УДК 343.6 : 004 (477)
Осінська Дар'я Сергіївна
Осітрова Юлія Олександрівна –
студентки 3 курсу
Інституту підготовки кадрів до органів юстиції України
Національного юридичного університету Імені Ярослава Мудрого

Dariia S. Osinska,
Yuliia O. Ositrova –
3d year students of
Personnel Training Institute for the Bodies of Justice of Ukraine
Yaroslav Mudryi National Law University
(77 Pushkinska Street, Kharkiv, 61024, Ukraine)

Боротьба з кіберзлочинністю на національному та міжнародному рівні

В статті проаналізовано проблемні моменти регламентації та вирішення проблем кіберзлочинності в Україні враховуючи зарубіжний досвід. Вказано на наявність проблемних питань, а саме: відсутність окремого нормативно-правового акту, який би визначав діяльність, функції та спеціальну компетенцію органів внутрішніх справ щодо запобігання кіберзлочинності, закріплення в Законі України «Про основні засади забезпечення кібербезпеки України» положень, які б створювали нормативно-правову базу для захисту населення від інформаційних злочинів.
Ключові слова: *індивідуальна інформація, інформаційний злочин, інформація, кібербезпека, кіберзлочин.*

В статье проанализированы проблемные моменты регламентации и решения проблем киберпреступности в Украине, учитывая зарубежный опыт. Указано на наличие проблемных вопросов, а именно: отсутствие отдельного нормативно-правового акта, который бы определял деятельность, функции и специальную компетенцию органов внутренних дел по предотвращению киберпреступности, закрепления в специальном законе положений, которые бы создавали нормативно-правовую базу для защиты населения от информационных преступлений.
Ключевые слова: *индивидуальная информация, информационный преступление, информация, кибербезопасность, киберпреступлений.*

Yu.O. Ositrova, D.S. Osinska Fighting against Cybercrime at the National and International Levels

The increasing access to and subsequent use of technology has dramatically impacted the way in which people communicate and conduct their daily lives. The internet for example connects people and companies from opposite sides of the world quickly, easily, and relatively cheaply.

However, the internet and computer can be used in negative ways, which can have destructive impact on societies. Cybercrime is a threat against different organisations and people who computers connected to the internet and particularly mobile technology.

Cybercrime can be defined as a type of crime committed by cybercriminals who use a computer as a tool and the internet as a connection in order to reach a variety of objectives such as fraud, illegal downloading of files such as music and films, and spam mailing which is sending a phony e-mail in order to steal private information or access to a protected website (Cross, 2002:2). Cybercrime is a concern that has been attracting media attention since 1945, when the United Nations created an international cooperation and collective security network of 192 countries to cooperate and solve international problems and one of a growing issue is cybercrime (Portnoy and Goodman, 2009).

This article aims to analyze the problem moments of regulation and solving the problems of cybercrime in Ukraine, taking into account foreign experience.

It is pointed out that there are problematic issues, namely: the lack of a separate legal act that would define the activities, functions and special competence of the bodies and departments of internal affairs to prevent cybercrime, fixing in the Law of Ukraine "On the basic principles of ensuring cybersecurity of Ukraine" created a legal framework to protect the public from information crimes, as well as the lack of standards that would establish responsibility for crimes in to protect your personal information, intercept foreign countries sensitive to public and private information.

Keywords: *individual information, information, information crime, cybercrime, cybersecurity.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій, масове використання мережі Інтернет має на сьогоднішній день як переваги, так і недоліки. З кожним роком злочини у сфері ІТ стають однією з прогресуючих груп суспільно небезпечних діянь. Більшість провідних країн світу, таких як США, Китай, Росія, Німеччина, одним із найголовніших завдань протидії злочинності вважають саме боротьбу з кіберзлочинами. Це й не дивно, оскільки щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисячі. Так, Всесвітнє дослідження економічних злочинів та шахрайства 2018 року показує нам, що кіберзлочини входять в топ-п'ятірку економічних злочинів.

Генеральний секретар Організації Об'єднаних Націй Антоніу Гутерріш у травні 2018 року у день відкриття 27-ї сесії Комісії ООН з попередження злочинності та кримінального правосуддя зазначив, що нові технології, створюють нові форми злочинності. Збитки світової економіки від кіберзлочинності оцінюються у 1,5 трлн. дол. на рік. А за негативним сценарієм у 2019 році вони сягатимуть 2 трлн. дол.

