УДК 004:343.9
DOI: 10.31866/2617-796x.3.1.2020.206112

Філіпенко Тетяна,
доктор наук з державного управління,
професор кафедри права та публічного адміністрування,
Маріупольський державний університет,
Маріуполь, Україна
tatkafili@gmail.com
https://orcid.org/0000-0001-9870-0889

СТАН ТА НАСЛІДКИ КОМП'ЮТЕРНОЇ ЗЛОЧИННОСТІ

Метою статті є аналіз технічної та правової складової проблеми комп'ютерної злочинності, а також огляд питань інформатизації та правового регулювання інформаційних відносин. Це є актуальною проблемою, оскільки цифрові технології впевнено ввійшли в сучасне життя і, на жаль, стали знаряддям вчинення таких злочинів, як тероризм, шпигунство, шахрайство, крадіжка, дитяча порнографія тощо.

Методами дослідження є методи аналізу правових відносин у сфері інформаційно-комп'ютерних технологій, класифікація кіберзлочинів і вплив цифрової недоброчесності на суспільство як з морального, так і з правового чи економічного погляду.

Новизною дослідження є розкриття сутності злочинного порушення функціонування інформаційних систем та техніко-технологічного боку злочину. Наслідки таких злочинів можуть бути доволі трагічними, навіть незважаючи на те, що спосіб їх скоєння суттєво відрізняється від традиційних терористичних актів чи техногенних катастроф. Зважаючи на вказані чинники, вчинення та аналіз кіберзлочинності є актуальною та важливою проблемою сьогодення, а зі швидким розвитком цифрових технологій з'являються нові методи скоєння злочинів, а отже, є необхідність для розробки й аналізу сучасних підходів до їх запобігання.

Висновки. Важливою відмінністю комп'ютерних злочинів є, так би мовити, відсутність традиційних ознак злочину, на кшталт відбитків пальців, речових доказів тощо. Специфікою комп'ютерних злочинів також є феномен інструментарію комп'ютерних посягань. На відміну від традиційних способів злочину (зброя, ніж і т. п.) інструментарій комп'ютерних – різноманітні програмні засоби комп'ютерних втручань.

Ключові слова: кіберзлочинність; кібербезпека; комп'ютерна безпека; кібератака; інформаційний тероризм.

Вступ. Інформаційні технології надають унікальні можливості для активного й ефективного розвитку економіки, політики, держави та суспільства, відкривають широкі можливості для всіх громадян. Але поряд з комп'ютеризацією відбувається розвиток комп'ютерної злочинності, розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки грошових коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем. Крім того, на думку фахівців з питань інформатизації та правового регулювання

© Філіпенко Т. В.

інформаційних відносин, комп'ютери є знаряддям вчинення таких злочинів, як тероризм, шпигунство, шахрайство, крадіжка, дитяча порнографія тощо.

Результати дослідження. Дослідження й аналіз численних випадків впливів на інформацію і несанкціонованого доступу до неї показують, що їх можна розподілити на випадкові та навмисні. Навмисні загрози можуть бути виконані за допомогою довготривалої масованої атаки несанкціонованими втручаннями або вірусами.

Наслідки, до яких призводить реалізація загроз: руйнування (втрата) інформації, модифікація (зміна інформації на помилкову, коректну за формою і змістом, але яка має інше значення), ознайомлення з нею сторонніх осіб. Ціна вказаних подій може бути різною: від невинних жартів до відчутних втрат, що в деяких випадках становлять загрозу національній безпеці країни. Попередження наведених наслідків у автоматизованій системі і є основною метою створення системи безпеки інформації. Для створення засобів захисту інформації необхідно визначити природу загроз, форми та шляхи їх можливого вияву і здійснення (Голубєв та Юрченко, 1998, с.36).

У юридичній літературі використовується така загальна класифікація можливих наслідків злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж.

1. Порушення функцій: а) тимчасові порушення, котрі призводять до плутанини в графіках роботи, розкладі тих чи тих дій і т. ін.; б) недоступність системи для користувачів; в) пошкодження апаратури (деякі практичні спеціалісти вважають, що пошкоджень апаратури, коли це стосується незаконного доступу, не буває); г) пошкодження програмного забезпечення.

