УДК 336.71:330
DOI https://doi.org/10.32850/sulj.2021.1.29

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ СУЧАСНІЙ КІБЕРЗЛОЧИННОСТІ В МЕРЕЖІ «ДАРКНЕТ»

Тімашов В. О., Діденко Д. Ш.

Стаття присвячена аналізу міжнародного досвіду протидії сучасній кіберзлочинності в мережі «Даркнет». Розглянуто проблемні питання, пов'язані з міжнародною та національною законодавчою базою у сфері захисту та запобігання злочинністю у цій мережі. Проаналізовано головні міжнародні документи, що регулюють питання кіберзлочинності, та виявлено шляхи їх удосконалення.

Увагу зосереджено на тенденціях кіберзлочинності в мережі «Даркнет», досліджено прояви кіберзлочинності й активності кібератак світового рівня та національного простору. Також розглянуті питання забезпечення нині кібербезпеки, які однаково стосуються фізичних і юридичних осіб, а також держави загалом.

Досліджено напрями міжнародної взаємодії у сфері протидії кіберзлочинності в мережі «Даркнет», що базуються на міжнародних нормативно-правових актах.

У статті досліджуються окремі питання, пов'язані з використанням новітніх технологій мережі «Даркнет» у злочинній діяльності, вирішення яких надалі призведе до мінімалізації випадків вчинення такого правопорушення. Виявлено особливості злочинів у сфері вебтехнологій, основні проблеми щодо їх виявлення, розкриття та розслідування.

Розкрито основні прогалини в законодавстві, необхідність підвищення рівня вмінь та навичок спеціалістів, яких залучено для попередження порушень у мережі «Даркнет». З'ясовано, що існує необхідність у вдосконаленні механізму підготовки спеціалістів задля підвищення рівня ефективності роботи та професійності. Це дасть змогу не тільки збільшити рівень розкриття злочинів, але й запобігти їх виникненню. Своєю чергою зменшення злочинної діяльності в мережі «Даркнет» сприятиме безпечнішому існуванню суспільства.

З'ясовано та досліджено погляди вчених, які вивчали це питання. Розглянуто низку аспектів, пов'язаних із розвитком сучасного кіберпростору, та новітніх методів, що вигадують володарі незаконного бізнесу у цій мережі.

Досліджено практику різних країн у розкритті кіберзлочинів. Проаналізовано законодавство України на міжнародному рівні. Шляхом аналізу чинного законодавства, наукових статей та інших ресурсів були визначені і викладені недоліки та позитивні аспекти правового регулювання.

На основі досліджених матеріалів сформульовано висновки та пропозиції щодо вдосконалення сфери розкриття й попередження злочинів, ведення незаконного бізнесу в мережі «Даркнет». Визначено можливі способи вирішення найбільш актуальних питань з удосконалення цієї сфери з метою забезпечення охорони та захисту основоположних прав суб'єктів різних держав світу.

Ключові слова: *Інтернет, мережа «Даркнет», кіберзлочинність, міжнародне співробітництво, міжнародні кіберзлочини.*

Timashov V. A., Didenko D. Sh. The international experience in combating modern cybercrime in the Darknet network

The article is devoted to the analysis of the international experience in combating modern cybercrime in the Darknet. Issues related to the international and national legal framework in the field of protection and prevention of crime in this network are considered.

The main international and documents regulating cybercrime issues are analyzed and the ways of their improvement are revealed. Attention is focused on the trends of cybercrime in the network "Darknet", the manifestations of cybercrime and the activity of cyberattacks of world level and national space are studied. Also considered are issues of cybersecurity to date, which apply equally to individuals and legal entities, as well as the state.

The directions of international cooperation in the field of combating cybercrime in the Darknet network, based on international regulations, are studied.

The article is researched some issues related to the use of the latest technologies of the Darknet network in criminal activities, the solution of which will minimize the commission of such an offense in the future. The peculiarities of crimes in the field of web technologies, the main problems of their detection, detection and investigation are revealed.

We revealed the main gaps in the legislation, the need to increase the level of skills and abilities of specialists involved in the prevention of violations in the network

"Darknet". It was found that there is a need to improve the mechanism of training in order to increase the level of efficiency and professionalism. This will allow not only to increase the level of crime detection, but also to prevent their occurrence. So, reducing criminal activity in the Darknet network will contribute to a safer existence of society.

