УДК 343.85
DOI https://doi.org/10.24144/2788-6018.2023.01.76

ІСТОРИКО-ПРАВОВІ АСПЕКТИ ВИНИКНЕННЯ ЗЛОЧИННОСТІ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Бодунова О.М.,
кандидат юридичних наук, доцент
завідувач кафедри правничої лінгвістики
Державного податкового університету,
ORCID ID: 0000-0001-9179-5985

Бодунова О.М. Історико-правові аспекти виникнення злочинності у сфері інформаційних технологій.

У статті досліджено історію виникнення кіберзлочинності. Зазначено, що на сьогодні важливим напрямом суспільної діяльності є інформатизація всіх державних і недержавних структур. Інтернет-технології активно впроваджуються у всі сфери людської діяльності, у повсякденне життя кожного українця. За їх допомогою виникає «інформаційне суспільство», суттєво перетворюються всі сфери, як виробництва і технологій, так і соціальних, економічних відносин, духовне життя людства тощо.

Інтернет-технології стали поширеним способом вчинення кримінальних правопорушень. Кількість так званих «комп'ютерних кримінальних правопорушень» зростає кожного дня. І на сьогодні, в умовах воєнного стану інформаційні технології є одним із основних способів реалізації кримінально протиправної мотивації.

Кіберзлочинність, порівняно з традиційними видами злочинності в Україні (вбивства, корисливі кримінальні правопорушення тощо), є відносно новим явищем і найбільшою загрозою XXI століття водночас, адже інформаційні технології також є способом вчинення багатьох традиційних кримінальних правопорушень.

Зроблено висновок, що хоча злочинність у сфері інформаційних технологій є відносно новим видом злочинності, вона завдає значної матеріальної шкоди, і з моменту свого виникнення пройшла 5 етапів розвитку: 1) поява такого явища як злочинність у сфері інформаційних технологій та формування ідей та субкультури хакерів; 2) становлення злочинності у сфері інформаційних технологій як міжнародного виду злочинності; виникнення злочинних угрупувань хакерів, які спеціалізуються на вчиненні кримінальних правопорушень у різних країнах; 3) злочинність у сфері інформаційних технологій стає транснаціональною; 4) використання мережі Інтернет для досягнення політичної мети, поява а також використання кібератак проти урядів окремих держав; 5) активне використання інформаційних технологій під час війни, що супроводжується широким залученням засобів масової інформації задля дезінформації населення, поширенні кібершахрайства та кібертероризму.

Ключові слова: кіберзлочинність, злочинність у сфері інформаційних технологій, генеза, запобігання, кримінальні правопорушення

Bodunova O.M. Historical and legal aspects of the emergence of crime in the field of information technologies.

The article examines the emergence of the history of cybercrime. It is noted that today the industrial direction of public activity is the informatization of all state and non-state structures. Internet technologies are actively being implemented in all spheres of human activity, in the everyday life of every Ukrainian. With their help, the «information society» is created, all spheres, such as production and technology, as well as social and economic relations, the spiritual life of mankind, etc., are significantly transformed.

Internet technologies have become an advanced way of committing criminal offenses. The number of so-called «computer criminal offenses» is increasing every day. Even today, in the conditions of martial law, information technologies are one of the main ways of implementing criminal and illegal motivation.

Cybercrime, according to the traditional types of crime in Ukraine (murder, use of criminal offenses, etc.), is a relatively new phenomenon and the biggest threat of the 21st century at the same time, because information technologies are also a way of committing many traditional criminal offenses.

It was concluded that although crime in the field of information technologies is a fairly new type of crime, it causes significant material damage, and since its inception there have been 5 stages of development: 1) the manifestation of such a phenomenon as crime in the field of information technologies and the formation of ideas and a hacker subculture; 2) the development of crime in the field of information technology as a type of international crime; the emergence of criminal groups of hackers who specialize in committing criminal offenses in different countries; 3) crime in the field of information technologies becomes

transnational; 4) the use of the Internet to achieve a political goal, the appearance and use of cyber attacks against the governments of individual states; 5) active use of information technologies during the war, accompanied by widespread involvement of mass media for disinformation of the population, expansion of cyber fraud and cyber terrorism.

Key words: cybercrime, crime in the field of information technologies, genesis, prevention, criminal offenses.

