УДК 347:77
DOI https://doi.org/10.32782/2524-0374/2021-1/18

НЕОБХІДНІСТЬ УПРОВАДЖЕННЯ НА ЗАКОНОДАВЧОМУ РІВНІ ЗАСОБІВ ЗАХИСТУ ПРАВА НА ДОМЕННЕ ІМ'Я ВІД DOS (DDOS) АТАК В УКРАЇНІ

THE NEED TO IMPLEMENT AT THE LEGISLATIVE LEVEL MEANS OF PROTECTION OF THE RIGHT TO A DOMAIN NAME FROM DOS (DDOS) ATTACKS IN UKRAINE

Коваленко Я.І., аспірант
кафедри інтелектуальної власності та інформаційного права
Інститут права
Київського національного університету імені Т.Г. Шевченка

Найпоширенішими проблемами у сфері захисту права на доменне ім'я як у світі, так і в Україні є проблематика так званого «кіберсквотингу» та «тайпсквотингу». Проте більшістю провідних країн світу було вже вжито необхідних заходів для врегулювання цих питань, у т. ч. і в Україні, про що свідчить нещодавнє приєднання України, в особі реєстратора домену верхнього рівня «.UA» ТОВ «Хостмастерс», до договору з WIPO (Всесвітньої організації із захисту прав інтелектуальної власності), на підставі цього договору у користувачів і власників доменів рівня «.UA» з'явиться можливість вирішення доменних спорів на основі процедури, закріпленої UDRP [1], що за своєю природою має прискорити та зробити більш ефективним вирішення доменних спорів, які б виникали з приводу «кіберсквотингу» та «тайпсквотингу». Проте все ще залишається проблема DoS (DDOS) атак, хоч вона і є менш поширеною у сучасному світі, однак збитки, які можуть бути нанесені за допомогою такого протиправного діяння, є значно більшими, ніж ті, що можуть бути заподіяні «кіберсквотингом» і «тайпсквотингом». Сьогодні діяння, які б уособлювали DoS (DDOS) атаки, не закріплені у національному законодавстві, крім того, норми, які б мали кваліфікувати це діяння як злочин, є морально застарілими та не відповідають сьогоднішнім запитам суспільства, наприклад: Постанова Кабінету Міністрів України «Про затвердження порядку підключення до глобальних мереж передачі даних»; Закон України «Про телекомунікації»; статті Цивільного кодексу України та Кримінального кодексу України. Ці нормативні акти містять архаїчний підхід до визначення та кваліфікації DoS (DDOS) атак. З огляду на викладене вище автор вважає за доцільне на підставі аналізу законодавства зарубіжних країн і «кейсів» знайти єдиний підхід для розуміння (кваліфікації) DoS (DDOS) атак як протиправного діяння й виокремлення його з-поміж інших порушень у мережі Інтернет. Ще однією метою статті є ототожнення DoS (DDOS) атак як умисного протиправного діяння та ненавмисного діяння суб'єкта мережі Інтернет, наслідки яких є схожими за своєю природою.

Ключові слова: доменне ім'я, веб-сайт, реєстратор, реєстрант, інформаційні технології, DoS (DDOS) атака, IP-адреса.

The most common problems in the field of domain name protection both in the world and in Ukraine are the problems of so-called "cybersquatting" and "type squatting". However, most of the world's leading countries have already taken the necessary measures to resolve these issues, including in Ukraine, as evidenced by the recent accession of Ukraine, represented by the registrar of the top-level domain ".UA" LLC "Hostmasters", to the agreement with WIPO (World Intellectual Property Organization), on the basis of this agreement, users and owners of ".UA" domains will have the opportunity to resolve domain disputes based on the procedure established by the UDRP [1], which by its nature should speed up and make more effective resolution domain disputes that would arise over "cybersquatting" and "type squatting". However, the problem of DoS (DDOS) attacks still remains, although it is less common in the modern world, but the damage that can be caused by such an illegal act is much greater than that that can be caused by "cybersquatting" and "type squatting". Today, acts that would represent a DoS (DDOS) attack are not enshrined in national law, in addition, the rules that should qualify this act as a crime are morally outdated and do not meet today's demands of society, for example: Resolution of the Cabinet of Ministers of Ukraine "On approval of the procedure for connection to global data transmission networks"; Law of Ukraine "On Telecommunications"; articles of the Civil Code of Ukraine and the Criminal Code of Ukraine. These regulations contain an archaic approach to the definition and qualification of DoS (DDOS) attacks. Given the above, the author considers it appropriate on the basis of analysis of foreign legislation and "cases" to find a single approach to understanding (qualification) DoS (DDOS) attacks as an illegal act, and identify it among other violations on the Internet. Another purpose of this article is to identify DoS (DDOS) attacks as intentional wrongdoing and unintentional action by an Internet entity whose consequences are similar in nature.

