УДК 341.4
DOI https://doi.org/10.51989/NUL.2021.4.27

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АСПЕКТ

Якимчук Мирослава Юріївна,
кандидат педагогічних наук,
доцент кафедри спеціальних юридичних дисциплін
Національного університету водного господарства та природокористування

У статті розглянуто основні аспекти правового регулювання кіберзлочинності в національному праві через призму міжнародного. Проаналізовано визначення поняття «кіберзлочинність», його історичний розвиток. Дослідження наукових студій дало змогу уточнити визначення поняття «міжнародна кіберзлочинність», яке ми будемо розуміти як протиправну поведінку міжнародного значення, яка здійснена за допомогою комп'ютерної техніки задля несанкціонованого отримання інформації. У статті згадано і проаналізовано резонансний приклад кібератаки, якого названо вірусом «Petya». У сучасному світі країни розробляють нові методи боротьби з такими злочинами, зокрема зазначено, що США сформувала так звані «NIST Cyber security Framework» – стандарти з безпеки, які дозволяють виявляти, реагувати і навіть запобігати кіберзлочинам; Каліфорнія випустила Акт про повідомлення щодо порушення правил безпеки «Notice of Security Breach Act», згідно з яким компанії мають право вільно вибрати для себе спосіб забезпечення приватності своїх систем; Європейський Союз прийняв Директиву щодо мережевої та інформаційної безпеки «NIS Directive on security of network and information systems», що визначив важливе значення надійності й безпеки мережевих та інформаційних систем для економічної та суспільної діяльності; Україна створила підрозділ «CERT-UA», який у межах своїх повноважень проводить аналіз та накопичення даних про кіберінциденти, веде державний їх реєстр. Узагальнюючи все проаналізоване вище, ми зробили висновки, що в сучасному світі існує багато видів кіберзлочинів: комп'ютерне шпигування, поширювання комп'ютерних вірусів, інтернет-шахрайство, дефейс, кібертероризм тощо – ці злочини можуть мати більш масштабний об'єм і загрожувати міждержавній безпеці. У статті згадано і виокремлено умовні групи злочинів проти приватності, цілісності інформаційних даних, за Конвенцією про кіберзлочинність. Аналіз наукової літератури дав можливість констатувати, що кіберзлочинність дійсно є актуальною проблемою сучасності, проте світове співтовариство спрямувало свої сили на її розв'язання через прийняття відповідних документів.

Ключові слова: *кіберзлочин, міжнародна кіберзлочинність, несанкціоноване отримання інформації, інформаційна безпека, кіберінцидент, веб-сайт, кіберправо, міжнародний злочин.*

Yakymchuk Myroslava. Special aspects of the legal regulation of combating cybercrime in Ukraine: comparative and legal aspect

The article considers the main aspects of legal regulation of cybercrime in national law through the prism of international law. The definition of the concept of "cybercrime", its historical development is analyzed. Research has made it possible to clarify the definition of "international cybercrime", which we will understand as illegal behavior of international importance, which is committed with the help of computer technology to obtain unauthorized information. The article mentions and analyzes a resonant example of a cyber attack called the "Petya" virus. In today's world, countries are developing new methods to combat such crimes, including that the United States has developed the so-called "NIST Cyber security Framework" – security standards that can detect, respond to and even prevent cybercrime; California has issued a Notice of Security Breach Act, which allows companies to freely choose how to ensure the privacy of their systems; The European Union has adopted the NIS Directive on the security of network and information systems, which defines the importance of the reliability and security of network and information systems for economic and social activities; Ukraine has established a CERT-UA division, which, within its powers, analyzes and collects data on cyber incidents and maintains a state register of them. Summarizing all the above, we concluded that in today's world there are many types

of cybercrime: computer espionage, the spread of computer viruses, Internet fraud, interface, cyber terrorism, etc. – these crimes can be large-scale and threaten interstate security. The article mentions and identifies conditional groups of crimes against privacy, integrity of information data, under the Convention on Cybercrime. An analysis of the scientific literature has made it possible to state that cybercrime is indeed an urgent problem of our time, but the world community has focused its efforts on solving it through the adoption of relevant documents.

