ТКАЧЕНКО П. І.,
аспірант кафедри кримінально-правових дисциплін
(Дніпропетровський державний університет внутрішніх справ Міністерства внутрішніх справ України)

ТКАЧЕНКО А. О.,
провідний фахівець навчально-методичного відділу
(Дніпровський гуманітарний університет)

КОВАЛЬЧУК Д. В.,
студент V курсу магістратури
(Національний технічний університет «Дніпровська політехніка»)

УДК 343
DOI https://doi.org/10.32842/2078-3736/2023.3.41

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ, ЯКА ВЧИНЯЄТЬСЯ ЗА ПОПЕРЕДНЬОЮ ЗМОВОЮ ГРУПОЮ ОСІБ: АНАЛІЗ ПРОБЛЕМ І ПЕРСПЕКТИВ

З огляду на стрімкий розвиток цифрових технологій та Інтернету, проблема кіберзлочинності, яка вчиняється за попередньою змовою групою осіб, стає все більш актуальною та такою, що потребує виокремлення заходів протидії та запобігання із врахуванням сучасного курсу. У статті проаналізовано сучасний стан кіберзлочинності, актуальні проблеми, зокрема загрози, які існують, як для національної так і міжнародної безпеки. Надано визначення поняттю «кіберзлочинність» та характеристику спектру існування даного виду протиправної діяльності. За результатами кримінально-правового аналізу наголошено на необхідності закріплення відповідальності за кіберзлочини на законодавчому рівні із урахуванням іноземного досвіду, країн партнерів. Здійснено вступний аналіз проблеми кримінально-правової характеристики кіберзлочинності, яка вчиняється за попередньою змовою групою осіб. Зосереджено увагу на відсутності конкретизованого визначення поняття «кіберзлочину», у вітчизняному кримінальному законодавстві, проте викладено положення ст. ст. 361–363 Кримінального кодексу України (далі – КК України), якими закріплено відповідальність за незаконне втручання в роботу комп'ютерів та мереж, незаконне використання та зміну комп'ютерної інформації та систем. У статті використано закордонні дослідження та викладено думки провідних іноземних вчених щодо загроз кіберзлочинності у безпековому вимірі. Виокремлено актуальні проблеми при виявленні та документуванні кіберзлочинів, зокрема оперативно-розшукові та кримінально-процесуальні колізії, які мають місце в практичній площині на етапі досудового розслідування. Висвітлено сучасний стан кіберзлочинності її розвиток та поширення, наголошено на необхідно-

сті кримінологічного дослідження із визначенням характеристики особи, яка вчиняє кіберзлочин, детермінанти та заходи запобігання. Визначено необхідність в подальшому розвитку забезпечення ефективності сфери кібербезпеки із врахуванням практики європейських партнерів, зокрема адаптації національного законодавства до міжнародних стандартів. Обґрунтовано необхідність не лише позитивним рівнем кібербезпеки, а й створенням привабливої платформи в сучасній державі для міжнародних інвестицій в сферу цифровізації.

Ключові слова: *кіберзлочинність, злочини в сфері кіберпростору, кіберзлочин вчинений за попередньою змовою групою осіб, кримінально-правова характеристика, кримінальна відповідальність.*

Tkachenko P. I., Tkachenko A. O., Kovalchuk D. V. Criminal-legal characteristics of cybercrime committed by a group of persons based on a prior conspiracy: analysis of problems and prospects