Key words: domain name, website, registrar, registrant, information technology, DoS (DDOS) attack, IP address.

Постановка проблеми. На цьому етапі розвитку суспільства досить важко собі уявити людину, яка б ніколи не чула про всесвітню мережу Інтернет. У 21 ст. Інтернет відіграє важливу роль у повсякденному житті кожної особи, більшість мають свою персональну сторінку у соціальних мережах, створено мільйони різноманітних мессенджерів, майже щодня люди так чи інакше використовують здобутки інформаційних технологій для комунікації між собою. Такий же стан речей й у «світі бізнесу», адже зараз важко уявити хоча б якусь компанію, представника малого, середнього, або великого бізнесу, яка б не мала власного веб-сайту. Однак із розвитком інформаційних технологій як в Україні, так і в усьому світі починають з'являтися недобросовісні користувачі мережі Інтернет, котрі з метою недобросовісної конкуренції, а інколи і для розваги користуються прогалинами у системі всесвітньої мережі Інтернет для отримання певної переваги над свої конкурентами. Такий стан породжує чималу кількість суперечок щодо використання доменних імен.

За результатами вивчення й аналізу норм чинного вітчизняного законодавства, порівняння їх із нормами міжнародно-правових актів було виявлено основні напрями модернізації наявних приписів національного законодавства й обґрунтовано необхідність їх приведення у відповідність до загальносвітових тенденцій у сфері захисту права на доменне ім'я.

Аналіз останніх досліджень і публікацій. В Україні питання щодо пошуку шляхів застосування заходів юридичної відповідальності за здійснення DoS(DDOS)-атак до порушників, можливості захисту порушуваного права власників доменних імен досі належно не розкриті. Загалом проблеми, пов'язані з доменними іменами, розглядали такі вчені, як О.М. Андрусенко, Н.М. Булат, О.М. Коршакова, В.І. Грицай, О.М. Волощенко, С.С. Патрушев, К.Г. Татарникова та ін. Проте, на жаль, результати наукових дискусій не відображені в чинному законодавстві, а тому не вплинули на національну практику правозастосування у сфері захисту права на доменне ім'я. Наше дослідження проводилося на підставі аналізу іноземного досвіду правозастосування й особливостей правового регулювання, а також на роботах іноземних науковців та експертів, серед яких можна назвати таких авторів, як S. Agarwal, T. Dawson, C. Tryfonas, M. Broersma, D. Meyer, E. Messmer, S. Musil, J.P. Kleinhans, C. Thompson, C. Peterson, P. Vlissidis та ін.

Постановка завдання. На основі проведеного аналізу норм національного законодавства, а також міжнародних

актів у сфері регулювання правовідносин, що виникають із приводу захисту права на доменне ім'я, виокремити основні напрями, які б допомогли модернізувати та вдосконалити наявні в національній правовій системі засоби захисту такого права.

