УДК 355.488: 681.3

МАРІЦ Д.О., *кандидат юридичних наук, доцент,*
кафедра інформаційного права
та права інтелектуальної власності НТУУ “КПІ”

“КІБЕРАТАКА” – ВІЙНА МАЙБУТНЬОГО

Анотація. *У статті досліджуються проблеми правового регулювання правовідносин, які виникають у сфері кібернетичної безпеки.*
Ключові слова: *кібератака, кібербезпека, вірус, кібершпіонаж, кіберзлочинці.*

Аннотация. *В статье исследуются проблемы правового регулирования правоотношений, которые возникают в сфере кибернетической безопасности.*
Ключевые слова: *кибератака, кибербезопасность, вирус, кибершпионаж, киберпреступники.*

Summary. *The article examines the issues of legal regulations in the field of cyber security.*
Keywords: *cyber attack, cyber security, virus, cyber spying, cyber criminals.*

Постановка проблеми. Питання кібербезпеки є основним для розробки програмних продуктів у галузі перспективних технологій, оскільки автоматизовані системи управління технологічними процесами важливих об’єктів знаходяться під загрозою як звичайних вірусів, так і цілеспрямованих атак. Тому захист інфраструктури інформаційних технологій є першочерговим завданням для спеціалістів у сфері інформаційної безпеки. Розширення інформаційного простору опосередковується впровадженням ноу-хау, досягнень науки та техніки, Інтернет ресурсів. Це безумовно впливає на інформаційну конкуренцію, а відтак і на кібернетичну безпеку, як окремих суб’єктів у суспільстві так і держави в цілому. За останнє десятиріччя кібернетична безпека сформувалася у самостійний науковий напрям, що має свою специфіку поставлених задач та методів дослідження [1]. У перекладі з грецької, кібернетика – це мистецтво управління. Однак таке управління, а часто-густо і контроль, використовується поза межами правового поля. Тому незвичним, а можливо і незрозумілим, на перший погляд, видається переплетіння суто технічних галузей з гуманітарними. Водночас юридичним аспектам захисту від кібератак на інформаційні ресурси не приділено достатньої уваги правознавцями, що і обумовлює актуальність даної проблематики.

Аналіз останніх досліджень і публікацій. Основні праці, які прямо або опосередковано стосуються такого явища як “кібератака” належать Богушу В.М., Бурячку В. Л., Духвалову А.П., Захаровій М.В., Корченко А.О., Хропаті І.В. Однак, ці напрацювання належать фахівцям у галузі технічних наук і більшою мірою стосуються розробок моделей захисту інформаційних ресурсів, що дозволяє визначити здатність відповідної системи захисту протистояти кібератакам. Водночас, лише спільними зусиллями, як представників технічних наук так і юридичних, можна досягти відповідних зрушень для досягнення спільної мети – здійснення кібернетичної безпеки, що черговий раз підкреслює як необхідність детального вивчення технічних питань щодо запобігання та попередження вчинення протиправних дій в інформаційному просторі, так і вироблення відповідної законодавчої бази.

Метою статті є з’ясування порядку правового регулювання правовідносин у сфері інформаційної безпеки, що заподіюються шляхом вчинення кібератак у Інтернет-мережі.