In view of the rapid development of digital technologies and the Internet, the problem of cybercrime, which is committed by a group of persons based on a prior conspiracy, is becoming more and more urgent and requires the identification of countermeasures and prevention measures taking into account the current course. The article analyzes the current state of cybercrime, current problems, in particular threats that exist for both national and international security. A definition of the term "cybercrime" and a description of the spectrum of existence of this type of illegal activity are given. According to the results of the criminal law analysis, it was emphasized the need to establish responsibility for cybercrimes at the legislative level, taking into account foreign experience and partner countries. An introductory analysis of the problem of the criminal-legal characteristics of cybercrime, which is committed by a group of persons based on a prior conspiracy, has been carried out. Attention is focused on the lack of a concrete definition of the concept of "cybercrime" in domestic criminal legislation, but the provisions of Art. Art. 361–363 of the Criminal Code of Ukraine, which establish liability for illegal interference with the operation of computers and networks, illegal use and alteration of computer information and systems. The article uses foreign research and presents the opinions of leading foreign scientists regarding the threats of cybercrime in the security dimension. Actual problems in the detection and documentation of cybercrimes are singled out, in particular operational-investigative and criminal-procedural collisions, which take place in the practical plane at the stage of pre-trial investigation. The current state of cybercrime, its development and spread is highlighted, the need for a criminological study to determine the characteristics of a person who commits a cybercrime, determinants and prevention measures is emphasized. The need for further development of ensuring the effectiveness of the cyber security sphere, taking into account the practice of European partners, in particular the adaptation of national legislation to international standards, has been determined. The need is justified not only by a positive level of cyber security, but also by the creation of an attractive platform in a modern state for international investments in the field of digitization.

Key words: *cybercrime, crimes in the sphere of cyberspace, cybercrime committed by a group of persons, criminal law characteristics, criminal liability.*

Вступ. Проблема кіберзлочинності становить загрозу національній та міжнародній безпеці. Відсутність чітко закріпленої юридичної відповідальності за вчинення кіберзлочину, зокрема за попередньою змовою групою осіб зумовлює дану протиправну діяльність до поширення, а програмно-цифрові новели до розвитку, суспільний рівень небезпеки від чого зростає ще більше.

Різноманітність поглядів на кримінально-правове визначення поняття «кіберзлочин» та недостатність кримінологічного дослідження зумовлюють в подальшому обґрунтовано здійснити комплексне кримінологічне вивчення проблематики сучасної кіберзлочинності.

Вивченню питання сфери кібербезпеки та кіберзлочинності, зокрема в кримінально-правовому аспекті присвячені наукові праці таких видатних українських та зарубіжних вчених, як Д. С. Азаров, О. А. Баранов, В. С. Батиргареєва, Ю. М. Батурін, П. Д. Біленчук, І. Г. Богатирьов, Т. М. Богданова, В. І. Борисов, Л. П. Брич, О. Ю. Бусол, Б. М. Головкін, О. О. Горішний, В. К. Грищук, І. І. Гуня, В. О. Глушков, Н. О. Гуторова, Л. М. Демидова, М. Ю. Дворецький, Ю. А. Дорохіна, О. О. Дудоров, К. М. Євдокімов, В. П. Ємельянов, А. Ю. Караманов, М. В. Карчевський, Д. І. Ковальов, Т. М. Лопатіна, К. Б. Марисюк, М. І. Мельник, М. А. Погорецький, О. Е. Радутний, Н. В. Савінова, І. І. Сухих, В. Я. Тацій, В. В. Тиенко та інші.

Водночас, В. П. Бєлєнький надаючи поняття «кіберзлочину» визначає його, як винне, суспільно небезпечне, кримінально каране втручання в сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, зроблені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв із вбудованими процесорами і контролерами, які можуть мати доступ до інформаційного простору [1, с. 6].

Кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов'язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію [2, с. 202].

Постановка завдання. Метою статті є розглянути питання кримінально-правової характеристики кіберзлочинності, яка вчиняється за попередньою змовою групою осіб, зокрема проаналізувати актуальні проблеми в даній сфері і перспектив їх вирішення.

Результати дослідження. З огляду на стрімкий розвиток цифрових технологій та Інтернету, проблема кіберзлочинності, яка вчиняється за попередньою змовою групою осіб, стає все більш актуальною та такою, що потребує виокремлення заходів протидії та запобігання із врахуванням сучасного курсу.