Виклад основного матеріалу. Якщо створення підґрунтя для розв'язання спірних правовідносин у правовідносинах щодо кіберсквотингу отримало в Україні позитивні результати, з огляду на укладений реєстратором домену верхнього рівня «.UA» ТОВ «Хостмастерс» та WIPO (Всесвітня організація з захисту прав інтелектуальної власності) договір, на підставі якого в домені «.UA» з'являється можливість для вирішення доменних спорів із використанням позасудової процедури на основі UDRP (Єдиної політики розв'язання доменних спорів), про що було повідомлено на конференції 7 грудня 2018 р. в Києві [1], то питання захисту права на доменне ім'я від DoS (DDOS) атак досі залишається не вирішеним в Україні.

DoS (DDOS) атака (англ. Denial of Service – «відмова в обслуговуванні») – це «напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена» [2]. Основною категорією DoS (DDOS) атак, яку використовують для недобросовісної конкуренції в мережі Інтернет, є атака на DNS-сервери; вони є за своєю суттю найпростішими та найефективнішими, основною метою таких атак є відмова в обслуговуванні DNS-сервера шляхом перенавантаження смуги пропускання або за допомогою захвату системних ресурсів. Проте така атака потребує великої кількості ресурсів, а саме комп'ютерів-зомбі. Комп'ютер-зомбі – у програмуванні таку назву має комп'ютер, який підключений до мережі Інтернет, заражений внаслідок хакерської атаки комп'ютерним вірусом і який може бути використаний зловмисниками для виконання різних задач, без відома власника комп'ютера, адже хакери (зловмисники) можуть мати віддалений доступ до «зараженого» комп'ютера [3]. Найпоширеніший приклад «комп'ютерів-зомбі» – це так званий «ботнет», коли через заражені комп'ютери без відома власника виконується розповсюдження спаму (розсилка рекламних листів через електронну пошту, оголошень тощо). Такі комп'ютери далі використовуються зловмисниками для проведення DoS-атак. Майже ніхто із власників не знає про те, що його комп'ютер було заражено та використано для розсилки спаму або інших протиправних дій.

Щодо самих DOS-атак, то через їх проведення користувачі мережі Інтернет, наприклад, не можуть потрапити на потрібну їм «веб-сторінку», тому що DNS-сервер не може перетворити доменне ім'я в IP-адресу сайту, але сьогодні атаки на DNS-сервери за допомогою комп'ютерів-зомбі є майже не актуальними, оскільки Інтернет-провайдери (постачальники Інтернет-послуг) швидко помічають непомірну кількість вихідного трафіку і проводять його блокування. Хакери або «зловмисники» тепер обходяться невеликою кількістю «комп'ютерів-зомбі» або не використовують їх зовсім. Нині вони використовують DNS-сервери [4], а саме прогалини в їх системі [5]. Для накопичення та збільшення сили атаки «зловмисник» збільшує «фіктивно» кількість DNS-запитів. Переважно це явище існує як наслідок не ідеальності DNS-серверів, адже у взірцевому випадку DNS-сервер окремого провайдера має приймати лише ті запити, які надходять йому від клієнтів (користувачів). У світі є велика кількість неправильно (некоректно) налаштованих DNS-серверів, які, на жаль, приймають запити від будь-якого користувача мережі Інтернет. Основою DDOS (DoS) атак є підміна кінцевої адреси, на яку користувач надсилає запит на адресу «жертви», домену, котрий «зловмисники» хочуть вивести з ладу. Через недосконаліть і неправильну налаштованість DNS-серверу «зловмисник» шле запит, з умовою, що відповідь від кінцевого адресата мала якомога більший обсяг інформації (наприклад, список всіх записів у таблиці DNS), у якому адреса (IP-адреса), на яку мала надійти відповідь на запит, замінюється на адресу жертви. Зазвичай DNS-сервери мають досить велику пропускну здатність, а тому атака у «зловмисника» не викликає жодних труднощів [6].

Отже, для того, щоб зрозуміти, як вдосконалити засоби захисту права на доменне ім'я, насамперед слід з'ясувати, чим є «інтернет», «веб-сайт» і «доменне ім'я», «DNS-сервер» і який взаємозв'язок між ними.

