ЮРИДИЧНІ НАУКИ

DOI: https://doi.org/10.32839/2304-5809/2019-4-68-24
УДК 343.3/7

Бабійчук В.С.
Національний юридичний університет імені Ярослава Мудрого

КІБЕРТЕРОРИЗМ ТА ПРОТИДІЯ ЙОМУ

Анотація. У статті проаналізовано сутність поняття кібертероризму, окреслено основні методи протидії даній загрозі. Розглянуто міжнародні та національні нормативно-правові акти, документи міжнародних організацій, що регулюють деякі аспекти кібертероризму. У загальних рисах окреслено історію становлення кібертероризму. Вказано, що не існує комплексного підходу до визначення кібертероризму у міжнародних актах. Наголошено на важливості перейняття зарубіжного досвіду боротьби з даним видом злочинності та на необхідності подальшого вдосконалення національного законодавства у цій сфері. Підкреслено важливість розвитку подальшої співпраці українських органів, створених в рамках протидії світовому кібертероризму, з світовими – Європейським центром по боротьбі з кіберзлочинністю, відділенням по боротьбі з кіберзлочинністю при Інтерполі та підрозділом по боротьбі з тероризмом при ОБСЄ.

Ключові слова: кібертероризм, інформаційні технології, кіберпростір, кіберзлочин, кібербезпека.

Babiychuk Valentina
Yaroslav Mudryi National Law University

CYBERTERRORISM AND COUNTERACTION TO IT

Summary. The article analyzed the essence of the concept of cyberterrorism, outlined the main methods of countering this threat. International and national legal acts, documents of international organizations regulating some aspects of cyberterrorism were examined. In a general way, outlined the history of the formation of cyberterrorism. It was stated that there was no comprehensive approach to the definition of cyberterrorism in international acts. The importance of adopting foreign experience in the fight against this type of crime and the need to further improve national legislation in this area. In article noted the importance of future cooperation between national bodies, which have been established to combat world cyberterrorism, with European Cybercrime Centre, Interpol office on combating information crime and OSCE. Also author examined the content and delivery of technical cooperation in the field of cyberterrorism and fact that the every country`s national security is profoundly impacted by the outcome of these efforts as a common work for mutual benefits to all humanity. All of these is intended to help overcome the adverse influence of cybercrime. In this article author analyzed such issues as information technology, cyberspace, cyber security, cybercrime as defined under domestic law and in international treaties. The importance of legal protection of the population from cyberterrorism. That article also emphasized that human safety must be one of the chief concerns and the highest priority of the Government. It must be recognized that national security is multifaceted concept that includes the legal rights of citizens to protect themselves against crime, protection of the vital interests of individuals, society from terrorism. Author also examined that the term «cyber security» must be understood as the type of protection of a country`s information space that allows the attainment of its national interests and observance of the rights of the individual, society and country as a whole. Cybercrime and notably cyberterrorism was repeatedly emphasized as one of new threats to political and economic stability of the country.

Keywords: cyberterrorism, information technology, cyberspace, cybercrime, cyber security.

Постановка проблеми. Наразі інформаційні технології, глобальні мережі, врешті-решт, персональні комп'ютери та мобільні телефони, народжені глобалізацією, є синонімами прогресу, визначними здобутками 21 століття. Члени сучасного інформаційного суспільства не уявляють свого життя без мережі Інтернет, комп'ютерної техніки, електроніки, телекомунікацій та радіотехніки, адже все це забезпечує людині доступ до інформації буквально в один «клік», дозволяє обмінюватися даними з надзвичайною швидкістю, а що вже говорити про електронну комерцію, фінансові та торгові транзакції, які проводяться за допомогою комп'ютерних мереж. Численні соціальні мережі об'єднують цілі континенти, а по глибоководним кабелям, що пронизують планету, без зупинки циркулюють колосальні обсяги інтернет-трафіку. Модернізація технологій, значні здобутки науки та техніки, які мали б слугувати виключно задля забезпечення комфорту людини, працювати на благо суспільства, часто використовуються у руйнівних, злочинних цілях. Прогрес 21 століття з його загальною інформатизацією проник і у сферу злочинної діяльності. Тепер злочинцю не потрібен безпосередній контакт з жертвою та стандартні знаряддя вчинення злочину, такі як вогнепальна чи холодна зброя, йому вистачить персонального комп'ютера або навіть смартфону, відповідного програмного забезпечення та доступу до інформаційних систем. Стандартні ознаки злочину – місце, обстановка, спосіб – також трансформуються та охоплюються наразі кіберпростором. Зловмиснику зараз достатньо доступу до автоматизованої системи, комп'ютерної мережі чи мережі електрозв'язку та наявності комп'ютера. Недосконалість людської природи заважає нам використовувати всі досягнення виключно собі