Key words: *cybercrime, international cybercrime, unauthorized receipt of information, information security, cyber incident, website, cyber law, international crime.*

Прогрес суспільства у сфері інформації, безумовно, надає країнам великі переваги в багатьох сферах суспільного життя, однак це тягне за собою не лише позитивні наслідки, адже чим швидше розвивається інформаційна сфера, тим більше виникає різноаспектних проблем, зокрема правопорушень у галузі інформаційно-комунікаційних технологій. Такі злочини відбуваються не лише на локальному рівні, а й на світовому, що спричиняють загрозу міжнародній інформаційній безпеці. Зауважимо, що жодна держава не може боротися із цією проблемою самостійно, тому виникає потреба в міжнародній співпраці з питань кібербезпеки.

Ця проблема перебуває в центрі уваги, адже щороку кіберзлочинність завдає державам та приватним особам дуже великої шкоди. На 73-й сесії Генеральної асамблеї ООН генеральний секретар А. Гуттереш оцінив щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів [4].

Мета роботи – дослідити міжнародну співпрацю в галузі боротьби з кіберзлочинністю.

Натепер питання правового регулювання кіберзлочинності є актуальним, тому й стало об’єктом дослідження таких вітчизняних і зарубіжних науковців, як М. Ануфрієва, Н. Ахраменко, Д. Біленчук, В. Бреннер, В. Голубев, О. Литвинов, В. Максимов, Б. Романюк, А. Юрасов, М. Якимчук, М. Яцишин та ін.

Цікавим для нашого дослідження є той факт, що перший злочин з використанням комп’ютера відбувся у 1983 році в США, так з’явився новий тип злочинів – інформаційні злочини, або ж кіберзлочини.

Початок XXI ст. характеризується стрімким розвитком науково-технічної сфери суспільства, що поряд із полегшенням життя особи в аспектах доступу до інформації, спілкування, проведення банківських операцій тощо призвело до неконтрольованого зростання масштабів кіберзлочинності.

Резонансним прикладом кібератаки є вірус «Petya» (27 червня 2017 р.), який зашифровує дані на комп’ютері та вимагає 300 доларів у такій цифровій валюті, як біткоїни, причому ця сума не допоможе відновити доступ, адже електронна адреса, на яку зловмисники просять відправити інформацію після здійснення платежу, блокується провайдером. Він вразив енергетичні компанії України, банки, аеропорт Харкова, урядові сайти, київський метрополітен, а згодом і розповсюдився на російські банки. Як зазначає Укрінформ [8], цей вірус поширився на Італію, Ізраїль, Сербію, Угорщину, Румунію, Польщу, Німеччину, Велику Британію, США, Францію та деякі інші країни. США звинуватили Росію в атаці вірусу «Petya» і пообіцяли розібратися в цьому.

Зауважимо, що кіберзлочинність набула широкого розповсюдження порівняно недавно, проте вона перетворилась на одну з найбільших міжнародних загроз. Кожного року злочинів у сфері кіберзлочинності стає все більше, що й зумовило потребу в утворенні міжнародно-правового співробітництва в цій галузі. З огляду на те що кіберзлочини є новим видом злочинів у міжнародному праві, науковці розділилися щодо характеристики їх понять.

Є. Скулиш, спираючись на висновки, зроблені на десятому конгресі ООН, визначає кіберзлочин у двох аспектах:

– у вузькому значенні: будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є безпека комп’ютерних систем і оброблюваних ними даних;

– у широкому розумінні (як злочин, пов’язаний з комп’ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов’язане з комп’ютерами, комп’ютерними системами або мережами,

включаючи незаконне володіння і пропозицію або розповсюдження інформації за допомогою комп'ютерних систем або мереж [7, с. 49].

В. Голубєв наголошує, що кіберзлочинність – це протиправна поведінка, яка спрямована на порушення відносин у суспільстві та приватної чи корпоративної безпеки під час того, як особи обмінюються інформацією за допомогою електронних пристроїв [2].

Сюзан В. Бреннер поділяє кіберзлочини за роллю комп'ютера в їх вчиненні: ті, в яких він є кінцевою ціллю; ті, в яких він діє як засіб; ті, в яких він грає незначну роль у вчиненні [3].

Закон України «Про основні засади забезпечення кібербезпеки України» визначає кіберзлочин (комп'ютерний злочин) як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [6].

А. Юрасов визначає, що кіберзлочинність – це злочинність, де комп'ютерна техніка є знаряддям та способом учинення протиправних діянь проти власності, немайнових та майнових прав та безпеки громадськості [10].

П. Біленчук доводить, що кіберзлочинність – це злочини, які здійснюються за допомогою комп'ютерних та інформаційних мереж, наслідком яких є незаконне отримання інформації [1].