Виклад основного матеріалу. Кібератака – це поняття, яке стало вже звичним явищем у сучасному суспільстві. Соціологи всього світу одностайно стверджують, що сучасне суспільство стало як ніколи раніше конфліктним. Кількість конфліктів у політичній, соціальній, трудовій, релігійній, а також особистісних сферах невпинно збільшується. В свою чергу, розвиток науки та новітніх технологій не завжди приносить користь, а навпаки – їх використання стає вдалим інструментарієм для винахідливих віртуальних злочинців. Тому у сучасному суспільстві досить розповсюдженим явищем стали злочини у кіберпросторі. Так, Кримінальний кодекс України вперше передбачив самостійний розділ про ці злочини – розділ XVI “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” (ст. 361-363[1]), положення цього розділу змінювалися і доповнювалися – це свідчить про актуальність цієї проблеми в суспільстві [2]. Кількість таких злочинів стрімко зростає, а от Інтернет-шахраїв впіймати доволі складно, говорять в обласному управлінні міліції. “Для справи злочинцю треба лише комп’ютер або інший гаджет та Інтернет, до якого можна підключитися деінде”, – розкриває схему злодюг в.о. начальника відділу у боротьбі із кіберзлочинністю УМВС Черкаської області Богдан Горбачов [3]. Водночас спостерігається вільне використання значної кількості термінів (та їх синонімів) що часто не узгоджені між собою. Так у Законі України “Про основи національної безпеки України” згадуються “комп’ютерна злочинність” та “комп’ютерний тероризм”, причому жоден з цих термінів на має свого визначення ані в цьому, ані в інших нормативних документах. В Законі України “Про боротьбу з тероризмом” поняття “комп’ютерний тероризм” не згадується взагалі, а ті елементи, що можуть до нього відноситись, прописані як складова частина поняття “технологічний терроризм” [4].

На сьогодні виникає нагальна потреба у спеціальному законі, який би врегульовував відносини, які виникають у кібернетичному просторі. Звичайно, така потреба виникла не сьогодні та не вчора, а прийняття таких необхідних нормативних актів значно затягнулось. На сьогодні простежується тенденція виникнення нових понять і термінів, і відповідно “шкутильгання” правотворчості, яка покликана в даному випадку опосередковувати та регулювати правовідносини в інформаційній сфері.

У червні 2013 року Верховною Радою України був розглянутий законопроект від 04.06.13 р. № 2207а “Про кібернетичну безпеку України”. Пройшло ще 2 роки і 19 червня 2015 року був поданий до розгляду проект № 2126а у новій редакції “Про основні засади забезпечення кібербезпеки в Україні” [5]. У статті першій пропонується наступне визначення *кібератаки* як несанкціонованих дій, що здійснюються за допомогою інформаційно-комунікаційних технологій та спрямовані на порушення конфіденційності, цілісності і доступності інформації, яка обробляється в інформаційній (автоматизованій), телекомунікаційній, інформаційно-телекомунікаційній системі, або порушення сталого функціонування такої системи.

На наш погляд, дане визначення потребує певного уточнення. Видається, що такі несанкціоновані дії спрямовуються не лише на конфіденційність, цілісність і доступність інформації, а направляються з метою знищення інформації або її підміни. Крім того такі хакерські дії можуть вчинятись з метою кібершпіонажу, що в подальшому призведе до використання такої інформації у власних цілях, або з метою її подальшого продажу зацікавленим особам, зокрема конкурентам у певній сфері діяльності. Водночас, в аналітичній записці Інституту стратегічних досліджень при Президентові України, пропонується таке визначення кібератаки – цілеспрямовані дії, які реалізуються в кіберпросторі (або за допомогою його технічних можливостей), що

призводять (можуть призвести) до досягнення несанкціонованих цілей (порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації, деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан громадян) [4]. Також в аналітичній записці надається ще 6 визначень поняття кібератака, які запропоновані різними державними органами.

Під *кібернетичною безпекою (кібербезпека)* проект (№ 2126а), розуміють стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. Аналізуючи інші нормативно-правові акти, на жаль приходимо до висновку, що законодавець не визначив ключових понять та термінів у сфері кібернетичної безпеки. Так, у зазначеному проекті закону № 2126а, під *кіберзлочином* визначають – суспільно небезпечне винне діяння у кіберпросторі, передбачене законодавством України про кримінальну відповідальність. А під *кіберзлочинністю* – сукупність кіберзлочинів.