The views of scientists who have studied this issue have been clarified and studied. A number of aspects related to the development of modern cyberspace and the latest methods invented by the owners of illegal business in this network are considered. The practice of different countries in detecting cybercrimes is studied. The legislation of Ukraine at the international level is analyzed.

By analyzing the current legislation, scientific articles and other resources, the shortcomings and positive aspects of legal regulation were identified and outlined. On the basis of the researched materials the conclusions and offers on improvement of the sphere of detection and prevention of crimes and conducting illegal business in the network "Darknet" are formulated and possible ways of the decision of the most actual questions on improvement of this sphere for protection and protection of the fundamental rights of subjects of the world.

Key words: *Internet, cybercrime, international cooperation, international cooperation, international cybercrime.*

Постановка проблеми та її актуальність. XXI століття характеризується бурхливим розвитком мережі Інтернет. Використання новітніх технологій дає змогу виконати велику кількість операцій, придбати товар чи замовити послугу, не витрачаючи зайвого часу та не виходячи з дому.

Водночас технологічний розвиток позначився і на кіберзлочинності. Одним із новітніх явищ є темна мережа «Даркнет», яка вирізняється особливою жорстокістю та різноманітністю злочинності, що викликає стурбованість не тільки в Україні, але і у всьому світі.

«Даркнет» – це частина Інтернету, в якій неможливо відслідкувати користувачів та адреси сайтів. «Даркнет», або темний Інтернет, або секретний Інтернет – це сукупність вебсайтів, які мають приховані IP-адреси сервера, на якому вони розміщені. Мережі «Даркнету» є децентралізованими, вони не контролюються кимось одним. Це забезпечує певну свободу дій користувачам.

Звісно, значна частина мережі «Даркнет» є законною. Для цілей використання доступ до цієї мережі можливий тільки через протокол Onion Router (або Tor) або аналогічні протоколи. Tor – це спеціально сконфігурований браузер, що дає змогу користувачам отримувати доступ до вебслужб способами, які важко або неможливо відстежити.

Між тим дослідник із Королівського коледжу Лондона виявив, що 57% вебсайтів із прихованими послугами в мережі Tor сприяють злочинній діяльності, включаючи продаж наркотиків, нелегальне фінансування та порнографію, із залученням до насильства, дітей та тварин [1].

Але залишаються інші 43% вебсайтів, які створюють загрозу для міжнародної спільноти та вирізняються своєю надмірно незаконною діяльністю. Недостатність досвіду в боротьбі з новими технологіями сьогодення є благодатним ґрунтом для злочинної діяльності, що постійно розвивається технологічно та створює постійні виклики для урядів майже всіх країн світу.

Аналіз останніх досліджень і публікацій. Проблемами правового регулювання захисту та протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська, П.Д. Біленчук, К.І. Бєляков, В.М. Бутузов, В.Д. Гавловський, М.В. Гуцалюк, М.А. Погорецький, В.Г. Хахановський, В.П. Шеломенцев, О.М. Юрченко та інші. Ці науковці звертали увагу на окремі питання протидії, захисту від кримінальних правопорушень в мережі Інтернет. Проте питання є значним для дослідження і потребує додаткової уваги.

Метою статті є визначення проблем та сутності міжнародної протидії та співпраці правоохоронних органів різних країн у боротьбі з кіберзлочинністю в мережі «Даркнет», стану їх правової визначеності, а також надання пропозицій до удосконалення роботи.

Виклад основного матеріалу. «Даркнет» – це частина Інтернету, що використовує технології шифрування і анонімності, призначені для запобігання відстеження.

Типові веббраузери розкривають свої унікальні IP-адреси (Інтернет-протоколи), що дає змогу відстежувати їх дії правоохоронними органами. Але веббраузер у «Даркнеті» видає помилкові IP-адреси, щоб замаскувати особистість користувача.

Сам браузер Tor був спочатку розроблений у Військово-морської дослідницької лабораторії США в 1990-х роках і опублікований у 2002 році. Оскільки Dark Web дозволяє користувачам залишатись анонімними завдяки шифруванню, це є привабливим для всіх, хто займається незаконною діяльністю, наприклад, незаконний продаж наркотиків чи контрафактними товарами, дитячою порнографією, секс-торгівлею. Але це також може бути корисно для тих, хто живе в авторитарній державі, бажаючи спілкуватися із зовнішнім

світом, а також забезпечує безпечний простір для викривачів [1].