Аналіз останніх досліджень та публікацій. Аналізуючи праці науковців у сфері кіберзлочинності, можна дійти висновку, що в нас немає єдиних взаємоузгоджених правил та положень, які регулюють захист інформації від кібервпливу, відповідальність за такі злочини та діяльність органів. Дослідженню цієї проблеми присвячено чимало праць вчених, зокрема С. Буяджи, Б. Головкіна, М. Кравчука, М. Кравцова.

Невирішені раніше проблеми. На даному етапі законодавче регулювання кіберзлочинності в Україні не встигає за розвитком технологій. Це проявляється в недосконалій регламентації питань, які стосуються захисту інформації від кібервпливу. Також існує потреба в доповненні Кримінального кодексу (далі – КК) України нормами, які б встановлювали відповідальність за різні прояви кіберзлочинів. Відсутність єдиного нормативно-правового акту, який визначав би діяльність, функції та спеціальну компетенцію органів і підрозділів внутрішніх справ, загострює проблему інформаційних злочинів. Також невирішеним залишається питання стосовно способів та шляхів міжнародної співпраці як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства. Тому на даний час існує гостра необхідність продовження досліджень у даній сфері.

Метою статті є окреслення найбільш проблемних моментів законодавчої регламентації кіберзлочинності та визначення шляхів їх вирішення, зокрема враховуючи зарубіжний досвід.

Виклад основного матеріалу. У сучасному світі, де розвиток інформаційних технологій з кожним днем набирає обертів, дуже важливим є врегулювання питання інформаційної безпеки в Україні. Належне врегулювання інформаційної безпеки буде слугувати забезпеченню національної безпеки в державі.

Чинним КК України встановлена відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361^1); несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах),

автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362); порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363^1). Тобто можна зробити висновок, що КК України регулює питання, які стосуються комп'ютерного злочину, а не кіберзлочину взагалі. Нерідко ці два поняття ототожнюють, проте, на нашу думку, це помилково, адже поняття «кіберзлочинність» більш точно відображає природу такого явища як злочинність в інформаційному просторі.

На думку В. Олійника, поняття «кіберзлочинність» за своєю суттю набагато ширше за поняття «комп'ютерна злочинність» і включає цілий спектр протиправних діянь. Кіберзлочин – це винне протиправне втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, здійснені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв доступу до модельованого за допомогою комп'ютера інформаційного простору. Відповідно поняття «комп'ютерна злочинність» відноситься до злочинів, вчинюваних проти комп'ютерів або комп'ютерних даних [1, с. 19-22].

Важливим внеском у протидію кіберзлочинності з боку держави стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII. У п. 8 ст. 1 зазначеного закону «кіберзлочин» (комп'ютерний злочин) визначено як 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 [2]. Проте, на нашу думку, цьому закону не вистачає деяких положень, які б підвищили рівень захищеності громадян. Наприклад, забов'язати державні організації посилити рівень захисту інформації від кібервпливу.

Діяльність правоохоронних органів також допомагає в боротьбі з кіберзлочинністю. Так, Міністерство внутрішніх справ України організовує діяльність підрозділів поліції та здійснює низку заходів, спрямованих на запобігання кіберзлочинності відповідно до загальнодержавних програм і планів щодо протидії окремим видам злочинів. Зазначені завдання і функції виконуються не Міністерством внутрішніх справ України загалом, а відповідними підрозділами його центрального апарату. Діяльність цих структурних підрозділів щодо попередження злочинності має суттєві відмінності. Якщо для одних управлінь, служб та підрозділів (які виконують контрольно-дозвільні функції) попередження є супутнім завданням у межах правоохоронної діяльності чи супутнім результатом функціональної діяльності, то для інших – однією із функцій у межах правоохоронної роботи (управління, служби і підрозділи, які безпосередньо проводять боротьбу з загальнокримінальною і організованою злочинністю і для яких її попередження є однією із функцій у межах правоохоронної діяльності поліції), а для третіх – функціональна діяльність включає в себе й попередження (органи, для яких попередження злочинів є процесуально-правовим обов'язком у межах досудового розслідування) [3, с. 119-120].