на благо, тож зі створенням перших комп'ютерів почалася ера злочинів проти цифрового середовища. Організована злочинність дуже швидко еволюціонує, особливу в епоху «Глобалізації 4.0» та розширює сферу свого негативного впливу на безпечне та впорядковане життя сучасних демократичних країн, на відміну від законодавства. ІТ розвиваються з блискавичною швидкістю, а реакція на це правоохоронних органів на жаль все ще змушує бажати кращого. Система не встигає за прогресом, а масштаб загрози зростає у геометричній прогресії. До речі, щодо актуальності обраної нами тематики дослідження. Проблема кібертероризму піднімалася цьогоріч на Всесвітньому економічному форумі у Давосі. Він проводився під гаслом: «Глобалізація 4.0: формування глобальної архітектури в епоху четвертої промислової революції», і, так би мовити, підсумував глобалізаційні процеси 2019 року. На ньому піднімались теми психологічного здоров'я людства, охорони довкілля, кліматичної кризи, військових конфліктів, інформаційної безпеки, протидії кіберзлочинності, кібертероризму, обговорювались недоліки ліберальної демократії, мінуси цифрової економіки, проблеми захисту персональних даних, штучний інтелект та його місце в сучасному світі і багато іншого.

Аналіз останніх досліджень і публікацій. Проблемою застосування кримінальної відповідальності за кіберзлочинність ті інші суспільно – небезпечні діяння, що вчиняються з застосуванням інформаційних технологій та питанням протидії і запобігання даним злочинам, аналізом даного феномену, вивченням його закономірностей та тенденцій займається достатньо велика кількість вітчизняних та зарубіжних науковців: С. Хантінгтон, С. Хоффман, М. Делягін, В. Голубев, П. Біленчук, Н. Розенфельд, В. Сивухін, С. Орлов, А. Музика, В. Голіна, Б. Головкін, Р. Дремлюга, В. Брижко, Л. Шеллі, Ф. Уільямс, А. Голуб та ін. Можна зробити висновок, що дана тема є доволі розробленою в науковій літературі, проте дуже дискусійною та оскільки прогрес ніколи не стоїть на місці і технології розвиваються шаленими темпами – кіберзлочинність також модернізується, стає транснаціональною і ставить світову безпеку під загрозу, тож всебічне вивчення, дослідження та розуміння сутності даного явища та протидія йому є наразі надзвичайно актуальними питаннями.

Мета статті. Головною метою даної роботи є безпосередній аналіз явища кібертероризму, дослідження питання встановлення кримінальної відповідальності за діяння у кіберпросторі та методи ефективної боротьби з даним видом злочинів, превентивні засоби, що могли б зменшити кількість правопорушень у цифровому просторі, а також питання щодо мінімізації негативних наслідків від злочинної діяльності з використанням інформаційних технологій, міжнародне співробітництво з протидії організованій кіберзлочинності, нормативно – правову базу щодо запобігання проявам кіберзлочинності.