Постановка проблеми. На сьогодні важливим напрямом суспільної діяльності є інформатизація всіх державних і недержавних структур. Інтернет-технології активно впроваджуються у всі сфери людської діяльності, у повсякденне життя кожного українця. За їх допомогою виникає «інформаційне суспільство», суттєво перетворюються всі сфери, як виробництва і технологій, так і соціальних, економічних відносин, духовне життя людства тощо.

Окрім цього, інтернет-технології стали поширеним способом вчинення кримінальних правопорушень. Кількість так званих «комп'ютерних кримінальних правопорушень» зростає кожного дня. Так, починаючи з 2018 року працівники Національної поліції України були залучені до більше ніж одинадцяти тисяч кримінальних проваджень, пов'язаних з кримінальними правопорушеннями у сфері новітніх інформаційних технологій. Найбільша кількість протиправних діянь вчиняється в Києві, на території Одеської, Миколаївської та Львівської областей [1]. І на сьогодні, в умовах воєнного стану інформаційні технології є одним із основних способів реалізації кримінально протиправної мотивації.

Серез кримінологів побутує думка про те, що злочинність у сфері інформаційних технологій – явище досить нове. Проте через поширеність і суспільну небезпечність вказаного виду злочинності необхідно дослідити його витоки для можливості аналізу дій злочинців у майбутньому.

Стан опрацювання цієї проблематики. Історичні витоки та причини злочинності у сфері інформаційних технологій, формування системи запобігання цьому виду злочинності науковці почали досліджувати відносно недавно. До таких вчених можна віднести О.С. Алавердова, Ю.М. Батуріна, П.Д. Біленчука, А.В. Войцехівського, М.Д. Діхтяренка, К.Ю. Ісмайлова, С.М. Круля, Є.Д. Скулиша, Т.Л. Тропіної, Б.Х. Толеубекова та ін. Проте на сьогодні не є достатньо дослідженими питання щодо історії становлення вказаного виду злочинності, і, на нашу думку, це питання є важливим і актуальним, оскільки вивчення причин і умов розповсюдження інтернет-злочинності дасть змогу сформувати цілісну і ефективну систему запобігання їх вчиненню.

Метою статті є дослідження та аналіз наукових працю щодо виникнення та поширення злочинності у сфері інформаційних технологій, формування заходів запобігання цим кримінальним правопорушенням задля удосконалення існуючої системи попередження злочинності в Україні.

Виклад основного матеріалу. Як ми уже відмічали, з появою та розповсюдженням інформаційних технологій у всі сфери життя суспільства почала розвиватись й кіберзлочинність. Щодня злочинці, використовуючи інформаційні технології в кримінально протиправних цілях, вчиняють все більшу кількість кримінальних правопорушень, ідучи на «крок вперед» працівників правоохоронних органів. Необхідність оновлення системи запобігання злочинності у сфері інформаційних технологій спонукає до якнайшвидшого пошуку найкращого шляху для її вдосконалення, який має включати в себе створення відповідних комп'ютерних систем і технологій, з високим рівнем безпеки в мережі та відповідної нормативно-правової бази, яка буде регулювати сповна це питання та встановлювати належну міру покарання за вчинення кримінальних правопорушень даного виду.

Варто зазначити, що кіберзлочинність, порівняно з традиційними видами злочинності в Україні (вбивства, корисливі кримінальні правопорушення тощо), є відносно новим явищем і найбільшою загрозою XXI століття водночас, адже інформаційні технології також є способом вчинення багатьох традиційних кримінальних правопорушень. Злочинці використовують інтернет-технології через їх основні характеристики: глобальність, анонімність користувачів, охоплення різної за віком та географічним положенням аудиторії. Саме це дає можливість особам отримати кримінально протиправний результат та уникнути відповідальності.

Становлення та розвиток кіберзлочинності не можна відокремлювати від інформаційної революції, тому початком її відліку доцільно вважати шістдесяті роки минулого століття. Саме у 1962 р. професор Джон Лікрайдер, опублікував свою концепцію розповсюдженої комп'ютерної мережі «Galactic Network» [2, с. 304].

Головним припущенням даної концепції було те, що в майбутньому з'явиться глобальна мережа, приєднатися до якої зможе кожен бажаючий, а також у тому, що дана мережа у своїй діяльності може об'єднувати усі комп'ютерні системи світу. Окрім загальної думки вчений детально охарактеризував принципи глобальної мережі, які стали основоположними для мережі Інтернет [3].

