***ДИКИЙ ОЛЕГ ВІКТОРОВИЧ***

*Національний університет «Одеська юридична академія»,*
*декан факультету кібербезпеки та інформаційних технологій,*
*кандидат юридичних наук, доцент*

## КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРВІЙНА: СУЧАСНІ ВИКЛИКИ

XIX століття стало епохою тотальної інформатизації та кібернетизації усіх сфер життя у всіх цивілізаційних країнах світу. З однієї сторони це дозволило покращити, спростити життя людей, з іншої створило нові виклики, наприклад кіберзлочинність.

Під час військової агресії російської федерації проти України першими завдавалися саме кібератаки – масові DDoS-атаки на державні сайти України, банківську систему, ще 23 лютого 2022 року, тобто за день до повномасштабного вторгнення та обстрілів українських міст. Очевидно, що такі атаки вчиняються не одинокими хакерами «любителями», а окремими структурами висококваліфікованих професіоналів, до того ж тісно зв'язаними із державним апаратом країни-агресора, а тому їх дії не охоплюються категорією «кіберзлочини», а маю іншу природу – «кібервійна».

У війні «XXI століття» кіберфронт виявися одним із серйозних напрямків активних дій, що безумовно пов'язано із цифровізацією обох сторін війни. Звернемося до дефініції терміну кібервійна. Так, американський експерт у галузі кібербезпеки Р. Кларк, пропонує так трактування: «кібервійна – дії однієї національної держави з проникненням у комп'ютери чи мережі іншої національної держави для досягнення цілей завдання шкоди чи руйнування» [1]. Вітчизняний експерт О. Мережко пропонує таке визначення: «Кібервійна – використання Інтернету та пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній, інформаційній безпеці та суверенітету іншої держави» [2].

Враховуючи сучасні тенденції Генеральна Асамблея Організації Об'єднаних Націй у резолюції від 17.12.2018 року виразила занепокоєність посиленням кіберзлочинності і використанням інформаційних та телекомунікаційних технологій при вчинені багатьох видів злочинів. У зв'язку з цим, рекомендувала державам-членам активізувати їх зусилля у боротьбі з кіберзлочинністю і злочинним використанням інформаційних і комунікаційних технологій у всіх його формах та розвивати міжнародне співробітництво в цій сфері, включаючи обмін електронними доказами [3].

Варто відзначити, що питання визначення кіберзлочинності та її протидії хоча є недосконалими, все ж є юридично визначеними. Однак зміст кібервійни, правил її ведення, кібератак та відповідальності за такі дії залишаються поза межами регулювання міжнародного права.

Не меншого значення має наукове вивчення кібервійни, як явища, яке у вітчизняній доктрині перебуває не досить розвиненим, незважаючи на прикладні дослідження вчених. Причин цьому може бути безліч, наприклад, відсутність чітких меж предмету дослідження, застарілі методики збору та аналізу емпіричного матеріалу, ігнорування у використані результатів досліджень вчених, у першу чергу, з розвинених країн Європи та США тощо. У зв'язку з цим природа кібервійни спотворюється, спрощується до комп'ютерних злочинів. Більше того, відсутність ґрунтовних кримінологічних досліджень кіберсередовища створюють реальні проблеми у практиці протидії і такому виду злочинності, як кіберзлочинність в контексті міжнародного співробітництва. Так, в доповіді по роботі двадцять п'ятої сесії комісії з попередження злочинності і кримінального правосуддя Економічної і соціальної ради ООН за 2016 рік було підкреслено важливість наявності адекватного національного законодавства та активізації міжнародного співробітництва в боротьбі з кіберзлочинністю.

Наприклад, учасники звертали увагу на необхідність розробки нового всеосяжного міжнародно-правового документу з кіберзлочинності, в якому основна увага буде приділена, зокрема, процесуальним питанням. Однак це питання є не вирішеним до сих пір, а головним міжнародним документом виступає Конвенція з кіберзлочинності Ради Європи, що була прийнята у 2001 році. До того ж повномасштабна війна в Україні так би мовити, виносить на показ недосконаліть та відсталість правого регулювання, в тому числі на рівні універсальних актів, явища кібервійни. Такі проблеми носять не просто теоретичний характер, а мають прикладний зміст. Так, з березня 2022 року було розпочато розслідування воєнних злочинів, скоєних росією в Україні. У цьому контексті досить нечітким видається кваліфікація кібератак, особливо на об'єкти критичної інфраструктури. Можливо теоретично припустити, що у випадку знищення майна такі дії повинні бути кваліфіковані відповідно до пп. 4 п. 2 ст. 8 Римського статуту міжнародного кримінального суду: «воєнні злочини означають: незаконне, безглузде та великомасштабне знищення та присвоєння майна, не викликане військовою необхідністю». Однак така правова невизначеність може породити і безвідповідальність. Так як, виникає наступне запитання, чи є інформація об'єктом майна в значенні універсальних норм. Вказане детермінує перед цивілізованим світом питання урегулювання в межах універсальних документів питань відповідальності та правил ведення кібервійни, а також питання протидії кіберзлочинності.

Науковим підґрунтям пошуку розробки може стати кіберкримінологія як приватно-науковий напрям кримінології. Так, вперше кіберкримінологія як науковий напрям була запропонована у 2007 році індійським вченим К. Джайшанкаром. У своїй роботі науковець визначає дефініцію кіберкримінології: «…як, вчення про причинно-наслідкові зв'язки при вчиненні злочинів, що відбуваються в кіберпросторі та їх вплив на фізичний простір» [4]. Безумовно, вказане визначення не відображає всю сутність кримінології загалом і кіберкримінології, як її

складової, а тому потребує додаткового дослідження крізь призму сучасних досліджень та умов в якому опинилося людство.

Очевидно, що кіберкримінологія за своєю природою є мультидисциплінарною галуззю дослідження. Вона охоплює криміналістику, соціологію, психологію, віктимологію комп'ютерні та інтернет-науки. До того ж, в основі кіберкримінології лежить вивчення злочинної поведінки та віктимізації в кіберпросторі з поведінкової теоретичної точки зору, що видається з одного боку перспективним, з іншого – надскладним. Це пов'язано, у першу чергу, з емпіричним матеріалом. Це одна із важливих проблем, які необхідно вирішити кіберкримінології для вироблення ефективних заходів протидії цьому виду злочинності. Саме кіберкримінологія повинна стати тією галуззю знань, яка дозволить більш детально дослідити кіберпростір з точки зору порушення норм закону.

***Список використаних джерел:***


1. Richard A. Clarke and Robert K. Knake»Cyber War: The Next Threat to National Security and What to Do About It» (Harper Collins 2010). 2011. 320 p.
2. Мережко А. А. Конвенция о запрещении использования кибевойны в глобальной информационной сети информационных и вычислительных ресурсов (Интернете). *Політичний менеджмент*. URL: https://web.archive.org/web/20111007185753/http://www.politik.org.ua/vid/publcontent.php3?y=7&p=57
3. Укрепление программы Организации Объединенных Наций в области предупреждения преступности и уголовного правосудия, в особенности ее потенциала в сфере технического сотрудничества. Принята резолюцией 73/186 Генеральной Ассамблеи ООН от 17 декабря 2018 года. *Организация Объединенных Наций : офіційний веб-сайт.* URL: https://undocs.org/pdf?symbol=ru/A/RES/73/186
4. Jaishankar K. Cyber criminology : Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*. № 1(1). P. 1–6.



**Ключові слова:** кіберкримінологія, кіберпростір, кіберзлочини.
**Key words:** cyber criminology, cyber space, cybercrime.