Поняття кіберзлочинність, яка вчиняється за попередньою змовою групою осіб використовується для опису випадків, коли згадана група осіб заздалегідь планує та координує свої дії для вчинення кіберзлочину. Водночас ми надаємо наступне визначення категорії кіберзлочину, а саме протиправне, кримінально каране діяння, яке вчиняється в сфері кіберпростору із використанням технічних засобів, програмно-обчислювальних машин, включаючи різноманітні форми незаконної діяльності, зокрема шахрайство, шпигунство, розповсюдження шкідливого програмного забезпечення, тощо.

Між тим варто зауважити, що кіберзлочинність, охоплює широкий спектр протиправних дій, здійснених в кіберпросторі в тому числі такі, що можуть вчинятися за попередньою змовою групою осіб, стаючи при цьому все більш поширеними в сучасному світі. За даними Johnson, протягом останніх десятиліть кіберзлочинність розширилася, і тепер вона включає все, від крадіжки до складених хакерських атак [8, с. 17].

Вітчизняне кримінальне законодавство не визначає конкретизоване поняття «кіберзлочину», проте встановлює відповідальність за незаконне втручання в роботу комп'ютерів та мереж, незаконне використання та зміну комп'ютерної інформації та систем, що передбачено ст. ст. 361–363 КК України.

На європейському рівні, Конвенція про кіберзлочинність Ради Європи визнає і встановлює відповідальність за кіберзлочини, зокрема такі, що вчинені за попередньою змовою групою осіб. Конвенція включає статті, які стосуються незаконного перехоплення даних,

системного пошкодження комп'ютерних даних, комп'ютерного шахрайства, дитячої порнографії, порушень авторського права та інших прав на комп'ютерні дані.

При цьому, важливим аспектом Конвенції є те, що вона вимагає від учасників вжити законодавчих та інших заходів для запобігання кіберзлочинності, включаючи злочини, вчинені за попередньою змовою групою осіб. Це важливо врахувати при подальшому розвитку українського законодавства в цій сфері.

Наприклад, у статті 8 «Незаконне втручання в системи» Конвенції вказано, що кожна Сторона повинна вжити необхідних законодавчих та інших заходів, щоб притягувати до відповідальності осіб, які незаконно, без права, завдають шкоди системам, що містять комп'ютерні дані або значною мірою порушують їх нормальне функціонування.

Це означає, що Європейський Союз встановив більш широкий спектр кримінальної відповідальності за кіберзлочинність. В Україні, на відміну від ЄС, ще не внесено змін до законодавства, які б відповідали цим вимогам проте розроблено достатньо широку базу, яка регулює в певній мірі дане питання.

Так, Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові, організаційні та технічні основи забезпечення кібербезпеки, а також встановлює механізми захисту від кіберзагроз.

Однак, незважаючи на наявність таких законодавчих норм, вирішення проблеми кіберзлочинності залишається важким завданням. Як вказано в роботі Gercke (2012), справжній виклик полягає не в тому, щоб визначити, чи є вчинок злочином, а в тому, як слід розслідувати і покарати винних [3, с. 42].

Також, згідно з Tallinn Manual, застосування міжнародного права до кібероперацій є складним і спірним питанням. Однак, це не означає, що міжнародне право не застосовується до кіберпростору [4, с. 109].

Враховуючи це, важливим є усвідомлення того, що кіберзлочини, вчинені за попередньою змовою групою осіб, можуть становити серйозне порушення міжнародного гуманітарного права, як це було вказано в роботі Droege (2012), кібератаки можуть спричинити значні страждання серед цивільного населення та порушити норми міжнародного гуманітарного права [5, с. 123].

Відповідно до міжнародних норм, національного законодавства України та Європейського Союзу, кіберзлочини, вчинені за попередньою змовою групою осіб, є серйозними правопорушеннями. Це підтверджує важливість неперервної боротьби з такими злочинами шляхом розробки та впровадження ефективних міжнародних стратегій та механізмів.

Однією з головних проблем у боротьбі з кіберзлочинністю, яка вчиняється за попередньою змовою, є те, що ці діяння періодично вчиняються транснаціонально. Злочинці можуть перебувати в одній країні, а наслідки їхніх дій мають місце в іншій. Це створює юридичні виклики щодо врегулювання юрисдикції та екстрадиції, особливо коли країни мають різні закони та норми щодо визначення міри відповідальності за кіберзлочини.

