні сервери, розташовані у різних частинах світу. Такий метод шифрування значно ускладнює можливість спостереження за діями користувача в мережі-Інтернет [3, с. 1087].

Водночас користувачі, залучені до незаконних операцій, таких як розповсюдження дитячої порнографії, торгівля наркотичними речовинами, людьми чи зброєю можуть бути виявлені правоохоронними органами, що застосовують спеціалізовані методи моніторингу для виявлення кіберзлочинців.

Зростання статистичних показників кіберзлочинності підкреслює необхідність посилення заходів кібербезпеки. DarkNet залишається одним із ключових осередків кіберзлочинної діяльності, що потребує розробки ефективних стратегій протидії та впровадження сучасних технологій моніторингу й контролю для зменшення ризиків у кіберпросторі.

Стратегічно важливим завданням державної політики України є розвиток державної системи стратегічного

планування, створення інтегрованої системи моніторингу, аналізу, прогнозування та прийняття рішень у сфері національної безпеки та оборони [4]. Зазначене включає забезпечення ефективної координації та злагодженого функціонування єдиної мережі ситуаційних центрів ключових державних органів у секторі безпеки та оборони, що сприятиме підвищенню рівня захищеності країни від сучасних загроз.

Між тим, дослідження сучасних стратегій протидії кіберзлочинності у DarkNet є вкрай актуальним і передбачає аналіз інноваційних методів відстеження анонімних дій, розробку нових технологій для моніторингу та оцінки ризиків, а також вироблення ефективних підходів до ідентифікації злочинних угруповань та припинення їх діяльності.

Враховуючи вищевикладене, необхідно зробити наступні висновки, що для ефективної протидії викликам у мережі-Інтернет необхідні не лише сучасні технічні заходи правоохоронних органів, а й удосконалення законодавства та міжнародне співробітництво. Важливо також підвищувати обізнаність користувачів щодо безпечного користування мережею DarkNet та можливих наслідків її порушення. Крім цього, слід досягти балансу між заходами безпеки та приватністю, забезпечити оперативне реагування на злочини та уникати порушень прав користувачів мережі DarkNet.

***Список використаних джерел***

1. Okhrimenko, Ivan M; Okhrimenko, Svitlana S; Yarovyi, Kyrylo V; Melnykov, Illia M; Kudinov, Vadym A; Marchenko, Olga G; Bordiyan, Yaroslav I. (2024) Motivational orientations of students towards internet dependent behavior and measures for its prevention Polski merkuriusz lekarski: organ Polskiego Towarzystwa Lekarskiego. 52 (3), 319-325. doi: 10.36740/Merkur202403108.

2. Ткачук Т. Ю. Тіньовий Інтернет: співвідношення можливостей і загроз. Інтернет речей: проблеми правового регулювання та впровадження : матеріали наук.-практ. конф., 24 жовт. 2017 р. Київ : Політехніка, 2017. С. 94–100.

3. Ahmed Ghappour, Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, 69 Stan. L. Rev. 1075, 1083 (2017); Restatement (Third) of the Foreign Relations Law of the United States § 432(2) (дата звернення 30.10.2024).

4. Про рішення Ради національної безпеки і оборони України від 26.05.2015 р. № 287/2015 «Про Стратегію національної безпеки України». URL: https://zakon.rada.gov.ua/laws/show/287/2015.