Поняття «веб-сайт» закріплено у ст. 1 Закону України «Про авторські та суміжні права» й означає «сукупність даних, електронної (цифрової) інформації, інших об'єктів авторського права і (або) суміжних прав тощо, пов'язаних між собою і структурованих у межах адреси веб-сайту і (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики і (або) числової адреси за Інтернет-протоколом» [7].

У свою чергу, закріплення понять серверу та веб-серверу у Постанові Кабінету Міністрів України «Про затвердження порядку підключення до глобальних мереж передачі даних» (п. 2) [8], дають підстави стверджувати про закріплення за кожним веб-сайтом у мережі Інтернет своєї адреси. Визначення останньої містить у законі України «Про телекомунікації» (ст. 1) й означає «визначений чинними в Інтернеті міжнародними стандартами цифровий та/або символьний ідентифікатор доменних імен в ієрархічній системі доменних назв» [9]. Окрім цього, закон розкриває поняття «домен», що деталізовано у постанові Кабінету Міністрів України «Про затвердження порядку підключення до глобальних мереж передачі даних».

DNS (Domain Name System) – це система доменних імен, яка пов'язує назви доменів з IP-адресами комп'ютерів, які відповідають цим доменам. Ця система включає в себе як регламентуючі документи, так і безліч DNS-серверів, що працюють в Інтернеті та повідомляють IP-адреси у відповідь на запит по доменних іменах [10].

IP-адреса (англ. Internet Protocol Address) – мережева адреса вузла в комп'ютерній мережі Інтернет [11].

Узагальнюючи всю наведену інформацію, можна зробити висновок, що домен (доменне ім'я) є унікальним набором символів, окремо закріпленим за кожним веб-сайтом, обслуговується DNS-сервером (частіше, оскільки перетворює доменну адресу (IP-адресу) з цифрового вигляду на символьно-цифровий), або веб-сервером (після обробки запиту DNS-сервером і перетворення домену (IP-адреси) із цифрових позначень на символьно-цифровий, або відразу, якщо запит йде на цифрову адресу і використовується для ідентифікації веб-сайту або доступу до нього у всесвітній мережі Інтернет.

Слід констатувати, що в Україні допоки не передбачено відповідальності для «зловмисників» за використання DDOS-атак. Фактично метою проведення DDOS-атаки є позбавлення силою суб'єкта («жертви») можливості користуватися певним ресурсом, у цьому разі це веб-сайт (домен).

При аналізі DDOS атак і способів захисту прав постраждалої особи в контексті міжнародно-правового регулювання істотну увагу було приділено розкриттю змісту принципу, закріпленого п. 4 ст. 2 Статуту ООН [12], а саме «принципу заборони застосування сили». На жаль, цей принцип не може бути використаний у контексті нашого розгляду, адже «тимчасова відмова служби навряд чи класифікується як застосування сили» [13, правило 11, п. 10]. Проте DDOS-атака може бути порушенням закону про невтручання та недоторканність суверенітету, наприклад, «DDOS-атака щодо державного військового супутника є беззаперечним порушенням суверенітету держави» [13, правило 4, п. 4]. Якщо розглядати DDOS-атаку в контексті екології, то це є ніщо інше як «забруднення» або транскордонні «викиди» [14].

Комітет Конвенції Європейського Союзу з питань кіберзлочинності криміналізує випадки DDoS у Настановах № 5 T-CY, а саме ст. 2, 4, 5, 11, 13 [16].

Подібний підхід закріплюється й у багатьох національних законоавствах. Так, законом Великої Британії «Про зловживання комп'ютером» 1990 р. забороняються DDOS-атаки; особам, які винні в їх проведенні, загрожує до 10 років в'язниці [17].

В Австралії DDoS, як і будь-яке інше високотехнологічне правопорушення, регулюється законодавством Співдружності в ч. 10.7. Комп'ютерні правопорушення, включеним до кримінального кодексу 1995 р. Загалом ці питання підпорядковуються австралійській поліції, коли постраждалі комп'ютер, система чи сервер перебувають в Австралії або серед залучених осіб є громадянин Австралії [15].