Виклад основного матеріалу. Розвиток сучасних кібернетичних, інформаційних та телекомунікаційних систем надає людству величезний спектр можливостей. Вони роблять світ єдиним, гомогенним. Ми можемо передавати дані на великій швидкості, робити детальні знімки планет та зірок, вивчати світовий океан. Науково-технічний прогрес призводить до «розмивання» національних кордонів та створення єдиного інформаційного простору та мереж. Наразі інформаційно-комунікаційні технології є основою усіх сучасних адміністративних та економічних систем, без них важко собі уявити нормальне функціонування усіх видів інфраструктур, державних інститутів та установ. Вони є універсальними, загальнодоступними та екстериторіальними. За допомогою ІТ зараз укладаються договори, проводяться грошові транзакції, що вже говорити про електронне урядування. Віртуальний світ. Проте у технологічного прориву та загальної комп'ютеризації є й інша сторона медалі – з розвитком ІТ удосконалюються також і методи перехоплення інформації, зловмисники – кібертерористи здійснюють несанкціонований доступ до комп'ютерних систем, з легкістю визначають коди доступу, підбирають ключі до шифрів або інших зашифрованих даних. тож виникає крайня необхідність захисту конфіденційності нашої інформації, безпеки користування Інтернетом та нормального його функціонування. У сучасному світі інформаційна безпека відіграє одну з провідних ролей у підтриманні порядку, стабільності та спокою як на території конкретних держав, так і на міжнародному рівні. Розвинені держави вкладають значні кошти у сферу безпеки ІТ. MarketsandMarkets, компанія, що займається статистикою, у своїх звітах надала такі цифри: станом на 2018 рік витрати фірм на захист від хакерів склали майже 153 мільярди, а за прогнозом на 2023 рік, вони можуть зрости до 248 мільярдів доларів [1]. Проте, навіть найрозвиненіші держави з потужним науковим потенціалом і повною казною страждають від людського впливу на сферу інформаційної безпеки. Людина, на відміну від автономного штучного інтелекту, сповнена слабкостей та пороків. Халатність, недостатньо високий рівень розвитку технологій забезпечення схоронності інформації – усе це спричиняє збитки на локальному рівні, і породжує все нові і нові загрози глобального рівня. У практиці повно випадків, коли рядові співробітники використовували робочі комп'ютери для персональних цілей, що є, на хвилиночку грубим порушенням корпоративної політики щодо безпеки, дана халатність призводила до викрадення секретної інформації, до встановлення зловмисниками контролю над усією локальною мережею компанії. Заражаються термінали, інформація про ваші персональні дані гуляє у вільному доступі, переведення коштів мережею через неможливість їхньої безпечної транзакції припиняється – це все прикрі наслідки невжиття заходів кібербезпеки. Проте, атаки можуть бути куди страшнішими: хакерами захоплюються керуючі органи держави, руйнується інфраструктура міст, спричиняються гучні міжнародні скандали. Наведемо декілька прикладів глобальних кібератак, які сколихнули світ у 2017 році: Wanna Cry, Petya, NotPetya, Bad Rabbit. Дані віруси вражали операційну систему Microsoft Windows шляхом шифрування файлів. Вони атакували державні підприємства, комерційні та урядові установи, банки,

медіа, комп'ютери приватних осіб, тощо. А чого вартий інцидент з колишнім системним адміністратором ЦРУ та АНБ Сполучених Штатів Америки Едвардом Сноуденом, який надав газетам «The Guardian» та «The Washington Post» дані про прослуховування і збирання спецслужбами персональних даних та листувань громадян, що призвело до масштабного політичного скандалу, розриву багатьох важливих для безпеки країн західного блоку міжнародних договорів і викликало недовіру в дипломатичних колах [2].