Оскільки така ідея та її втілення були новим та надзвичайно цікавим процесом, який міг спростити життя мільйонів людей по всьому світі, то результат не змусив себе чекати: скоро з'явилась перша мережа комп'ютерів ARPANet (Advanced Research Projects Agency Network), створена на

замовлення Міністерства оборони США. Головна мета цієї розробки полягала у тому, щоб створити розподілену систему, яка б не мала чіткого центру, і складалася б з взаємозамінних частин. Спочатку ARPANet мала у складі чотири комп'ютери, розташованих у великих дослідницьких центрах. Головним завдання мережі була передача інформації та електронне листування, тому жодні серйозні елементи, що обмежували б доступ, в її структурі не існували, оскільки тоді ніхто навіть і не припускав появи злочинців у мережі. Цей недолік надалі успадкує і мережа Інтернет, що в подальшому призведе до явища «анархізм». Непродуманість аспектів безпеки і юридичного контролю при розробці технічних принципів мережі, у майбутньому буде наслідком широкого розповсюдження кіберзлочинності.

Що стосується розвитку злочинності у сфері інформаційних технологій, то її витоки розпочинаються з кінця XX століття. Так, у 1970-х роках з'являються перші комп'ютерні злочинці, яких почали називати «хакерами». Хто ж точно був першим хакером, сказати важко, проте у переважній більшості літературних джерел про хакерів та для хакерів, як першого професійного кіберзлочинця згадують Джона Дрейпера, який також проводив першу спеціалізацію хакерів, - фрікери (phreaker), скорочене від телефонний хакер (phone haker). У рядах фрікерів того часу були усім відомі Стів Возняк та Стів Джобс, які в майбутньому стали засновниками «Apple Computers». Саме вони налагодили виробництво пристроїв для злому мереж у домашніх умовах. І цей час доцільно вважати початком розвитку кіберзлочинності [4, с. 296].

У 1983 році у США, а саме у штаті Мілуокі було проведено перший арешт Інтернет-злочинця, про який відразу повідомили громадськості. Безпосереднім приводом для цього був перший зареєстрований Інтернет-злом, який був вчинений групою підлітків із шести осіб, які називали себе «група 414» (414 – міжміський телефонний код штату Мілуокі). Ними було зламано 60 комп'ютерів протягом дев'яти днів, серед зламаних були комп'ютери Лос-Аламоської державної лабораторії. Один з членів групи після проведеного арешту, дав показання і інші її учасники отримали умовний термін відбування покарання [5].

Загалом у 80-х роках прослідковується значне збільшення кількості комп'ютерних атак. Якщо в 1988 р. було тільки шість звернень із даного приводу до центру Інтернет-безпеки CERT, який почав діяти у 1988 р., то в 1989 р. число звернень налічувало 132, а в 1990 – вже 252 [6, с. 118]. Злочинність з використання інформаційних технологій стає досить поширеним явищем, злочинці консолідуються у великі групи і мережа Інтернет стає ресурсом для вчинення різних кримінальних правопорушень. Кримінологи характеризують цей процес як другий етап розвитку кіберзлочинності, для якого характерною є поява нових спеціалізацій Інтернет-злочинців.

У 1984 р. Фред Коен опублікував повідомлення про відкриття перших шкідливих комп'ютерних програм, які здатні до саморозмноження, і визначив їх терміном «комп'ютерний вірус». Також він створив програму, яка ілюструвала спосіб зараження одного комп'ютера іншим [7, с. 320-324].

У 1986 р. в США прийнято перший комп'ютерний закон «The Computer Fraud and Abuse Act», який забороняв незареєстрований доступ до будь-якої комп'ютерної системи [8]. Особливістю даного закону був захист трьох видів несекретної інформації, а саме:

- інформації, що належить фінансовим установам (інформація щодо кредитних карток або ж особистих рахунків);
- інформації, що належить урядовим установам;
- інформації, що належить міжнародним або міжштатним організаціям [8].

Також цей нормативно-правовий акт передбачав відповідальність за пошкодження даних, зокрема, шляхом розповсюдження шкідливих програм.