У Сполучених Штатах люди, які беруть участь в атаках DDoS, ризикують бути звинуваченими в юридичних правопорушеннях на федеральному рівні, як кримінально, так і цивільно відповідно до Закону «Про комп'ютерні шахрайства та зловживання» (CFAA). Щоб людина порушила CFAA, вона повинна навмисно завдати шкоди комп'ютерній системі, що належить до міждержавної чи зовнішньої торгівлі; спроби DDoS-атак також можуть бути притягнуті до кримінальної відповідальності [18].

Сторони, які всупереч своєму волевиявленню відіграють роль посередника у векторі DDoS-атаки, такі як Інтернет-провайдери, можуть також вимагати відшкодування цивільних зборів для відшкодування своїх фінансових втрат на підставі порушення пункту договору «умови надання послуг», що, до речі, відображаються в кожному юридичному договорі. Вагомі порушення можуть призвести до судового позову за порушення договору і навіть до ув'язнення на строк, встановлений законодавством.

Крім того, DDOS-атаки мають вплив не тільки на свою «жертву», а й на осіб, на яких вони спрямовані не були. Для того, щоб підтвердити цю думку, що насправді DDoS-атаки мають чимало побічних ефектів, які можуть впливати на суб'єктів, котрі не є ціллю, пропонується той факт, що деякі засоби та методи DDOS-атак блокують законних користувачів або є підгрунтям для шахрайства. Наприклад, оповіщення на основі нефункціональних посилань, вичерпаних потоків, відеопотоків, а також повільне завантаження вебсайту. Як стверджує експерт із питань безпеки DDoS Барретт Ліон із цього приводу: «Деяким компаніям довелося ігнорувати свої сповіщення про шахрайство, коли вони перебували під DDoS-атакою, оскільки внаслідок неконтрольованої розсилки push-повідомлень вони самі могли розцінюватися як «зловмисники», які проводять таку атаку» [19, пар. 11].

Ще одним прикладом може слугувати особа, котра на Інтернет-дискусійному форумі під псевдонімом «Nightmare» поскаржилася, що на її компанію раз у раз проводиться DDoS-атака, внаслідок чого вона змушена звернутися до спеціалізованого захисту від DDoS. Проблема однак полягає в тому, що щоразу, коли захист від DDOS перебуває в активному режимі, законні користувачі не можуть увійти на її веб-сайт, що побічно є частковим ефектом відмови у наданні послуг [20]. Можливо, конкретна загроза в цьому разі є незначною з погляду пошуку рішення, але це свідчить про те, що DDoS-атака може впливати на IT-системи різними таємничими способами, тим самим залишаючи безліч невивчених цілей.

Поряд із цим експерти з питань безпеки стверджують, що атаки DDoS «також можуть завдати серйозної шкоди системам BACK END» [21]. Роблячи таку заяву, експерт посилається на юридичну фірму ACS.Law, роботу веб-сайту якої було припинено у 2010 р., за наслідком DDOS-атаки «хакерської групи 4chan». Після відновлення їх веб-сайту на головній сторінці з'явився файл резервної копії, вагою 350 Мб. Розглянутий файл, розповсюджений пізніше по мережі, містив конфіденційну інформацію про тисячі користувачів Інтернету, в т. ч. стосовно клієнтів фірми та їхньої конфіденційної інформації [22].

Наслідки можуть досягати зловісних масштабів, якщо судити за оцінкою, наданою радником конфіденційності О. Ханфом: «DDOS-атака може призвести до значної шкоди десяткам тисяч людей, а саме у вигляді шахрайства, крадіжок у осіб і, як результат, сильних емоційних наслідків» [23].

Щоб зрозуміти масштаб DDOS-атаки, можна розглянути приклад небезпечної тенденції, коли атака DDoS спочатку запускається для того, щоб відволікти увагу, піддається бурхливому розвиту, проте, на перший погляд, є непомітною (наприклад, надзвичайна велика активність на форумі якогось із веб-сайтів). Проте насправді це є первинним кроком, наприклад, такою «тактикою» користувалися Ганнібал Барка та Жуков.