2. Втрати значних ресурсів: грошей, речей, обладнання, інформації.

3. Втрата монопольного використання, яка обумовлена тим, що певна інформація цінна для власника лише доти, допоки він є її монопольним володарем.

4. Порушення прав: авторських, суміжних, патентних, винахідницьких тощо (Батурин, 1991, с.134-135).

А. А. Васильєв та Д. В. Пашнєв (2013, с.37) зазначають, що визначити вичерпний перелік можливих наслідків злочину у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку надзвичайно важко, оскільки в кожному разі ці наслідки залежать насамперед від змісту комп'ютерної інформації, яка зазнала шкоди. Характер шкоди в кожному конкретному злочині, як правило, залежить від тих суспільних відносин, які виступають не основним безпосереднім, а додатковим об'єктом. Це можуть бути відносини в різних сферах життєдіяльності людини, пов'язані з використанням ЕОМ, систем, комп'ютерних мереж і мереж електрозв'язку. Перешкоджаючи інформаційним відносинам, злочинець завдає або загрожує завдати шкоди тим суспільним відносинам, для інтенсифікації яких застосовуються комп'ютерні технології.

Суб'єктами вчинення комп'ютерних злочинів можуть бути як внутрішні користувачі (особи, які знаходяться в трудових відносинах з підприємством, на якому вчинений злочин), так і зовнішні користувачі (особи, які не знаходяться в трудових відносинах з підприємством, на якому вчинений злочин). Узагальнені дані

судово-слідчої практики свідчать, що внутрішніми користувачами вчиняється 94 % злочинів, тоді як зовнішніми користувачами – лише 6 %, при цьому 70 % – користувачі комп'ютерної системи, а 24 % – обслуговуючий персонал (Малій та Біленчук, 2019).

Загрозливим є той факт, що загальна кількість зловживань у сфері комп'ютерних технологій і розмір завданих при цьому збитків неухильно зростають. Це пояснюють декількома чинниками:

– високою динамічністю та масовістю впровадження в багатьох сферах людської діяльності різноманітних інформаційних технологій і процесів, що базуються на використанні засобів обчислювальної техніки;

– різким розширенням кола спеціалістів у галузі комп'ютерних технологій, підвищенням їхньої кваліфікації;

– недосконалістю законодавчої бази у сфері інформаційних відносин та інформаційної безпеки;

– недосконалістю чи відсутністю технічних засобів забезпечення інформаційної безпеки в конкретних інформаційних технологіях;

– низьким ступенем розкриття злочинів.

Тому є потреба осмислення комп'ютерної злочинності як соціального явища та напрацювання відповідних методик боротьби з нею, у тому числі виявлення і розслідування злочинів, які вчиняють використовуючи комп'ютерні технології.

Ефективна система боротьби з комп'ютерними злочинами передбачає створення законодавчого забезпечення такої боротьби, розробку захищених інформаційних технологій і засобів захисту з метою модернізації наявних інформаційних технологій.

Зміни в суспільних відносинах у результаті інформаційних процесів знайшли своє відбиття в нормативних актах Ради Європи, резолюціях, конвенціях, рекомендаціях і директивах Європарламенту та Євросоюзу. Процеси інформатизації відображаються в правовому просторі, нормативних та етичних нормах суб'єктів інформаційних відносин усіх розвинених країн світу.

За даними спеціалістів, станом на *листопад 2019* року у світі до Інтернету під'єднано *4,1 млрд людей*. Найвищий рівень підключення в Європі (82,5 %), а найнижчий – в Африці (28,2 %). Україна входить до першої десятки країн Європи за кількістю інтернет-користувачів. За даними Gemius, станом на *червень 2019 року* в Україні є 24,8 млн користувачів Інтернету. Згідно з даними щорічного дослідження «Kantar Україна» у *2019 році* 74 % населення України користується Інтернетом, 85 % з них – кожного дня (https://ucloud.ua/istoriya-internetu-vid-arpanet-do-sogodni/).