«Кіберзлочинність» є правничим терміном, що закріплений у Законі України «Про основні засади забезпечення кібербезпеки України» в редакції від 08.07.2018 р. і являє собою: «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» [3]. Поряд з даним терміном національне законодавство передбачає також поняття «індикаторів кіберзагроз», «інформацію про інцидент кібербезпеки», «кіберінцидент», «кібератаку», «кіберзагрозу», «кібербезпеку», «кіберзахист», «кіберзлочинність», «кібероборону», «кіберрозвідку», «кіберпростір», «кібертероризм», «кібершпигунство». Зосередимось на визначенні поняття кібертероризму, та звузимо коло термінів, які треба проаналізувати, також розглянемо історичний аспект кібертероризму, причини, що обумовили його виникнення, нормативно-правові засади боротьби з кібертероризмом. Взагалі «тероризм» (з лат. terror – страх, жах) за визначенням, наведеним словником сучасної української мови, – це найгостріша форма боротьби проти політичних і класових супротивників зі застосуванням насильства задля досягнення ідеологічної, політичної або релігійної мети. Характеризується особливою жорстокістю [11, с. 1242]. Тепер щодо терміну «кібертероризм». Якщо тлумачити широко – це загальнопланетарна загроза інформаційній безпеці людства. Поняття запропонував Баррі Коллін, науковий співробітник Institute for Security and Intelligence у Америці. Зокрема дане поняття дуже стисло тлумачить національне законодавство: «терористична діяльність, що здійснюється у кіберпросторі або з його використанням» [3]. Також тлумачать поняття «кібертероризму» міжнародні нормативно-правові акти, проекти конвенцій, наукові коментарі фахівців. Але переважно у вищезазначених джерелах висвітлюється лише одна сторона поняття, а саме аспект інформаційної безпеки та безпеки засобів обробки інформації. Єдиного підходу до визначення терору у кіберпросторі, якогось конкретного переліку його ознак у національному законодавстві не існує, але, узагальнюючи різноманітні наукові праці, за допомогою відомих кожному методів пізнання – порівняння, аналізу, синтезу та абстрагування можу вивести наступне – це навмисна, підкріплена злочинним мотивом, спрямована та несанкціонована атака на безпеку, конфіденційність, доступність, цілісність інформації, оброблюваної комп'ютером; на локальну чи підключену до Інтернету мережу; і спричинення дезорганізації у їх функціонуванні, дії спрямовані на порушення роботи серверів, що призводять до значних матеріальних збитків, становлять небезпеку для життя і здоров'я людини, інших суспільно небезпечних наслідків. Діяння скоюється з метою залякати населення, посягнути на громадську безпеку, впливу на органи державної влади задля виконання ними поставлених кібертерористами вимог, або просто привернути увагу до певної проблематики та викликати резонанс у ЗМІ, погіршення психологічного клімату в суспільстві.

Якщо перегорнути сторінки історії, можна знайти безліч згадок про терористичні акти минулого. Якщо висвітлювати їх всі – можна написати цілий трактат. Проте, обсяг даної статті обмежений регламентом, тож ми розкажемо про дві найвідоміші на нашу думку терористичні атаки в історії світового тероризму. А потім розглянемо основні етапи становлення безпосередньо кібертероризму. Зародки тероризму були зафіксовані в історичних джерелах ще у давні часи. Так, загальновідоме вбивство Юлія Цезаря Брутом та Касієм, науковці відносять до спрямованої терористичної атаки. А перша з відомих людству терористичних організацій з'явилася ще в 1 ст. н. е. і носила назву «сікарії». Дане організоване злочинне угруповання мало на меті боротьбу з римським пануванням, носило релігійний характер спрямування. Акти здійснювалися у світлі години доби і завжди увінчувались «успіхом» – великою кількістю постраждалих [10]. Все це знову підтверджує тезу, що недоліки людської природи супроводжують суспільство на всіх етапах його розвитку, і червоним маркером підкреслюють надзвичайну важливість здійснення превентивних заходів щодо виникнення злодіянь та призначення суворого покарання за них. Тепер стисло щодо віх розвитку кібертероризму. Науковці у своїх статтях виділяють такі етапи [4; 5], узагальнюючи їх можу навести такі: 1) 60-ті – 70-ті роки 20 ст. – злочини у кіберпросторі носять локальний характер та не несуть великої небезпеки; 2) 80-ті – 90-ті роки 20 ст. – комп'ютерні злочини зросли у кількісному та якісному показниках. Виникає субкультура хакерів, скоюється перший з зафіксованих кіберзлочинів, проведена перша широкомасштабна DoS атака; 3) 90-ті роки 20 ст. – наш час – кібератаки стають потужнішими, виникають терористичні організації, що застосовують високі інформаційні технології та саботують роботу публічних органів, корпоративних мереж, втручаються у роботу військових, проводяться шпигунські кібероперації, в штатах створено Консорціум з досліджень у галузі кібербезпеки, розроблений документ RFC 2196 щодо комп'ютерної безпеки в мережі Інтернет, створений комітет Cyber Security, прийнята після страшних терористичних актів 11 вересня Конвенція Ради Європи про кіберзлочинність.