Такі DDOS-атака вразила Sony та кілька банків США. Згідно з повідомленням, опублікованим відділом протидії погрозам «Dell Secure Works», така тактика використовувалася як «прикриваючий вогонь», тоді як «зловмисники» намагалися виконати шахрайський переказ коштів, який оцінюється до 2,1 млн доларів [24] Очевидно, що «атаки DDoS, ймовірно, використовувалися як відволікання банківського персоналу, щоб запобігти негайному виявленню шахрайської операції, яка здебільшого необхідна для припинення банківського переказу» [24].

Також не секрет, що DDoS-атаки ускладнюють ведення бізнесу, якщо не унеможливлюють. Цей побічний ефект відчули: 1) банки – наприклад, HSBC, Wells Fargo, Capital One, Bank of America, Sun Trust тощо; 2) інші фінансові установи – наприклад, Visa, MasterCard тощо; 3) уряди – практично кожен провідний уряд (сайт ФБР; Білого Дому); 4) медіа – наприклад, WikiLeaks і Virgin Media.

І цей перелік не є вичерпним. Вплив на бізнес із погляду грошових втрат, зниження довіри, загального бентежного розголосу тощо є величезним. Переважно DDoS-атаки настільки широко розповсюджені, що це явище бере свій початок із моменту, коли людина змогла його ідентифікувати, можна сказати, що воно є всюдисущим.

Парадоксальним у цьому питанні є також те, що деякі особи, котрі самі себе називають «хактивісти», не сприймають проведення DDOS-атаки як злочину, який порушує право іншої особи на доменне ім'я. Так звані «хактивісти» зазначають, що атаки DDoS були використані ними для проведення «мирних Інтернет-зібрань», а тому засудження за такі дії є порушенням Першої поправки та права на свободи зібрань і висловлювань. Мета громадянського непокори є зовсім протилежною: спровокувати суспільство, політиків, законодавців тощо, розпалити моральний діалог, який може призвести до тривалих змін [25]. Ці особи повністю ігнорують той факт, що DDOS-атака у більшості країн світу є кібер-злочином, за який передбачена кримінальна відповідальність, а також той факт, що від їхніх дій першочергово страждає власник веб-сайту (домену), а також право інших осіб на доступ до інформації, яка була або могла бути розміщена на «атакованому» веб-сайті.

Важливо наголосити, що всі описані злочини з використанням DDOS-атак є виявленими й описаними на територіях країн, де за це правопорушення передбачено чітко визначену юридичну відповідальність, починаючи від кримінальної та закінчуючи цивільної. Проте, якщо аналізувати вітчизняне законодавство, то ним не визначено відповідальність для зловмисників, які використали такий інструмент; не визначено суб'єктний склад правопорушників, предмет правопорушення / злочину, визначення складу злочину, а також його розмежування між цивільною, кримінальною або адміністративною відповідальністю, відсутній механізм виявлення та доведення факту скоєння описаного вище правопорушення та механізм захисту, відновлення порушеного права. Крім того, в чинному законодавстві України не закріплені поняття «DNS-сервер», «DoS (DDOS) атака» або поняття, які хоча б якось могли допомогти притягнути до відповідальності «зловмисників», котрі були б винні у проведенні DDOS-атак.

Щоб ще раз підкреслити необхідність впровадження та закріплення цивільно-правових і кримінально-правових санкцій у національному законодавстві за проведення DDOS-атак, у статті буде приведено ще декілька прикладів, коли DDOS-атаки були причиною збитків окремих компаній.

Насамперед слід згадати справу «Lufthansa», рішення в якій відповідає стандарту того, що в судовій практиці відомо як «прецедент». Історія починається у 2001 р., коли активіст Фогель прийняв рішення про проведення онлайн-протесту проти практики німецького перевізника дозволяти місцевим органам влади використовувати свій літак для видачі біженцям притулку. Ним було розміщено повідомлення «Місцем зборів є www.lufthansa.com»; також він зазначив, що «згідно зі ст. 8 німецької конституції всі німці мають право збиратися без попереднього повідомлення або дозволу мирно і без зброї». У визначений активістом Фогелем час близько 13 000 користувачів Інтернету відвідали сайт, щоб взяти участь у протесті Фогеля. Створене таким чином зібрання демонстрантів фактично позбавило всіх користувачів можливості перейти на цей веб-сайт. Проте згодом нормальне функціонування веб-сайту відновлюється.