Необхідно також відзначити значну роль міжнародних договорів у сфері співробітництва боротьби з кіберзлочинністю у кримінальних справах. Наприклад, Угода між Кабінетом Міністрів України і Урядом Турецької Республіки про співробітництво передбачає надання взаємної допомоги в попередженні й розкритті кіберзлочинів. Це означає, що у разі виникнення такої необхідності правоохоронні органи обох держав зобов'язані всебічно та двосторонньо сприяти діяльності один одному [4, с. 203].

Але зважаючи на прогалини в українському законодавстві необхідно звернути увагу на позитивний досвід іноземних держав та міжнародних організацій у досліджуваній сфері,

який можна буде імплементувати в національне законодавство.

ООН уже тривалий час проводить діяльність, пов'язану із правовим врегулюванням ключових питань у сфері боротьби з кіберзлочинністю. Так, починаючи із 1955 року і до цього часу скликається один раз на п'ять років Конгрес ООН з попередження злочинності та поводження з правопорушниками. У 1990 році VIII Конгрес ООН ухвалив резолюцію, де проголошується, що держави-члени ООН повинні збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності [5].

На сьогодні одним із провідних міжнародно-правових актів у сфері боротьби з кіберзлочинністю є Конвенція Ради Європи про кіберзлочинність. Вона спрямована на врегулювання таких основних питань, як кримінально-правова характеристика злочинів щодо комп'ютерної інформації; кримінально-процесуальні аспекти боротьби зі злочинністю, направлені на забезпечення збирання доказів при розслідуванні комп'ютерних злочинів; міжнародна співпраця у кримінально-процесуальній діяльності, направленій на збирання доказів скоєння таких злочинів за кордоном. Також Конвенція називає п'ять видів комп'ютерних злочинів: незаконний доступ; незаконне перехоплення; втручання в дані; втручання в систему; незаконне використання пристроїв [6].

Однією із перших держав, що зайнялась розробкою відповідних нормативно-правових актів у досліджуваній сфері, є США. Так, у 2015 році в Національній стратегії внутрішньої безпеки США був передбачений розділ «Кіберзахист», у змісті якого наголошується на необхідності захисту від кібератак на теренах кіберпростору та проголошено курс на посилення законодавчої бази та підвищення стандартів захисту прав та інтересів громадян.

Важливими проблемами, що постали перед США є саме проведення оперативно-розшукових заходів та покарання порушників закону, збільшення міри відповідальності за вчинення комп'ютерних злочинів і захист прав та інтересів громадян у разі завдання шкоди, посилення відповідальності за порушення у сфері захисту індивідуальної інформації, у тому числі шляхом інсталяції програмного забезпечення для збору індивідуальної інформації, ідентифікації користувача без його відома та згоди.

Головною метою боротьби з кіберзлочинністю у США є захист не лише державних, а й інтересів кожного індивіда. Наприклад, за неналежне зберігання та обробку персональної інформації чи її знищення у відмінний, від встановленого законом спосіб, у США встановлено кримінальну відповідальність. Для порівняння, у країнах Європейського Союзу кримінальні справи можуть заводитися лише у випадку завдання шкоди державній безпеці та основним правам громадян [7, с. 124]. Тобто протиправна діяльність у кіберпросторі США санкціонується значно жорсткіше, ніж у Європі.

Варто також відзначити прогресивний розвиток законодавства Білорусі у досліджуваній сфері. КК Білорусі безперечно сприйняв концепцію комп'ютерної злочинності, майбутні її тенденції, і в цьому відношенні навіть випередив Конвенцію Ради Європи про кіберзлочинність. Так, до КК Білорусі 1999 р. була включена глава 31 «Злочини проти інформаційної безпеки», що містить 7 складів злочинів. 8 листопада 2011 р. був прийнятий Указ Президента Республіки Білорусь № 515 «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», який передбачає створення Ради з розвитку інформаційного суспільства при Президентові Республіки Білорусь, а також затверджує Положення про Раду з розвитку інформаційного суспільства при Президентові Республіки Білорусь. Наявність цих нормативно-правових актів дало змогу підсилити інформаційну безпеку в державі шляхом врегулювання багатьох питань у сфері боротьби із кіберзлочинністю.