Аналіз наукових студій дав можливість нам уточнити дефініцію поняття *«міжнародна кіберзлочинність», яке ми будемо розуміти як протиправну поведінку міжнародного значення, яка здійснена за допомогою комп'ютерної техніки задля несанкціонованого отримання інформації.*

На сучасному етапі деякі країни розробили дієві методи боротьби з кіберзлочинністю. США сформувала так звані «NIST Cyber security Framework» – стандарти з безпеки, які дозволяють виявляти, реагувати і навіть запобігати кіберзлочинам. Каліфорнія випустила Акт про повідомлення щодо порушення правил безпеки «Notice of Security Breach Act», згідно з яким компанії мають право вільно вибрати для себе спосіб забезпечення приватності своїх систем.

Зазначимо, що ЄС прийняв Директиву щодо мережевої та інформаційної безпеки «NIS Directive on security of network and information systems», що визначила важливе значення надійності та безпеки мережевих та інформаційних систем для економічної та суспільної діяльності, зокрема для функціонування внутрішнього ринку, та заснував для всіх держав, які підтримали дану Директиву, комп'ютерні групи реагування на надзвичайні ситуації «CERT» [3].

Цікавим для нашого дослідження є той факт, що Україна на основі цієї практики створила підрозділ «CERT-UA», який у межах своїх повноважень проводить аналіз та накопичення даних про кіберінциденти, веде державний їх реєстр; надає власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів; організовує та проводить практичні семінари з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту; розміщує на своєму офіційному веб-сайті рекомендації щодо протидії сучасним видам кібератак та кіберзагроз; взаємодіє з правоохоронними органами, забезпечує їх своєчасне інформування про кібератаки. CERT-UA діє передусім на основі Закону України «Про основні засади забезпечення кібербезпеки України», що у свою чергу встановлює основні принципи кібербезпеки, її об'єктів та суб'єктів, національну систему кібербезпеки, межі міжнародного співробітництва, фінансування, відповідальність, державно-приватну взаємодію у сфері кібербезпеки та деякі інші основні положення [6].

Варто також виокремити положення, прописані в Конвенції про кіберзлочинність, що ратифікована Верховною Радою, де передбачено відповідальність за такі види кіберзлочинів, як: незаконний доступ до інформації, нелегальне перехоплення інформації, втручання в дані, втручання в систему, зловживання пристроями, підробка, пов'язана з комп'ютерами, шахрайство, пов'язане з комп'ютерами, правопорушення, пов'язані з дитячою порнографією, та правопорушення,

пов'язані з порушенням авторських та суміжних прав [5].

Незважаючи на такий об'єм структур та нормативно-правових актів, В. Цимбалюк [9, с. 33] підкреслює, що будь-які спроби держав ЄС здійснювати заходи міждержавного чи наддержавного обмеження прояву свободи в електронному сегменті телекомунікації неминуче зустрічали активний суспільний спротив під гаслами протидії посяганням на право кожного поширювати, отримувати, шукати інформацію будь-якими засобами, незалежно від кордонів держав. Науковець убачає цю проблему в недостатній кодифікації кіберправа, а у своєму авторефераті зазначає, що саме формування узгоджених як стандартів інституційних ознак законодавства про інформацію в окремих країнах на науковому рівні дозволить вирішити проблеми міжнародного співтовариства щодо синхронізації та спеціалізації правового регулювання у глобальній інформаційний сфері суспільства і в комплексі вирішувати проблеми міжнародного співробітництва держав в умовах формування нового етапу глобального інформаційного суспільства – глобальної кіберцивілізації.

Зазначимо, що в сучасному світі існує багато видів кіберзлочинів, які найбільше можуть завдати шкоди: комп'ютерне шпигування, поширювання комп'ютерних вірусів, інтернет-шахрайство, дефейс, кібертероризм тощо. На нашу думку, найгірше те, що ці злочини можуть мати більш масштабний об'єм і загрожувати міждержавній безпеці. Зауважимо, що саме цей факт сприяв налагодженню міжнародної співпраці в цій сфері. Натепер багато міжнародних організацій, таких як ООН, Група 8, Рада Європи, Інтерпол, Організація економічного співробітництва і розвитку, зайнялись створенням нормативно-правової бази для початку співпраці у сфері кібербезпеки.

Варто зазначити, що в 1995 р. відбулася І Міжнародна конференція Інтерполу з кіберзлочинності. Цікавим є той факт, що в 1996 р. країни G8 прийняли рішення про започаткування певної групи з протидії міжнародним злочинам у сфері комп'ютерних технологій. Також у кожній країні було створено контактний центр для боротьби з інформаційними злочинцями, який працював цілодобово.