Саме для запобігання та протидії кіберзлочинності у 2001 р. у Будапешті була прийнята Конвенція про кіберзлочинність [2], яка була ратифікована Верховною Радою України із застереженнями і заявами Законом № 2824-IV від 07.09.2005 р.

Конвенцією визначено кілька груп правопорушень, які належать до кіберзлочинів, зокрема:

- правопорушення проти конфіденційності;
- правопорушення, пов'язані з комп'ютерами;
- правопорушення, пов'язані зі змістом;
- правопорушення, пов'язані з порушенням авторських та суміжних прав [2].

Крім того, в Україні прийнято Закон «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 5 жовтня 2017 р., яким зазначено, що кіберзлочин, або комп'ютерний злочин, – це суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена українським законодавством щодо кримінальної відповідальності та/або яке визнано злочином міжнародними договорами України [3].

В Україні стрімко розвиваються технології та методи злому та розкриття кіберполіцією Інтернет-злочинів, тому перейняття досвіду інших країн є доцільним явищем для досягнення позитивного результату.

Одним з основних способів спіймати злочинців є робота під прикриттям, що іноді може призвести до реальних зв'язків, коли, наприклад, офіцер, який видається продавцем, отримує поштову адресу покупця. Крім того, суб'єкт розслідування може спіткнутися і розкрити особисту інформацію. Оскільки найбільше злочинів припадає на США, то й багато транзакцій, що проводяться через «Даркнет», виконуються Поштовою службою США. Поліція іноді може поєднувати підказки в Інтернеті з кадрами спостереження, аналізом почерку та іншими підказками. Не менш цікавим способом є ідентифікування відбитків пальців на упаковці, що потенційно може розкрити особу відправника.

Хоча анонімність біткойнів ускладнює відстеження перерахування коштів, Міністерство національної безпеки США має спеціальну робочу групу, орієнтовану на відстеження відмивання грошей за допомогою криптовалют. Інші підходи передбачають використання складних технологій та методів злому.

Наприклад, ФБР використовувало шкідливе програмне забезпечення для пошуку сайту дитячої порнографії Playpen. Програмне забезпечення змусило користувачів, які натиснули на форум, розкрити їх справжні IP-адреси, які потім були надіслані слідчим. Ще одна техніка злому використовувала вразливість браузера Tor, дозволяючи слідчим розкривати IP-адреси вебринків мережі «Даркнет» та її користувачів [4].

Нині боротьба зі злочинами в мережі «Даркнет» вийшла на світовий рівень. Такі країни, як США та Великобританія, ведуть активну боротьбу та намагаються розкрити якомога більше кіберзлочинів. Міжнародне співробітництво та взаєморозуміння мають вирішальне значення для досягнення спільної мети в боротьбі з кіберзлочинами.

Професор Стенфордської школи права Ахмед Гаппур опублікував оглядову статтю про урядову співпрацю та подальші результати діяльності для міжнародного права. У своїй статті Гаппур затверджує, що «використання правоохоронними органами хакерських методів для проведення досліджень, передбачених у процесі передачі даних у мережі «Даркнет», може порушити суверенітет інших країн» [5].

Дійсно, суверенітет держави є важливим пріоритетом для міжнародного співтовариства, який має враховуватися владою під час злому «Даркнету» через те, що ризик результату переслідувань та електронний слід може виявитися в іноземній країні. Національне право допускає здійснення договірної юрисдикції зарубіжним державним управлінням за наявності п'яти обставин:

1) дії, що мають останні результати в країнах;
2) захист інтересів націй;
3) національність злочинця;
4) громадянство жертви;
5) універсальна юрисдикція [8].

Проблема в тому, що, коли влада починає зламувати «Даркнет», вона не знає, чи є ефект на власній території. Анонімність закладена в суті «Даркнету».

Уряд не буде знати жодного з вищезазначених факторів, поки не виявить злочинну операцію. Тільки тоді буде встановлено національність злочинця/жертви, внутрішні наслідки та відношення до загальної національної юрисдикції.

Багато країн усвідомили важливість питання щодо можливості знайти злочинців у «Даркнеті». Чим більше хакерів адаптується та спричинить нові руйнування, тим більше країн визнає необхідність реагувати та запобігати майбутнім кібератакам. У результаті цього усвідомлення іноземні держави оприлюднили конвенції, спрямовані на запобігання та припинення кіберзлочинів.