Висновки. Підсумовуючи викладене слід зазначити, що кіберзлочин – це протиправне, винне діяння, що здійснюються за допомогою комп'ютера в мережі Інтернет, яке з кожним днем набирає все більше обертів та охоплює весь світ.

Вважаємо за доцільне перейняти досвід США та доповнити КК України новими нормами, які б встановлювали відповідальність за злочини у сфері захисту індивідуальної інформації, перехоплення іноземними державами конфіденційної державної і приватної інформації, а також відкритої інформації, що передається урядовими й комерційними телекомунікаціями, що може завдати шкоди державі або її громадянам.

Наголошуємо на тому, що в Україні окремого нормативно-правового акту, який би визначав діяльність, функції та спеціальну компетенцію органів і підрозділів внутрішніх справ щодо запобігання кіберзлочинності немає. На нашу думку, створення та прийняття такого акту значно б вплинуло на організацію та ефективність такої діяльності.

Проаналізувавши Закон України «Про основні засади забезпечення кібербезпеки України», пропонуємо доповнити його важливими положеннями, які б створювали нормативно-правову базу для захисту населення від інформаційних злочинів.

Вважаємо, що боротьба з кіберзлочинністю на рівні держави є майже безрезультатною, оскільки наші навички да досвід не дають змогу частіше за все знайти злочинця та покарати його. Тому потрібна допомога кожної країни та об'єднання сил проти потужного ворога.

Список використаних джерел:

1. Олійник В. М. Кіберзлочинність як умова порушення громадської безпеки України. *Актуальні питання розслідування кіберзлочинів.* Харків. 2013. Вип. 106. С. 19-22.

2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовт. 2017 р. № 2162-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 06.05.2019 р.).

3. Кравцова М. О. Проблеми правового регулювання запобігання кіберзлочинності органами внутрішніх справ. *Європейські перспективи*. 2014. № 10. С. 118-124.

4. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект: дис. … канд. юрид. наук. Київ, 2018. 203 с.

5. Резолюція Генеральної Асамблеї ООН від 14.01.1990 р. №45/113. URL: http://zakon4.rada.gov.ua/laws/show/995_204 (дата звернення: 20.05.2019 р.).

6. Конвенція про кіберзлочинність: Конвенція Ради Європи від 07 вер. 2005 р. № 2824-IV. URL: http://zakon4.rada.gov.ua/laws/show/994_575 (дата звернення: 20.04.2019 р.).

7. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. *Наукові записки Інституту законодавства Верховної Ради України*. 2013. № 3. С. 123-126.

References:

1. Oliinyk V. M. Kiberzlochynnist yak umova porushennia hromadskoi bezpeky Ukrainy. *Aktualni pytannia rozsliduvannia kiberzlochyniv*. Kharkiv. 2013. Vyp. 106. S. 19-22.

2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovt. 2017 r. № 2162-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (data zvernennia: 06.05.2019 r.).

3. Kravtsova M. O. Problemy pravovoho rehuliuvannia zapobihannia kiberzlochynnosti orhanamy vnutrishnikh sprav. *Yevropeiski perspektyvy*. 2014. № 10. S. 118-124.

4. Buiadzhy S. A. Pravove rehuliuvannia borotby z kiberzlochynnistiu: teoretyko-pravovyi aspekt: dys. … kand. yuryd. nauk. Kyiv, 2018. 203 s.

5. Rezoliutsiia Heneralnoi Asamblei OON vid 14.01.1990 r. №45/113. URL: http://zakon4.rada.gov.ua/laws/show/995_204 (data zvernennia: 20.05.2019 r.).

6. Konventsiia pro kiberzlochynnist: Konventsiia Rady Yevropy vid 07 ver. 2005 r. № 2824-IV. URL: http://zakon4.rada.gov.ua/laws/show/994_575 (data zvernennia: 20.04.2019 r.).

7. Kravchuk M. M. Mizhnarodnyi dosvid pravovoho rehuliuvannia zakhystu personalnykh danykh v merezhi Internet. *Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy*. 2013. № 3. S. 123-126.