Окрім цього, існує оперативно-розшукова та кримінально-процесуальна проблема, яка полягає у виявленні, встановленні та фіксуванні кіберзлочинів. Кіберзлочинці використовують різноманітні техніки для приховування своєї діяльності та ідентичності, включаючи використання зашифрованих послуг, анонімних мереж, криптовалюти для фінансових транзакцій та інше.

Держави повинні використовувати свій кримінально-правовий арсенал для розробки стратегій протидії цьому виду злочинності. Це може включати в себе впровадження нових законів, оновлення існуючих норм, зміцнення міжнародного співробітництва та удосконалення оперативно-розшукових і слідчих технік.

Для подальшого зміцнення боротьби з кіберзлочинами, вчиненими за попередньою змовою групою осіб, необхідно посилити міжнародне співробітництво, розвивати та вдосконалювати законодавчу базу, а також збільшувати обізнаність суспільства про цей вид злочинності.

Одним з критичних аспектів кіберзлочинності є її глобальний характер. Це вказує на важливість міжнародного співробітництва в галузі боротьби з кіберзлочинами, як це

було підкреслено в «The Regime Complex for Managing Global Cyber Activities» Nye (2014), де йдеться саме про необхідність визнання кіберпростору як глобального спільного надбання [6, с. 75].

Така співпраця включає в себе обмін інформацією, координацію дій та розробку спільних стратегій для виявлення та відстеження злочинців, що діють в кіберпросторі. Важливим є також розвиток міжнародних норм, що регулюють діяльність в кіберпросторі [7, с. 38].

Незважаючи на складність боротьби з кіберзлочинами, досвід України та Європейського Союзу показує, що розробка ефективних механізмів виявлення, розслідування та притягнення до відповідальності може значною мірою сприяти зменшенню рівня кіберзлочинності.

Останнім часом все більше країн впроваджують в своє законодавство відповідні положення, спрямовані на боротьбу з кіберзлочинами. Це підтверджується документом «The Global War for Internet Governance», де зокрема визначено, що держави все більше визнають необхідність контролю за кіберпростором, який належить до їх території але не мають права втручатися в кіберпростір інших держав [8, с. 118].

Загалом, кіберзлочинність, вчинена за попередньою змовою, є складною та багатогранною проблемою, яка вимагає від держави глибокого розуміння технологій, законів та міжнародного співробітництва. У майбутньому її подолання буде потребувати ще більшої консолідації зусиль на національному та міжнародному рівнях.

В порівнянні із законодавством Європейського Союзу, Кримінальний кодекс України включає статті 361-1, 361-2, 361-3, 361-4, які виписують відповідальність за кіберзлочинність. Однак, на відміну від ЄС, українське законодавство досі не має прямих посилань щодо відповідальності за вчинення кіберзлочинності. Це може бути однією з проблем, які потребують невідкладної уваги.

Для подальшого розвитку в сфері кібербезпеки, особливо в контексті боротьби з кіберзлочинністю, важливе активне співробітництво з міжнародними партнерами, адаптування національного законодавства до міжнародних стандартів та використання найкращих практик.

Однак, незважаючи на наявність науково-юридичного потенціалу, законодавчого арсеналу, практика застосування цих норм в Україні виявляє деякі проблеми. Зокрема, часто виникають труднощі з доказуванням вини осіб, які вчиняють злочини в кіберпросторі, особливо коли вони вчиняються за попередньою змовою групою осіб. Справа в тому, що ці злочини часто характеризуються високим рівнем анонімності та технічної складності, що ускладнює їх розкриття та розслідування.

Більше того, у багатьох випадках злочинці знаходяться за межами України, що робить екстрадицію складною, а іноді неможливою. Це потребує підвищення рівня міжнародного співробітництва та обміну інформацією між правоохоронними органами різних держав.