Наразі кібертероризм є потужною та глобальною кримінальною галуззю, що спричиняє суспільству значну шкоду, приносить великі збитки державам, посягає на міжнародний мир та безпеку.Тепер щодо міжнародних нормативно-правових актів, які мають на меті протидіяти організованій кіберзлочинності та запобігати вчиненню кіберзлочинів. Основним документом є Конвенція Ради Європи по боротьбі з кіберзлочинністю. Організація Об'єднаних Націй у своїй Конвенції

проти транснаціональної організованої злочинності визначає злочини у сфері ІТ одним з переліку транснаціональних організованих злочинів [6]. Також варто зазначити, що оскільки кібертероризм є транснаціональним і транскордонним злочинним діянням і здійснюється у глобальному інформаційному просторі – Інтернеті, часто при розслідувані злочинів проти інформації виникає конфлікт юрисдикцій. Виникає крайня необхідність транскордонного співробітництва задля запобігання вчиненню даних діянь та мінімізації негативних наслідків від їх учинення. Якщо керуватися Конвенцією – при розслідуванні примат визнається за національним законодавством. Також, в рамках протидії організованій кіберзлочинності, у ЄС був створений Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre), відділення по боротьбі з кіберзлочинністю при Інтерполі, підрозділ по боротьбі з тероризмом при ОБСЄ. Україна, переймаючи досвід своїх зарубіжних колег, відкрила Департамент кіберполіції. Підрозділи кіберполіції України реалізують державну політику щодо запобігання та протидії кіберзлочинам, зокрема кібертероризму. А в рамках міжнародного співробітництва у протидії кібертероризму у 2018 році міністр внутрішніх справ України навідався з офіційним візитом до Сінгапуру, де вони разом з міністром внутрішніх справ приймаючої країни обговорили основні аспекти боротьби з кіберзагрозами та умови співпраці з Глобальним інноваційним комплексом Інтерполу у Сінгапурі [7]. У 2016 році задля безпеки користування кіберпростором, інформаційно-комунікаційними технологіями та протидії терористичним актам у електронному середовищі, зокрема щодо запобігання терористичним актам з боку країни агресора, набрало чинності рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Система кібербезпеки в країні складається з: Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України та ін. [8]. У червні 2017 року приватний та державний економічні сектори України атакував сумнозвісний вірус «Petya». Даний інцидент продемонстрував, що наша держава не в змозі оперативно реагувати на кібертерористичні акти і є зовсім беззахисною перед скерованими кібератаками. Того ж року за ініціативою депутатів був запропонований дуже дискусійний законопроект №6688, «Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері». Він мав визначити основні засоби протидії кібертероризму та значно розширити повноваження СБУ у кіберсфері, визначити основні поняття у галузі ІТ, внести зміни до Кримінального Кодексу і окреслити такий вид кримінальних заходів як блокування інформаційних систем. Але поряд з цим піднялося питання щодо обмеження даним актом свободи слова в Інтернеті. Тож законопроект ще потребує подальшого удосконалення [9].