Наприклад, Рада Європи «оприлюднила» Конвенцію про кіберзлочинність, яка зобов'язує країни, що її підписали, криміналізувати різні акти комп'ютерного зловживання та екстрадувати або притягнути до відповідальності правопорушників.

Більше 50 країн, включаючи США, підписали Конвенцію ЄС про кіберзлочинність [6]. Однією з кінцевих цілей Конвенції ЄС є «проведення в першочерговому порядку спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, зокрема, шляхом прийняття відповідного законодавства та сприяння міжнародному співробітництву» [2]. Україна також ратифікувала цю Конвенцію.

У своїй статті професор Гаппур підкреслює, що порушення державного суверенітету може мати наслідки, з якими США не готові боротися (іноземне переслідування, контрзаходи тощо), які можуть порушувати державний суверенітет, виконуючи правоохоронні функції на територіях іншої держави без згоди іншої держави [7].

Однак яскравим прикладом є Конвенція ЄС про кіберзлочинність. Безліч країн визнали необхідність співпраці з іноземними державами для боротьби зі зростаючою небезпекою кіберзлочинності.

Як зазначає Орін Керр у своїй статті, «використання одного уряду NIT (техніка розслідування мереж) для розслідування злочинів у мережі «Даркнет», як правило, інші уряди вітають, а не побоюються» [7].

Професор Орін Керр наводить розслідування про проблему одного зі злочинних сайтів як приклад співпраці між іноземними державами. Він був вебсайтом для дитячої порнографії, доступним лише в темній мережі, який мав понад 100 000 унікальних облікових записів користувачів. NIT, встановлений Сполученими Штатами відповідно до ордера, закінчився обшуком понад тисячі комп'ютерів у багатьох країнах. Це призвело до подальших розслідувань та сотень арештів по всьому світу [7].

Нещодавно австралійський уряд застосував фішинг-атаку, щоб зламати комп'ютери користувачів «Даркнету», які відвідували вебсторінки дитячої порнографії під назвою «The Love Zone». Принаймні в одному з відомих випадків австралійський уряд увірвався в комп'ютери в США. Немає жодних ознак того, що уряд Сполучених Штатів або американська громадськість були ображені іноземними пошуками.

Навпаки, влада США розпочала розслідування та порушила національні кримінальні справи на основі злому іноземного уряду [8].

Згадані вище приклади – це лише кілька прикладів, що демонструють міжнародну співпрацю між країнами в боротьбі з кіберзлочинами. Однак може бути ситуація, при якій розслідування в країні, яка не є підписантом Конвенції та не співпрацює в зусиллях із боротьби з кіберзлочинністю, що своєю чергою може звести таке розслідування нанівець.

Висновки. Якщо підсумовувати вищезазначене, Україна також має певний досвід у розкритті міжнародних кіберзлочинів. Необхідно розуміти, що є загальні потреби та проблемні питання щодо більш активної боротьби з кіберзлочинністю в Україні.

Наприклад, необхідно удосконалити законодавство в частині перевірки міжнародних/національних пакунків, відвантажених поштою чи іншими службами, відслідковувати швидкісні зміни в обсязі злочинності. Правоохоронні органи бачать докази постійного розширення незаконної вебдіяльності, але в основному не мають кількісних даних, щоб надати ефективні відповіді та рішення щодо її розкриття.

Окрім того, глобалізація є необхідним явищем покращення боротьби країн із кіберзлочинністю в мережі «Даркнет». Адже його діяльність перетинає державні та транснаціональні кордони. Характер «Даркнету» між юрисдикціями робить необхідною співпрацю між слідчими агенціями різних країн. Якщо агенції його уникатимуть через перехресний юрисдикційний характер, злочинні павутини можуть бадьоріше вести свою діяльність через відсутність примусу до закриття незаконного бізнесу за допомогою цієї мережі.

Простежується необхідність демістифікації «Даркнету». Деякі представники правоохоронних органів можуть мати занепокоєння з приводу того, що їм та їхнім підрозділам помстяться зловмисні вебкористувачі та як вони будуть діяти проти інтересів мережі. Враховуючи відсутність остаточних кількісних даних, правоохоронці можуть діяти без вичерпної інформації щодо того, як це працює і що потрібно для вирішення цих вебпроблем.