Зважаючи на ці складнощі, існує велика потреба в подальшому розвитку правового регулювання кіберзлочинів, а також в підвищенні рівня професійної підготовки та технічного оснащення правоохоронних органів. Це може включати проведення спеціалізованих навчальних курсів, збільшення числа спеціалістів в галузі кібербезпеки, розробку нових технологій для виявлення та протидії кіберзлочинності, а також вдосконалення механізмів міжнародного співробітництва в цій сфері.

З кримінологічної точки зору слід підкреслити наступні факти. Вже сьогодні кіберзлочинність постає значним ризиком національної та міжнародної безпеки. Сьогодні жертвами злочинців, що виникають у віртуальному просторі стають не лише люди, а й держави. Застосування однотипних заходів запобігання кіберзлочинності не може бути саме ефективним, адже не досліджено сучасну кримінологічну характеристику цих злочинів, а в ній не виявлено детермінанти [9, с. 57].

Підсумуємо, кіберзлочинність стає все більшою проблемою в сучасному світі, а відповідно до цього зростає потреба в ефективних законодавчих інструментах для боротьби з нею. В Україні вже існують певні законодавчі норми для боротьби з вказаною сферою

протиправної діяльності але вони не в змозі відповідати вимогам сучасного світу, оскільки кіберзлочинність набирає стрімкий курс до поширення та розвитку.

Для подальшого розвитку в сфері кібербезпеки, варто врахувати практику європейських партнерів, зокрема адаптувати національне законодавство до міжнародних стандартів. Це не тільки допоможе покращити стан кібербезпеки в країні але й зробить Україну більш привабливою для міжнародних інвестицій в цифрову сферу.

Крім того, варто зауважити, що лише за умов суворого дотримання законних вимог, проведення системної роботи, провадження на законних підставах комплексних перевірок, реалізації програми протидії злочинам, можливо дійти результату поліпшення ситуації в сфері інформаційної безпеки на яку зокрема постягаються суб'єкти. Впровадження досліджень різних видатних науковців в сфері протидії кіберзлочинам, дозволить виділити в результаті нові профілактичні методи, заходи запобігання та методологію ліквідації останніх [10, с. 203].

Висновки. Таким чином, для досягнення прогресу в цій важливій області, потрібно поєднати зусилля, як на національному, так і на міжнародному рівні. На сьогоднішній день проблематика кіберзлочинності, яка вчиняється за попередньою змовою групою осіб в світлі кримінально-правової науки не є дослідженою на достатньому рівні, а отже становить підґрунтя для подальших наукових розробок. Разом з цим, вказана актуальна проблема потребує комплексного кримінологічного дослідження із виділенням в такому причин та умов злочинності, характеристики особи, яка вчиняє кіберзлочин та заходи спеціально-кримінологічного запобігання.

Список використаних джерел:

1. Бєлєнький В.П., Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України. Академія адвокатури України, Київ – 2016.

2. Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. / В. М. Болгов, Н. М. Гадіон, О. З. Гладун та ін. – К. : Національна академія прокуратури України, 2015. – 202 с.

3. Gercke, M. (2012). *Understanding Cybercrime: A Guide for Developing Countries* (pp. 40-45). ITU.

4. Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 108-112). Cambridge University Press.

5. Droege, C. (2012). *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.* International Review of the Red Cross, 94(886), 122-125.

6. Nye, J. S. (2014). *The Regime Complex for Managing Global Cyber Activities* (p. 75). Global Commission on Internet Governance Paper Series.

7. United Nations General Assembly (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (p. 38). A/70/174.

8. Nardis, L. (2014). *The global war for internet governance*. Yale University Press.

9. Ткаченко, П., & Ковальчук, Д. (2020). Окреслення кримінологічного становлення кіберзлочинності на рівні протидії та запобігання. *Збірник наукових праць ΛΌГОΣ*, 56-60.

10. Ткаченко, П. І., & Кузьменко, А. О. (2019). Детермінація злочинів в сфері економіки та їх запобігання.