Цікаво, що у цьому ж році було заарештовано члена групи «Legion of Doom» Лойда Бланкеншипа, відомого під псевдонімом «The Mentor», який написав знаменитий «Маніфест хакера», – «The Haker Manifesto». Висловлені у даному документі ідеї, навіть до сьогодні вважаються фундаментом хакерської ідеології та культури, а також зазнали чималої популярності в мережі Інтернет. Так, збільшення кількості комп'ютерних кримінальних правопорушень пов'язано зі поширенням кримінально протиправних ідей у цій сфері.

У 1994 р. світ дізнався про так звану «справу Володимира Льовіна», яку міжнародною кримінальною поліцією було віднесено до категорії «транснаціональний мережевий комп'ютерний злочин». Міжнародна організована злочинна група, що складалася з 12 людей, використовуючи мережу Інтернет та мережу передачі даних «Спрінт/Теленет», подолала захист від незареєстрованого доступу, намагалася здійснити 40 грошових переказів, загальна сума яких становить 10 млн. 700 тис. 952 долари США з особистих рахунків клієнтів банку, які знаходяться в 9 країнах світу, на інші рахунки, зареєстровані у США, Фінляндії, Ізраїлі, Швейцарії, Німеччині, Нідерландах [8, с. 18]. Варто зазначити, що це перший кіберзлочин, про який стало відомо суспільству. Саме з цього періоду стало зрозуміло, що такі протиправні дії можуть завдавати великої матеріальної шкоди.

У 1998 р. 12-річний хакер зламав комп'ютерну систему, яка координувала водоспуск дамби Теодора Рузвельта в Арізоні. Небезпека його злодіянь полягала у тому, що у разі відкриття зливних

воріт дамби вода могла б затопити міста Темп і Месе, загальна чисельність населення яких нараховувала близько 1 млн. жителів. Оцінка даного діяння стала підґрунтям для появи таких термінів як «Інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм». До того ж, це вказало на те, що найбільш уразливою до кібератак є сама мережа Інтернет, адже усі її ключові елементи доступні з будь-якої точки світу [9].

Відмітимо, що у цей час кібертероризм і кібершахрайство набувають транснаціонального характеру, адже ці кримінальні правопорушення починають вчинятися злочинними угрупуваннями, зокрема, тими, що мають міжнародний характер. Небезпечним фактором стало і те, що з розвитком мережі серйозні наслідки могли наступати не тільки у разі умисних кібератак, а й через некомпетентність або ж необережність спеціалістів. Так, у 1997 р. помилка співробітника «Network solutions» стала наслідком того, що сайти, назви яких мали в закінченні «.net» та «.com» стали недоступними. Що свідчить про те, що збій в роботі усієї глобальної мережі стався через неуважність однієї людини [9].

Окрім цього, новою загрозою кібератак стало широке використання їх у політичній сфері. Розповсюдженими були випадки, коли певний перелік осіб одночасно заходить на відповідний сайт, відправляє електронні листи, пише у форумах з метою обмежити або припинити доступ на сайт іншим користувачам. У результаті це призводить до обмеження відвідування цього веб-сайту або взагалі зупинки його роботи.

Вперше акцію подібного типу здійснила група, що має назву «Strano Network», яка протестувала проти політики французького уряду щодо питань ядерних програм та й в соціальній сфері. 21 грудня 1995 року дана організована група протягом години здійснювала кібертерористичні дії проти сайтів урядових агентств. При цьому учасники атаки діяли з різних куточків світу за єдиною вказівкою: їм потрібно було за допомогою мережі Інтернет одночасно зайти на урядові сайти, після чого деякі з них дійсно були виведені з робочого стану [9, с. 132–137].

З часом кіберзлочинність переросла у транснаціональну. Першою Інтернет-війною вважається конфлікт у Косово, в якій групи користувачів комп'ютерної мережі використовували інформаційні технології для критики бойових дій в Югославії та НАТО, свідомо порушуючи при цьому роботу автоматизованих мереж, електронно-обчислювальних машин, внаслідок чого отримуючи доступ до сайтів, надалі з метою змінити вміст. Разом з тим, в мережі інтернет активно обговорювалися негативні сторони інформаційної війни.