Термін “кіберзлочинність” часто вживається поряд з терміном “комп’ютерна злочинність”, причому нерідко ці поняття використовуються як синоніми. Поняття “кіберзлочинність” (в англ. варіанті – cybercrime) ширше, ніж “комп’ютерна злочинність” (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Так, Оксфордський тлумачний словник визначає приставку “cyber” як компонент складного слова, що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення міститься у Кембриджському словнику. Таким чином, “cybercrime” – це злочинність, пов’язана як з використанням комп’ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін “computer crime” в основному відноситься до злочинів, скоюваних проти комп’ютерів або комп’ютерних даних [6]. У зв’язку з ратифікацією Україною Конвенції “Про кіберзлочинність” від 7 вересня 2005 року вважаємо за доцільне використовувати термін “кіберзлочинність”.

Звичайно, йдеться не лише про суто технічний підхід до вирішення проблеми боротьби з кіберзлочинцями шляхом декларування визначень та понять у певному нормативному акті, оскільки, на жаль, на сьогодні існують так звані “мертві норми”, які існують лише на папері. Крім цього, відповідно до експертного висновку, що був наданий Київським відділенням Всесвітньої асоціації з розроблення методологій та стандартів у галузі управління, аудиту і безпеки інформаційних технологій ISACA (Information Systems Audit and Control Association) проект закону № 2126а не охоплює та не гарантує захисту від актуальних кібер-загроз; створення системи інформаційної безпеки, адекватної стратегіям розвинених держав в цій галузі. Зокрема проект закону не містить основних компонентів для побудови державної інформаційної безпеки: план легалізації програмного забезпечення в критичних об’єктах інфраструктури [7].

“Naikon” – “Kaspersky Lab” провела дослідження однієї з найбільш активних кампаній щодо кібершпіонажу у Південно-Східній Азії. В результаті чого з’ясувалось, що від дій злочинців вже протягом 5 років страждають військові, громадські організації в 11 країнах регіону, зокрема на Філіппінах, Малайзії, Камбоджі, Індонезії, В’єтнамі, Сінгапурі, Непалі, Таїланді, Лаосі та Китаї. Злочинці, володіли китайською мовою, готували усю необхідну для кібератаки інфраструктуру, на території країни, що дозволяло підключатись в режимі реального часу до мережі своїх потенційних жертв та отримувати необхідну інформацію. В арсеналі шпіонського “Naikon” – 48 команд для різноманітних віддалених операцій, у тому числі на перевірку даних, які знаходяться в корпоративній мережі, що піддається атаці, завантаження файлів, встановлення додаткових модулів. До жертв такі програми потрапляють за допомогою цільового

фішингу – листів, які містять додатки, що потенційно можуть зацікавити отримувача. Насправді такі додатки містять виконуючий файл, який завантажує шпіонську програму на комп’ютер. У 2014 році “Kaspersky Lab” відзначила значний стрибок у активності угрупування. Одразу після трагедії із зниклим літаком Malaysia Airlines, який виконував рейс МН 370, злочинці здійснили масову розсилку по організаціях, які потенційно володіли інформацією про трагедію. Кіберзлочинці, які стоять за “Naikon”, змогли створити гнучку інфраструктуру, яка може бути розгорнута у будь-якій країні, яка їх зацікавить та дозволить перенаправляти інформацію з систем жертв на сервер злочинців. Крім того, отримання потрібних даних значно спрощується завдяки наявності спеціально визначених операторів, які займаються визначеним колом користувачів [8].

Для попередження кібератак, а також ефективної боротьби з ними, погоджуємось з думкою В.М. Богуша та В.Л. Бурячка, що наступним кроком має стати підготовка спеціалістів: діяльність, яких буде пов’язана із протидією кіберзлочинності та забезпеченням кібербезпеки особистості, підприємства та держави у цілому. Найбільш цікавими з точки зору майбутніх працедавців можуть стати знання, які стосуються:

- теоретичних основ кібернетичної безпеки;
- правових та організаційних засад протидії кіберзлочинності;
- методів та засобів протидії кіберзлочинності;
- програмного забезпечення систем кібернетичної безпеки;
- криптографічних механізмів кібернетичної безпеки;
- кібернетичної безпеки підприємств;
- основ кібернетичної безпеки держав тощо [9, с. 129].