На цьому історія не закінчується, тому що «Lufthansa» порушила кримінальну справу щодо Фогеля, а прокуратура Франкфурта, яка була стороною звинувачення, порушила обвинувальний акт проти Фогеля та інших активістів. Захист пообіцяв, що вся подія – це не що інше, як протест, який проводився в Інтернеті. При ухваленні рішення у справі суд ґрунтувався на ухвалі Федерального конституційного суду Німеччини від 1995 р., в якій зазначалося, що блокування доступу до місця само по собі не є застосуванням фізичної сили, яка вимагає примусу. Апеляційний суд підтвердив рішення першої інстанції та залишив його без змін. За наслідками розгляду Фогеля було виправдано, та не притягнуто до будь-якої відповідальності.

Якщо розглядати цю ситуацію прагматично, то проведене Фогелем «зібрання», теоретично має всі ознаки кібер-злочину, яке порушило права компанії «Lufthansa» щодо їхнього веб-сайту (доменного імені).

У разі доведення Франкфуртською прокуратурою умислу Фогеля провести DDOS-атаку з метою блокування сайту «Lufthansa», швидше за все його було б притягнуто до кримінальної відповідальності. Недоведення умислу Фогеля та неможливість ототожнення права «на мирне зібрання» із «кібер-злочином DDOS-атакою» свідчить про відсутність механізму розслідування таких правопорушень і запобігання їм.

У противагу рішенню німецьких судів пропонується до уваги обвинувальний акт у справі, яка знаходиться у провадженні суду США, стосовно членів «хакерського» угрупування «Anonymous». Шістнадцять можливих членів «Anonymous» були заарештовані за їхню участь у DDOS-атаці на PayPal, і їм загрожує понад 10 років в'язниці та 250 000 доларів штрафу. Підставою для їх звинувачення є припис CFAA, а саме змова та «навмисне пошкодження захищеного комп'ютера» [26].

Очевидно, що можливий вирок у цій справі не йде у порівняння з результатом справи «Lufthansa». На думку експертів, «непропорційність є просто приголомшливою, і необхідно провести калібрування покарань, виходячи з моральної цінності дискусійної DDOS-атаки» [27].

Висновки. Підсумовуючи викладене вище, слід відзначити, що нині не існує єдиної практики захисту права на доменне ім'я в контексті захисту від DDOS-атак. Як засвідчує практика, певні рішення у справах стосовно DDOS-атак, які не несли шахрайського умислу або умислу навмисно завдати економічних збитків «жертві» такої атаки, мали виправдувальний характер. Проте все ж таки вважаємо за необхідне змістовно розширити нормативно-правові акти, якими регулюються відносини у сфері захисту права на доменне ім'я, а саме доповнити п. 2 Постанови Кабінету Міністрів України «Про затвердження порядку підключення до глобальних мереж передачі даних» і ст. 1 Закону України «Про телекомунікації» поняттями «IP-адреса», «DNS-сервер». Також слід внести зміни у відповідні статті чинних Цивільного кодексу України та Кримінального кодексу України, за прикладом закону CFAA (США), аби передбачити відповідальність за проведення «зловмисниками» DDOS-атак, ціллю яких було шахрайство або навмисне позбавлення осіб доступу до певного веб-ресурсу.