Слід згадати, що на сьогодні практично будь-який політичний або збройний конфлікт йде поряд з організованою протидією у мережі Інтернет. Зокрема, у 2005 р. пройшов ряд кібератак, приводом для яких був шкільний підручник історії, який був виданий в Японії, та у своєму змісті змінював зміст подій в Китаї в 1930-1940-х рр. XX ст. Якщо детально, то в ньому «замовчувалися» військові кримінальні правопорушення японських військ під час вторгнення [10]. Такі кібератаки здійснювалися на веб-сайти державних органів, органів місцевого самоврядування, а також великих підприємств. Вони були синхронними, що свідчить про надзвичайну майстерність злочинців. Науковці припускали, що такі атаки були організовані саме для досягнення політичних цілей.

Не винятком є й Україна. Про використання в умовах воєнних дій інформаційних технологій у кримінально протиправних цілях російською федерацією відомо вже давно. Така діяльність посилилась у зв'язку з повномасштабним вторгненням країни-агресора на територію України. Використання фейкових профілів у соцмережах, втручання у діяльність урядових порталів, сайтів державних органів, поширення російської пропаганди та агресії росії проти України – це не весь перелік кримінальних правопорушень у сфері інформаційних технологій, які вчиняє дана держава. За даними американського видання «Вашингтон пост», ще у 2014 російська військова розвідка створила більше 30 псевдо-українських груп і акаунтів у соціальних мережах, а також 25 «провідних англомовних» видань. Видаючи себе за пересічних українців, працівники ГРУ вигадували новини та поширювали коментарі, щоб налаштувати проросійських громадян проти протестувальників [11]. Отже, можемо стверджувати про початок нового етапу розвитку злочинності у сфері інформаційних технологій, яких характеризується широким використанням засобів масової інформації у викривленні правдивої інформації, поширенні кібершахрайства та кібертероризму.

Висновки. Отож, можемо зробити висновок, що хоча злочинність у сфері інформаційних технологій є відносно новим видом злочинності, вона завдає значної матеріальної шкоди, і з моменту свого виникнення пройшла 5 етапів розвитку:

1) поява такого явища як злочинність у сфері інформаційних технологій та формування ідей та субкультури хакерів;

2) становлення злочинності у сфері інформаційних технологій як міжнародного виду злочинності; виникнення злочинних угрупувань хакерів, які спеціалізуються на вчиненні кримінальних правопорушень у різних країнах;

3) злочинність у сфері інформаційних технологій стає транснаціональною;

4) використання мережі Інтернет для досягнення політичної мети, поява а також використання кібератак проти урядів окремих держав;

5) активне використання інформаційних технологій під час війни, що супроводжується широ-

ким залученням засобів масової інформації задля дезінформації населення, поширенні кібершахрайства та кібертероризму.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Основні завдання Департаменту кіберполіції Національної поліції України. URL: https://www.cybercrime.gov.ua/contacts.
2. Торбяк М.М. Кіберзлочинність як суспільне явище. Матеріали науклвл-практичної конференції *«Національна юридична освіта й наука в європейському та євроатлантичному вимірах»*. К., 2019. URL: http://elar.naiau.kiev.ua/bitstream/123456789/16158/1/Національна%20юридична%20освіта%20й%20наука%20в%20європейському%20та%20євроатлантичному%20вимірах_p198-201.pdf.
3. Всесвітній огляд економічних злочинів URL: https:/ /www.pwc.com/ua/uk/ Україна.
4. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія / Запоріжжя: Гуманітарний університет «ЗІДМУ», 2003. 296 с.
5. Конвенція про кіберзлочинність: міжнародний документ: від 23.11.2001 // Сайт Верховної Ради України. URL: http://zakon5.rada.gov.ua/laws/show/994_575.
6. Голубєв В.О. Комп'ютерні злочини в банківській діяльності. З.: Павел, 1997. 118 с.
7. Кравцова М. А. Поняття кіберзлочинності і її ознаки. *Часопис Київського університету права.* 2015. № 2. С. 320–324.
8. Бутузов В.М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави.* 2010. № 1 (3). С. 18.
9. Оліярчик Т. Інтернет-шахраї: обдирають як липку! Офіційний сайт видання «Львівська пошта», № 118 (1587), 01.11.2014 р. URL: https://www.lvivpost.net/lvivnews/n/27275.
10. Пивоваров В.В., Терещенко К.В. Шахрайство її банківськими картками: окремі питання віктимологічної профілактики. *Карпатський приватний часопис.* 2015. С. 132–137.
11. National Security Inside a Russian disinformation campaign in Ukraine in 2014. Архів оригіналу за 25 грудня 2017. URL: https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html.