У 2001 р. було прийнято в рамках ООН Резолюцію «Щодо боротьби зі злочинним використанням інформаційних технологій», де зазначено про співробітництво державного і приватного сектору в боротьбі з кіберзлочинами; про введення відповідальності за інформаційні правопорушення, міжнародну співпрацю правоохоронних органів, захист від незаконного втручання в комп'ютерні системи тощо.

Зазначимо, що в 2001 р. в Будапешті було прийнято найголовніший правовий акт, що регулює питання співробітництва держав у галузі протидії кіберзлочинам – Конвенцію про кіберзлочинність.

За Конвенцією можна визначити такі умовні групи злочинів проти приватності, цілісності інформаційних даних:

– правопорушення в галузі несанкціонованого доступу до даних: незаконне перехоплення (ст. 3), пошкодження пристроїв (ст. 6);

– злочини, пов'язані з протиправним використанням комп'ютерів: підроблення, пов'язане з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8);

– злочини, пов'язані зі змістом, до яких відноситься створення, розповсюдження та зберігання дитячої порнографії (ст. 9);

– злочини, пов'язані з порушенням авторських та суміжних прав (ст. 10) [5].

У 2009 р. було ухвалено Угоду про співробітництво у сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва, а в 2014 році підписано Конвенцію про кібербезпеку і захист персональних даних Африканського Союзу.

Аналіз наукової літератури дав можливість нам констатувати, що з початком розвитку комп'ютерних та інформаційних технологій з'являється поняття «кіберзлочинність». На нашу думку, саме кодифікація інформаційного законодавства на міжнародному рівні дозволить систематизувати всі ті здобутки у вигляді прийнятих конвенцій, директив, законодавчих актів міжнародної спільноти та внутрішніх нормативів окремих держав і зможе вигідно й перспективно регулювати відносини в інформаційному просторі та створити

ефективне вдосконалення правової бази боротьби з кіберзлочинністю.

Отже, кіберзлочинність дійсно є актуальною проблемою сучасності, світове співтовариство спрямувало свої сили на її розв'язання через прийняття відповідних документів. Їхня мета – перетворити новий і в деяких аспектах невідомий міжнародний інформаційний простір на структурований, зрозумілий та підкорити його відповідним законам конфіденційності та достовірності інформації, збереження авторських прав, захист від шахрайства й інші актуальні на сучасному етапі проблеми.

Проведене дослідження не претендує на остаточне розв'язання всіх аспектів вибраної проблеми. Перспектива подальшого дослідження може бути спрямована на вивчення та аналіз можливих шляхів кодифікації кіберправа.

ЛІТЕРАТУРА:

1. Біленчук Д.П. Кібершахраї – хто вони? *Міліція України*. 1999. № 7–8. С. 32–34.

2. Голубев В.А. «Кибертерроризм» – миф или реальность? URL: //www.crime-research.org

3. Директива Європейського Парламенту і Ради (ЄС) про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзувід 6 липня 2016 року. URL: https://zakon.rada.gov.ua/ laws/show/984_013-16#Text

4. Кібербезпека: вразливі моменти. URL: https://yur-gazeta.com/ publications/practice/ inshe/kiberbezpeka-vrazlivi-momenti.html

5. Конвенція про кіберзлочинність від 23.11.2001 р. URL: http://zakon.rada.gov.ua/laws/ show/994_575

6. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 р. №2163-VIII. URL: http://search.ligazakon. ua/l_doc2.nsf/link1/T172163.html

7. Скулиш Є. Теоретико-методологічні засади визначення об'єкта та предмета кіберзлочинів. *Правова інформатика.* 2014. № 2 (42) С. 47–53.

8. Укрінформ «Вірус Petya». URL:https://www.ukrinform.ua/tag-virus-petya

9. Цимбалюк В. Кодифікація інформаційного законодавства України : автореф. дис. ... на здобуття наукового ступеня доктора юридичних наук. 12.00.07. Харків, 2013. 45 с.

10. Юрасов А.В. Основы электронной коммерции : учебник. Москва : Горячая линия-Телеком, 2008. 480 с.

11. Brenner S. Cybercrime: criminal threats from cyberspace. 2006. 281 p. URL: https://books.google.com.ua/books?id=gsWQxgbLbUC&pg=PA39&hl=uk&source=gbs_toc_r&cad=4#v=onepage&q&f=false