Україна, інтегруючись у світове співтовариство, за роки незалежності здійснила стрибок у єдиний світовий інформаційний простір у багатьох сферах суспільного життя. Наприклад, створення єдиної загальнодержавної системи електронних платежів під егідою Національного банку України є певним досягненням держави, сприяє укріпленню її суверенітету, економічній безпеці, здатності краще протистояти загальносвітовим і регіональним потрясінням. Зараз важко уявити перспективну сферу суспільної діяльності, в якій би не використовувалися сучасні

комп'ютери, локальні та глобальні комп'ютерні мережі, програмні комплекси від найпростіших до найвищого рівня складності (Філіпенко та Калайда, 2007, с.25).

Водночас надзвичайну стурбованість у спеціалістів викликає загрозливий розрив між рівнем утілення інформаційних комп'ютерних технологій і рівнем засобів їх правового, організаційно-технологічного захисту.

Отже, стан інформаційно-телекомунікаційних систем і рівень їх захисту є одним із найважливіших факторів, що впливає на інформаційну безпеку держави. Економічні збитки від комп'ютерних злочинів сьогодні стоять на одному рівні з перевагами, здобутими від упровадження електронно-обчислювальних машин у практику, а соціальні та моральні втрати взагалі не підлягають оцінці (Голубєв, 2003, с.34).

На 73-ій сесії Генеральної Асамблеї ООН генеральний секретар Антоніу Гуттереш оцінив щорічні збитки від кіберзлочинності у світі в розмірі 1,5 трлн доларів. На жаль, прогнози експертів з кібербезпеки невтішні. У майбутньому кількість злочинів і збитків від кібератак зростатиме, адже правопорушники йдуть щонайменше на крок попереду механізмів, які мають державні органи та приватних осіб щодо запобігання і розкриття таких злочинів (Нікулеску, 2019).

За підсумками 2018 року працівники Департаменту кіберполіції Національної поліції України були залучені до розслідування понад 11131 кримінальних проваджень, у тому числі: 1139 – у сфері протиправного контенту, 3697 – у сфері платіжних систем, 3607 – у сфері е-комерції, 2688 – у сфері кібербезпеки. Найбільша кількість злочинів була зосереджена в місті Києві (2277), а також на території Одеської (1084), Миколаївської (903) та Львівської (729) областей. Протягом року поліцейські виявили 6 тисяч злочинів, учинених у сфері використання високих інформаційних технологій, у тому числі: 680 – у сфері протиправного контенту, 2398 – у сфері платіжних систем, 1598 – у сфері е-комерції, 1325 – у сфері кібербезпеки.

У 2018 році працівники кіберполіції України викрили понад 800 осіб, які були причетні до вчинення злочинів у сфері високих інформаційних технологій. Згідно зі статистикою, більша частина підозрюваних – чоловіки у віці від 25 до 40 років. У сфері кібербезпеки найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet. За результатами міжнародної співпраці у 2018 році було викрито 8 транснаціональних хакерських угруповань і взято участь у понад 30 міжнародних операціях.

Позитивним моментом діяльності кіберполіції України є те, що у 2018 році було підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного сектору. Серед них – представники міжнародних компаній у сфері інформаційної безпеки та IT-компанії, а також поліція Австралії, Сингапуру, Катару та ще низки країн. Крім того, налагоджено ефективну взаємодію з найвідомішими світовими соціальними мережами (https://cyberpolice.gov.ua/results/2018).

Якщо порівнювати традиційні злочини і комп'ютерні, то останні відрізняються насамперед феноменом розповсюдження в часі та просторі, місцем і суб'єктом посягання. Інакше кажучи, щоб вкрасти гроші, немає потреби проникати в сховище банку, перетинати кордони, долати системи охорони та сигналізації. Досить

мати комп'ютер, вихідну інформацію щодо доступу та захисту електронних систем банку, набір хакерських програм і досвід такої роботи.

Інший важливий аспект комп'ютерних злочинів – це феномен безликості інформації. Такі традиційні ознаки криміналістичної експертизи, як почерк, відбитки пальців тощо – в електронних імпульсах комп'ютера безликі.

Специфікою комп'ютерних злочинів також є феномен інструментарію комп'ютерних посягань. На відміну від традиційних способів злочину (зброя, ніж і т. п.) інструментарій комп'ютерних злочинів – різноманітні програмні засоби комп'ютерних втручань.