Висновки з даного дослідження і перспективи розвитку. Переважна більшість з нас користуються мережею Інтернет, електронною поштою, мобільним телефоном, системою електропостачання, банками, системами відеонагляду, мобільним зв'язком тощо, та мало хто здогадується скільки спеціальних служб, сервісів, керуючих систем пристроїв (брандмауерів, антивірусів) сумлінно працюють задля забезпечення конфіденційності, схоронності інформації на кіберпросторах. Проте, як показує практика, Україна технічно абсолютно не готова до адекватної протидії спрямованим кібертерористичним атакам, а це стратегічно важливо, вдосконалювати засоби боротьби з кібертероризмом, задля економічної та політичної стабільності держави, національної безпеки загалом, особливо в умовах гібридної війни.

В Україні вже 12 років діє потужний орган з реагування на кіберзагрози «CERT-UA» – спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації, який співпрацює з Службою зовнішньої розвідки. Але методи кібертерористів постійно вдосконалюються, тож потрібне подальше вдосконалення існуючих засобів та методів протидії цій кіберзагрозі, розбудова інституцій з кіберзахисту, поглиблення міжнародного співробітництва у даній галузі, зокрема з НАТО та ЄС, з метою запозичення нових технологій в області кібербезпеки та перейняття зарубіжного досвіду, співпраця міністерств, відомств та підприємств у області віртуальної безпеки, а також інформування населення щодо основних заходів «кібергігієни». Необхідно далі аналізувати національне інформаційне законодавство та, можливо, підняти питання про прийняття нових нормативно-правових актів у цій сфері, які б узгодили та впорядкували існуючі поняття в галузі кіберпростору та звели їх до спільного знаменнику. Наприклад Кримінальний кодекс не регламентує поняття кібертероризму, тож воно розглядається на рівні зі звичайним тероризмом. Чи є дані поняття тотожними дослідникам ще належить з'ясувати. Кодекс виділяє у злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж і мереж електрозв'язку і перелічує їх у розділі шістнадцять. У міжнародних актах також немає єдності, комплексності у підході до визначення кібертероризму, а це ускладнює процес складання світових стратегій з кібербезпеки та міжнародного співробітництва загалом.

Список літератури:

1. Харламов П. Пігулка від хакерів: як бізнес захищає себе від кібератак. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak (дата звернення: 14.04.2019).
2. Сноуден накликав гнів США на Росію й Китай. URL: https://www.bbc.com/ukrainian/politics/2013/06/130625_snowden_usa_china_ko (дата звернення: 14.04.2019).
3. Про основні засади забезпечення кібербезпеки України : Закон України в редакції від 08.07.2018 р. № 2469-VIII. *Відомості Верховної Ради України.* 2018. № 31. Ст. 241. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 19.04.2019).

4. Гнатюк С.О. 2013. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security*, vol. 19, no 2.
5. Марків С.І. Кіберзлочинність. Нова кримінальна загроза. URL: http://gurt.org.ua/articles/34602/
6. Зозуля Є.В. Діяльність органів державної влади та управління України щодо нормативно-правового та організаційного забезпечення міжнародного співробітництва у боротьбі з кіберзлочинністю. *Наука. Релігія. Суспільство.* 2011. № 2. С. 54–60.
7. Підрозділи кіберполіції України та Сінгапуру співпрацюватимуть у протидії кібертероризму. URL: https://www.cyberpolice.gov.ua/news/pidrozdily-kiberpolicziyi-ukrayiny-ta-singapuru-spivpraczyuvatymut-u-protydiyi-kiberteroryzmu-6275/ (дата звернення: 17.04.2019).
8. Президент затвердив Стратегію кібербезпеки України. URL: https://www.president.gov.ua/news/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-36856 (дата звернення: 18.04.2019).
9. Зименко Є. Законопроект № 6688: боротьба з кібертероризмом чи впровадження цензури в Інтернеті? URL: http://yur-gazeta.com/publications/practice/inshe/zakonoproekt-6688-borotba-z-kiberterorizmom-chi-vprovadzhennya-cenzuri-v-interneti.html (дата звернення: 19.04.2019).
10. Степанченко О. Про історію тероризму на Близькому Сході. URL: https://islam.in.ua/ua/istoriya/pro-istoriyu-teroryzmu-na-blyzkomu-shodi (дата звернення: 20.04.2019).
11. Бусол В.Г. Великий тлумачний словник сучасної української мови. Ірпінь : Видавництво «Перун», 2003. С. 1242.