Інформаційна війна 21 сторіччя відрізняється від “холодної війни” тим, що способів впливу на маси стало набагато більше. Якщо раніше більшість людей довіряли ЗМІ, як єдиному джерелу інформації, яке не могло збрехати, то зараз довіра до телебачення значно впала, і будь-яка інформація, яка надходить через екран, повинна підкріплюватись чимось дуже значним, яскравим і навіть лячним. Щоб належним чином надавати таку інформацію, ЗМІ була створена ціла система, яка спрямовується на те, щоб тримати увесь світ на “гачку”. Інтернет став не просто інноваційним проривом, а як наслідок став використовуватись як інформаційний важіль. Мільйони людей витрачають більшу частину свого життя у просторах всесвітнього павутиння, і частина такого життя дуже особиста, навіть інтимна. І можливо, більшість вірить в те, що це його особистий віртуальний простір, який начебто залишиться секретним від інших. В такі ігри грають не тільки Android з Apple, але і антивірусні компанії, які із задоволенням запускають вірусні програми, проти яких потім і борються. Ось такий віртуальний театр відбувається повсякчас у кіберпросторі. Конфлікти, які виникають, не вирішуються, а натомість розробляються більш закручені стратегії, які дозволяють здійснювати більш ефективні кібератаки. Вони можуть вивести з ладу об’єкти оборонного призначення, та будь-які інші об’єкти, які представляють інтерес для кіберзлочинців. Зокрема, такі можливості продемонстрував вірус “Стакснет”, який виявили експерти у 2010 році.

Спеціалісти впевнені, що “Стакснет” є найбільш складною, шкідливою програмою, яка відноситься до абсолютно нового покоління комп’ютерних вірусів. Ця програма може обновлюватись через глобальну комп’ютерну мережу, отримуючи обновлення з віддалених серверів. Зі слів німецького фахівця, ціллю даного вірусу є конкретне підприємство, тобто він здатен працювати виключно точно на об’єкт. Такий складний комп’ютерний вірус дозволяє провести атаку на найважливіші промислові об’єкти, і є новою епохою у методах ведення війни. У війнах майбутнього такі технології

отримають широке розповсюдження, оскільки кібератаки дозволять на певний час знешкодити бойові системи управління. Тому для боротьби з кібератаками необхідні значні ресурси, а також спільна робота структур безпеки багатьох країн.

Так, перші зразки вірусу “Potao” датуються 2011 роком, однак атаки з його використанням до цього часу залишались поза межами публічного поля. Значний зріст заражень, за даними ESET LiveGrid, спостерігався у 2014 – 2015 роках. Вірусні експерти пов’язують це з додаванням механізму заражених зйомних USB-носіїв. За оцінкою експертів ESET, атакувальники приступили до підготовки атак на українських користувачів у 2014 році. Оператори “Potao” опанували новий вектор зараження. Вони створили шкідливу веб-сторінку MNTExpress, яка імітувала сайт російського сервісу Pony Express. Потенційним жертвам направлялись SMS із шкідливою зноскою, “трек-кодом” та особистим зверненням, що вказує на точну направленість атаки. У березні 2015 року експерти ESET виявили зразки “Potao” на стратегічних об’єктах, включаючи уряд, військові відомства та одне з найбільших інформаційних агентств. Атаки здійснювались шляхом фішингових повідомлень на електронну пошту із шкідливими вкладками – виконуючими файлами під виглядом документів Microsoft Word із назвами, які можуть привертати увагу та зацікавити отримувача. Ця кібергрупа, яка розповсюджує “Potao”, досі активна. На це вказує зразок шкідливого програмного забезпечення від 20 липня 2015 року, який було направлено потенційній жертві у Грузії. У якості документа-принади використовується pdf-файл [10].