На увагу заслуговує техніко-технологічний спосіб скоєння злочину. Суть його – злочинне порушення функціонування інформаційних систем, обумовлене впливом на їхні вразливі компоненти. І хоча цей вид злочину суттєво відрізняється від традиційних терористичних злочинів, наслідки за своєю трагічністю можуть бути подібними до великих техногенних катастроф.

Висновки. Отже, стрімке зростання глобальних комп'ютерних і телекомунікаційних систем та мереж, можливість підключення до них через звичайні телефонні лінії спричинили, крім безсумнівних переваг, появу цілої низки специфічних проблем, однією з яких є забезпечення ефективного захисту інформації та засобів її обробки. Поширення інформаційних технологій надає можливості їх використання для здійснення професійної кримінальної діяльності організованого злочинного світу через учинення традиційних злочинів нетрадиційними засобами, а також стимулює появу нових і раніше невідомих правопорушень.

СПИСОК ПОСИЛАНЬ

Батурин, Ю.М., 1991. *Проблемы компьютерного права*. Москва: Юридическая литература.

Васильєв, А.А. та Пашнєв, Д.В., 2013. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Вісник Кримінологічної асоціації України,* 5, с.34-42.

Голубєв, В.О. та Юрченко, О.М., 1998. *Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту.* Запоріжжя: Павел.

Голубєв, В.О., 2003. *Інформаційна безпека: проблеми боротьби з кіберзлочинами*. Запоріжжя: ЗІДМУ.

Історія Інтернету від Arpanet до сьогодні. [online] Доступно: <https://ucloud.ua/istoriya-internetu-vid-arpanet-do-sogodni/> [Дата звернення 28 березня 2020].

Малій, М. та Біленчук, П., 2019. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний вісник України*, [online] 39, с.14-15. Доступно: <https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/> [Дата звернення 28 березня 2020].

Нікулеску, Д., 2019. Кібербезпека: вразливі моменти. *Юридична газета Онлайн.* [online] Доступно: <https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html> [Дата звернення 28 березня 2020].

Підсумки 2018 року – Департамент Кіберполіції. *Департамент кіберполіції Національної поліції України.* [online] Доступно: <https://cyberpolice.gov.ua/results/2018/> [Дата звернення 29 березня 2020].
Філіпенко, Т.В. та Калайда, В.В., 2007. *Інформаційна безпека*. Донецьк: ДЮІ ЛДУВС.

REFERENCES

Baturin, Ju.M., 1991. *Problemy komp'juternogo prava* [Problems of computer law]. Moscow: Juridicheskaja literatura.
Filipenko, T.V. and Kalaida, V.V., 2007. *Informatsiina bezpeka* [Information security]. Donetsk: DIuI LDUVS.
Holubiev, V.O. ta Yurchenko, O.M., 1998. *Zlochyny u sferi kompiuternoi informatsii: sposoby skoiennia ta zasoby zakhystu* [Crimes in the field of computer information: methods of commission and means of protection]. Zaporizhzhia: Pavel.
Holubiev, V.O., 2003. *Informatsiina bezpeka: problemy borotby z kiberzlochynamy* [Information security: problems of combating cybercrime]. Zaporizhzhia: ZIDMU.
Istoriia Internetu vid Arpanet do sohodni [The history of the Internet from Arpanet to the present day]. [online] Available at: <https://ucloud.ua/istoriya-internetu-vid-arpanet-do-sogodni/> [Accessed 28 March 2020].
Malii, M. and Bilenchuk, P., 2019. Kibersvit u novomu tysiacholitti. Khto vony: kiberzlochyntsi, kibershakhrai, kiberterorysty? [Cyberspace in the new millennium. Who are they: cybercriminals, cybercriminals, cyberterrorists?]. *Yurydychnyi visnyk Ukrainy*, [online] 39, pp.14-15. Available at: <https://lexinform.com.ua/dumka-eksperta/kibersvit-u-novomu-tysyacholitti-hto-vony-kiberzlochyntsi-kibershahrayi-kiberterorysty/> [Accessed 28 March 2020].
Nikulesku, D., 2019. Kiberbezpeka: vrazlyvi momenty [Cybersecurity: vulnerable points]. *Yurydychna hazeta Onlain*. [online] Available at: <https://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html> [Accessed 28 March 2020].
Pidsumky 2018 roku – Departament Kiberpolitsii [Results of 2018 – Cyberpolice Department]. *Departament kiberpolitsii Natsionalnoi politsii Ukrainy*. [online] Available at: <https://cyberpolice.gov.ua/results/2018/> [Accessed 29 March 2020].
Vasyliev, A.A. and Pashniev, D.V., 2013. Osoblyvosti kvalifikatsii zlochyniv u sferi vykorystannia EOM (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku [Features of qualification of crimes in the field of use of computers, systems and computer networks and telecommunication networks]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy*, 5, pp.34-42.