ЛІТЕРАТУРА

1. Досудове вирішення спорів та інші анонси на конференції UADOM – 2018. URL: https://uadom.cctld.ua.
2. DoS-атака. Википедия – свободная енциклопедия. URL: https://ru.wikipedia.org/wiki/DoS-атака.
3. Компьютер-зомби. Википедия – свободная енциклопедия. URL: https://ru.wikipedia.org/wiki/Компьютер-зомби.
4. Eddy, W. TCP SYN Flooding Attacks and Common Mitigations. 2007. URL: https://tools.ietf.org/html/rfc4987.
5. McLEAN, A., Gates, G., Tse, AHow the Cyberattack on Spamhaus Unfolded. 2013. URL: https://archive.nytimes.com/www.nytimes.com/interactive/2013/03/30/technology/how-the-cyberattack-on-spamhaus-unfolded.html?_r=0
6. Agarwal, S., Dawson, T., Tryfonas, C. DDoS Mitigation via Regional Cleaning Centers. 2011. URL: https://research.sprintlabs.com/publications/uploads/RR04-ATL-013177.pdf.
7. Закон України «Про авторські та суміжні права» № 3793-XII від 23 грудня 1993 р., в редакції Закону № 2627-III від 11 липня 2001 р., із змінами. URL: https://zakon.rada.gov.ua/laws/show/3792-12.
8. Постанова Кабінету Міністрів України «Про затвердження порядку підключення до глобальних мереж передачі даних» від 12 квітня 2002 р. № 522. URL: https://zakon.rada.gov.ua/laws/show/522-2002-%D0%BF#Text.
9. Закон України «Про телекомунікації» № 1280-IV від 18 листопада 2003 р., із змінами. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text.
10. Что такое DNS. URL: https://1cloud.ru/blog/chto-takoe-dns.
11. Понятие и классификация IP адресов. URL: https://hyperhost.ua/ru/wiki/chto-takoe-ip-adres-kakie-tipy-byvayut.
12. United Nations. United Nations Charter. 1945. URL: http://www.un.org/en/documents/charter/.
13. The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual on the International Law Applicable to Cyber Warfare. 2012. URL: http://www.ccdcoe.org/249.html.
14. Healey J., Pitts H. Applying International Environmental Legal. 2012. URL: https://kb.osu.edu/bitstream/handle/1811/73113/ISJLP_V8N2_356.pdf?sequence=1.
15. Criminal Code Act 1995. URL: https://www.legislation.gov.au/Details/C2019C00043.
16. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575.
17. Computer misuse act. 1990. URL: http://www.legislation.gov.uk/ukpga/1990/18/contents.
18. Computer Fraud and Abuse Act. URL: https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ccmanual.pdf.
19. Messmer, E. Start-up Defense. Net debuts with anti-DDoS service. 2013. URL: http://www.networkworld.com/news/2013/080613-defense-net-272464.html
20. "Nightmare" forum user. Side Effects Of DDOS Protection? 2012. URL: http://ngemu.com/threads/side-effects-of-ddos-protection.148097/.
21. Vlissidis, P. Comment: preparing for DDoS in the legal sector. 2013. URL: http://www.legaltechnology.com/latest-news/comment-preparing-for-ddos-in-the-legal-sector/
22. Broersma, M. File-Share Law Firm Exposes Personal Data. 2010. URL: http://www.techweekeurope.co.uk/news/file-sharing-law-firm-exposes-personal-data-10071
23. Meyer, D. Privacy group takes on ACS: Law over porn data breach. 2010. URL: http://www.zdnet.com/privacy-group-takes-on-acslaw-over-porn-data-breach-3040090288/.
24. Musil, S. Cybercrooks use DDoS attacks to mask theft of banks' millions. 2013. URL: http://news.cnet.com/8301-1009_3-57599646-83/cybercrooks-use-ddos-attacks-to-mask-theft-of-banks-millions/.
25. Kleinhans, J.P. Why are Gandhi and Thoreau AFK? In search for civil disobedience online. 2013. URL: http://www.diva-portal.org/smash/get/diva2:639597/FULLTEXT01.pdf.
26. Thompson, C. Hacktivism: Civil Disobedience or Cyber Crime? 2013. URL: http://www.propublica.org/article/hacktivism-civil-disobedience-or-cyber-crime
27. Peterson, C. In Praise of [Some] DDoSs? 2009. URL: http://www.cpeterson.org/2009/07/21/in-praise-of-some-ddoss/.