Непоодинокими є випадки, коли служба безпеки певної компанії, намагається власноруч зламати свою ж систему захисту, перш ніж це зроблять зловмисники. Зокрема, банк Barclays був створений у Лондоні у 1896 році. На сьогодні це велика компанія, яка має мережу представництв в США, Європі, Азії. У Великобританії вся діяльність здійснюється через дочірній Barclays Bank PLC, який є другим за величиною активів банком у країні. Під керівництвом голови служби безпеки банку спеціалісти імітуватимуть спробу хакерів проникнути у систему. Основним завданням групи є тестування систем безпеки. Вони спробують найрізноманітніші варіанти злому, а також попередження атак. За результатами роботи мають бути виявлені та усунені вразливості у системі, доки ними не скористалися хакери [11].

Висновки.

В результаті викладеного приходимо до наступного:

- з’являються нові терміни, які не мають законодавчого закріплення у сфері кібернетичної безпеки, однак є широковживаними у засобах масової інформації, наукових працях та інших джерелах;
- виникає необхідність співпраці України з іншими країнами з метою попередження загроз, обміну досвідом щодо механізмів боротьби з кіберзлочинцями, розробки методів реагування на загрози;
- постає необхідність удосконалення законодавчої бази, шляхом приведення у відповідність термінології існуючих нормативно-правових актів та прийняття нових спеціальних законів у кібернетичній сфері. Однак це не виключає можливість здійснити уніфікацію нормативних актів, а також, можливо, і гармонізувати вітчизняне законодавство, шляхом сприйняття правових досягнень інших держав та використання таких положень у національному законодавстві.
- з метою реальної роботи механізму захисту інформаційної сфери, необхідно визначити коло суб’єктів, на яких буде покладатись обов’язок здійснення державної політики щодо кібернетичної безпеки України;

- крім правових аспектів, які мають сприяти зрушенням у досліджуваному напрямку, постає необхідність підготовки висококваліфікованих кадрів у сфері інформаційних технологій.

Використана література

1. – Режим доступу : http://is.ipt.kpi.ua/kibernetichna-bezpeka-matematichni-metodi-kibernetichnoyi-bezpeki-novi-spetsializatsiyi-fti
2. Кіберзлочинність в Україні. – Режим доступу : //www.science-community.org/ru/node/16132
3. Правоохоронці радять бути обачними із Інтернет-закупками. – Режим доступу : http://v4asno.com/pravoohorontsi-radyat-buty-obachnymy-iz-internetzakupamy
4. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : аналітична записка. – Режим доступу : //www.niss.gov.ua/articles/454
5. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=55657
6. Кіберзлочинність : проблеми боротьби і прогнози – Режим доступу : http://anticyber.com.ua/article_detail.php?id=140
7. Про основні засади забезпечення кібернетичної безпеки України : пропозиції Київського відділення ISACA до проекту закону України. – Режим доступу : //www.slideshare.net/IsacaKyiv/isaca-kyiv-chapter-comments-law-dss-vr-v-05
8. Країни Південно-Східної Азії роками перебувають в кібероблозі – Режим доступу : http://ru.focus.lv/tehnologijas/internets/strany-yugo-vostochnoy-azii-regiona-godami-prebyvayut-v-nastoyashchey-kiberosade
9. Богуш В.М., Бурячок В. Л. Рекомендації щодо розробки та запровадження профілю навчання “Кібернетична безпека” в Україні // Безпека інформації. – 2014. – Т. 20. – № 2. – С. 126-131.
10. Кибератаки “Potao” нацелены на госслужбы России и Украины – Режим доступу : //www.anti-malware.ru/news/2015-07-31/16575
11. Сотрудники спецотдела британского банка Barclays взломают собственную систему безопасности. – Режим доступу : //www.3dnews.ru/919603

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~