UDC 004:343.9

Filipenko Tetiana,
Doctor of Sciences (Public Administration),
Professor of Law and Public Administration,
Mariupol State University,
Mariupol, Ukraine
tatkafili@gmail.com
https://orcid.org/0000-0001-9870-0889

STATUS AND CONSEQUENCES OF COMPUTER CRIME

The purpose of the article is to analyze the technical and legal components of the problem of cybercrime, as well as an overview of informatization and legal regulation of information relations, this is a topical issue because digital technologies have confidently entered modern life, and, unfortunately, have become tools for crimes such as terrorism, espionage, fraud, theft, child pornography, etc.

The research methods are methods of analysis of legal relations in the field of information and computer technologies, classification of cybercrimes and the impact of digital dishonesty on society both from a moral and from a legal or economic point of view.

The novelty of the study is the disclosure of the essence of the criminal violation of the functioning of information systems, and the technical and technological side of the crime. The consequences of such crimes can be quite tragic, even though the way they are committed differs significantly from traditional terrorist acts or man-made disasters. Given these factors, the perpetration and analysis of cybercrime is a pressing and important issue today, and given the rapid development of digital technology, new methods of committing crimes are emerging, and therefore there is a need to develop and analyze modern approaches to their prevention.

Conclusions. An important difference between computer crimes is, so to speak, the absence of traditional signs of a crime, such as fingerprints, physical evidence, and so on. The specificity of computer crimes is also the phenomenon of computer encroachment tools. Unlike traditional methods of crime (weapons, knives, etc.), the tools of computer crime are various software tools for computer intervention.

Keywords: cybercrime; cybersecurity; computer security; cyber attack; information terrorism.

УДК 004:343.9

Филипенко Татьяна,
доктор наук по государственному управлению,
профессор кафедры права и публичного администрирования,
Мариупольский государственный университет,
Мариуполь, Украина
tatkafili@gmail.com
https://orcid.org/0000-0001-9870-0889

СОСТОЯНИЕ И ПОСЛЕДСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ

Целью статьи является анализ технической и правовой составляющих проблемы компьютерной преступности, а также обзор вопросов информатизации и правового регулирования информационных отношений. Это актуальная проблема, поскольку цифровые технологии уверенно вошли в современную жизнь и, к сожалению, стали орудием совершения таких преступлений, как терроризм, шпионаж, мошенничество, кража, детская порнография и тому подобное.

Методами исследования являются методы анализа правовых отношений в области информационно-компьютерных технологий, классификация киберпреступлений и влияние цифровой недоброчестности на общество как с моральной, так и с правовой или экономической точек зрения.

Новизной исследования является раскрытие сущности преступного нарушения функционирования информационных систем и технико-технологической стороны преступления. Последствия таких преступлений могут быть довольно трагическими даже несмотря на то, что способ совершения существенно отличается от традиционных террористических актов или техногенных катастроф. Учитывая указанные факторы, совершение и анализ киберпреступности является актуальной и важной проблемой современности, а в связи с быстрым развитием цифровых технологий появляются новые методы совершения преступлений, а следовательно есть необходимость для разработки и анализа современных подходов к их предотвращению.

Выводы. Важным отличием компьютерных преступлений есть, так сказать, отсутствие традиционных признаков преступления, например, отпечатков пальцев, вещественных доказательств и тому подобное. Спецификой компьютерных преступлений также является феномен инструментария компьютерных посягательств. В отличие от традиционных способов преступления (оружие, нож и т. д.) инструментарий компьютерных преступлений – различные программные средства компьютерных вмешательств.

Ключевые слова: киберпреступность; кибербезопасность; компьютерная безопасность; кибератака; информационный терроризм.

15.04.2020