Звичайно, без вдосконалення наявних навичок не можна вийти на новий рівень розслідування. Додаткове навчання та дослідження основ командою фахівців могли би показати гарний результат. Для протидії злочинам у «Даркнеті» можна створити дві гілки навчання майбутніх фахівців, що будуть боротися із цим видом порушень. Перш за все, це робота з цифровими доказами, методами їх виявлення. Для спеціалізованих підрозділів це цілеспрямоване навчання з питань збереження

доказів, а також підвищення кваліфікації щодо методів, які використовуються злочинцями в темній мережі. Але залишається відкритим питання щодо наявності експертів у цій галузі.

Не менш важливим питанням є проблема доказової бази, оскільки збільшується кількість даних, нерозбірливих форматів, функцій шифрування. Анонімність програмного забезпечення створює додаткові труднощі для збору та розшифрування доказів. З цією метою з'являється пріоритетна задача використання найкращих та найновіших стандартів та інструментів. Доцільно переймати досвід інших країн, ділитися власним та об'єднувати ресурси.

Доведено, що успішні операції правоохоронних органів проти інтересів темної мережі зазвичай забороняють користувачам швидко адаптуватися до певного ринку вебмережі. Саме тому користувачі «Даркнету» можуть часто обмінюватися інформацією про те, як уникнути виявлення правоохоронних органів. І це також потрібно брати до уваги та змінювати, осучаснювати методи, способи та підходи щодо виявлення та попередження злочинів.

І наостанок, анонімність. Існує загроза зі сторони злочинців мережі на провокації або незаконні дії у бік правоохоронців, які займаються конкретною справою. Не є секретом, що «Даркнет» вирізняється особливою жорстокістю та власними методами ведення бізнесу. Саме тому необхідно убезпечити службовців від усіх наявних загроз.

Міжнародне співробітництво та взаєморозуміння мають вирішальне значення для досягнення спільної мети в боротьбі з кіберзлочинами.

Однак зловити кіберзлочинців у країнах, де існує міжнародний договір чи угода, не є проблемою. Проблема полягає в тому, що деякі найпоширеніші кіберзлочини нині походять з країн, в яких немає взаємних домовленостей, таких як Північна Корея. Однак, якщо Сполучені Штати навмисно намагаються відслідковувати та знищувати відомих північнокорейських хакерів, дії Сполучених Штатів можуть бути виправдані принципом, що Сполучені Штати можуть здійснювати кримінальну юрисдикцію на основі наслідків у межах нації та захищати інтереси нації.

Також варто пам'ятати, що ефективна робота правоохоронців із протидії кіберзлочинності в мережі «Даркнет», перш за все, ґрунтується на досконалому законодавстві, яке своєю чергою підлаштоване під міжнародні стандарти та сучасний науково-технічний розвиток.

Література

1. Daniel Moore and Thomas Rid. Cryptopolitik and the Darknet, Survival, 2016, № 58(1), P. 7–38. URL: https://www.tandfonline.com/doi/full/10.1080/00396338.2016. 1142085 (дата звернення 11.03.2021).

2. Конвенція про кіберзлочинність : Закон України від 07.09.2005 р. № 2824-IV. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 11.03.2021).

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon.rada.gov.ua/laws/show/ 163-19 (дата звернення 14.03.2021).

4. Dark Web Crimes. URL: http://www.findlaw.com/criminal/criminal-charges/dark-web-crimes.html (дата звернення 11.03.2021).

5. Ahmed Ghappour. Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web, 69 Stan. L. Rev. 2017, 1075. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2742706 (дата звернення 15.03.2021).

6. Chart of Signatures and Ratifications of Treaty 185. *Treaty Office*, Council of Europe. URL: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=IAInZomh (дата звернення 11.03.2021).

7. 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 12.03.2021).

8. To Catch a Criminal: Hacking into the Dark Web and International Law Implications. URL: https://law.utah.edu/to-catch-a-criminal-hacking-into-the-dark-web-and-international-law-implications/ (дата звернення 12.03.2021).

Тімашов В. О.,
доктор юридичних наук, доцент,
професор кафедри адміністративного,
фінансового та інформаційного права
Київського національного
торговельно-економічного університету

Діденко Д. Ш.,
студентка магістратури
Київського національного
торговельно-економічного університету