References:

1. Harlamov P. Pigulka vid hakeriv: yak biznes zahischae sebe vid kiberatak [The pill from hackers: how a business protects itself from cyber attack]. URL: https://mind.ua/publications/20192978-pigulka-vid-hakeriv-yak-biznes-zahishchae-sebe-vid-kiberatak (data zvernennya: 14.04.2019).
2. Snouden naklikav gniv SShA na Rosiyu y Kitay [Snowden has caused US anger against Russia and China]. URL: https://www.bbc.com/ukrainian/politics/2013/06/130625_snowden_usa_china_ko (data zvernennya: 14.04.2019).
3. Pro osnovni zasadi zabezpechennya kiberbezpeki Ukrayini : Zakon Ukrayini v redaktsiyi vId 08.07.2018 r. # 2469-VIII. *Vidomosti Verhovnoyi Radi Ukrayini.* 2018. # 31. St. 241. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (data zvernennya: 19.04.2019).
4. Gnatyuk S.O. (2013). Kiberterorizm: istoriya rozvitku, suchasni tendentsiyi ta kontrzahodi. [Cyberterorism: history of development, current trends and countermeasures]. *Ukrainian Scientific Journal of Information Security*, vol, 19, no 2.
5. MarkIv S.I. Kiberzlochinnist. Nova kriminalna zagroza [Cybercrime. New criminal threat]. URL: http://gurt.org.ua/articles/34602/
6. Zozulya E.V. (2011). Diyalnist organiv derzhavnoyi vladi ta upravlinnya Ukrayini schodo normativno-pravovogo ta organizatsiynogo zabezpechennya mizhnarodnogo spivrobitnitstva u borotbi z kiberzlochinnistyu [Activities of the bodies of state power and management of Ukraine concerning normative-legal and organizational support of international cooperation in the fight against cybercrime]. *Nauka. Religiya. Suspilstvo*, № 2, pp. 54–60.
7. Pidrozdili kiberpolitsiyi UkraYini ta Singapuru spivpratsyuvatimut u protidiyi kiberterorizmu [The cyberpolice units of Ukraine and Singapore will cooperate in countering cyberterrorism]. URL: https://www.cyberpolice.gov.ua/news/pidrozdily-kiberpolicziyi-ukrayiny-ta-singapuru-spivpraczyuvatymut-u-protydiyi-kiberteroryzmu-6275/ (data zvernennya: 17.04.2019).
8. Prezident zatverdiv Strategiyu kiberbezpeki Ukrayini [The President approved the Strategy of Cybersecurity of Ukraine]. URL: https://www.president.gov.ua/news/prezident-zatverdiv-strategiyu-kiberbezpeki-ukrayini-36856 (data zvernennya: 18.04.2019).
9. Zimenko E. Zakonoproekt № 6688: borotba z kiberterorizmom chi vprovadzhennya tsenzuri v Interneti? [Draft Law No. 6688: Fighting cyberterrorism or introducing censorship on the Internet?]. URL: http://yur-gazeta.com/publications/practice/inshe/zakonoproekt-6688-borotba-z-kiberterorizmom-chi-vprovadzhennya-cenzuri-v-interneti.html (data zvernennya: 19.04.2019).
10. Stepanchenko O. Pro istoriyu terorizmu na Blizkomu Shodi [About the History of Terrorism in the Middle East]. URL: https://islam.in.ua/ua/istoriya/pro-istoriyu-teroryzmu-na-blyzkomu-shodi (data zvernennya: 20.04.2019).
11. Busol V.G. (2003). Velikiy tlumachniy slovnik suchasnoyi ukrayinskoyi movi. [Great explanatory dictionary of modern Ukrainian language]. Irpen : Perun Publishing House, p. 1242. (in Ukrainian)