УДК 347:77
DOI https://doi.org/10.32782/ln.2023.21.06

Горшкова О.О.
суддя
Харківський окружний адміністративний суд

Тайхманн Фабіан
доктор юридичних наук, доктор економічних наук,
адвокат, нотаріус, LL.M.

ДОСВІД ПРОТИДІЇ DDOS-АТАКАМ В УКРАЇНІ: ОКРЕМІ ПРАВОВІ АСПЕКТИ

Стрімкий розвиток інформаційних технологій та масової комп'ютеризації призвели до еволюційних змін кримінального середовища не тільки на рівні окремих держав, а й у всьому світовому співтоваристві. Відсутність належного контролю суспільних відносин у зазначеній сфері призвело до того, що мережа Інтернет практично безкарно стала використовуватися як місце і основний засіб вчинення різних правопорушень, в тому числі, кримінально караних. Особливо важливим питання протидії протиправним практикам у сфері інформаційного простору постало в умовах активного процесу діджиталізації на всіх рівнях влади та бізнесу в Україні в умовах повномасштабного вторгнення.

Варто визнати, що кібератаки сьогодні в окремих своїх проявах на ряду з реальними збройними нападами завдають значної шкоди охоронюваним інтересам в державі, в цілому, та національній безпеці, зокрема. Гаджети та Інтернет-мережа активно інтегруються в функціонування суспільства, більшість платформ державного управління, комунікації та взаємодії переноситься в онлайн, що особливо актуально в часи воєнного стану, а відтак нормальне функціонування відповідних сервісів забезпечують стабільну роботу як органів влади, так і приватних структур, порушення чого може призвести до значних збитків. Досить поширеним методом такого виведення із ладу є перенавантаження, тобто навантаження окремого веб-ресурсу, поки останній не стане недоступний. Такий процес отримав назву – DoS-атака (англ. Denial of service attack – атака до відмови сервісу). У даному доробку пропонується проаналізувати суть цього явища як протиправної практики та національні організаційно-правові основи протидії йому.

В Україні питання щодо пошуку шляхів застосування заходів юридичної відповідальності за здійснення DoS (DDoS)-атак до порушників, протидії даним протиправним практикам розглядали О.М. Андрусенко, Н.М. Булат, О.М. Коршакова, В.І. Грицай, О.М. Волощенко, С.С. Патрушев, К.Г. Татарникова та інші, однак комплексно дана проблема так і залишається невирішеною, що актуалізує як науково-теоретичні пошуки, так і висвітлення практичного погляду з окресленої теми.

Організаційно-правова структура протидії DDoS-атакам включає в себе функціонування відповідних державних органів, технічні та правові засоби. Так, першочергово слід відзначити, що національний досвід у зазначеній сфері містить функціонування кіберполіції та Держспецзв'язку, як одного із основних суб'єктів кібербезпеки України, відповідального за кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, за координацію діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту. Подібний орган діє в Швейцарії під назвою Швейцарський Національний центр кібербезпеки (NCSC).

Дослідженню технічних та правових аспектів протидії вказаному явище повинне передувати з'ясування суті даного явища та його ознак, механізму дії.

У науковій літературі зазначається, що «DDoS-атака або атака типу «відмова в обслуговуванні» (Distributed Denial of Service) спрямована на комп'ютерну систему з метою створення несприятливих умов для використання певних ресурсів або сервісів користувачами» [1].

Як слушно відмічається у зарубіжній науковій літературі (Teichmann F.), розподілені атаки типу «відмова в обслуговуванні» (DDoS) – це мережна спроба зробити веб-сайт або службу недоступними шляхом навантаження сервера трафіком. Іншими словами, це швидка комерціалізація пропускної спроможності мережі. DDoS-атака може бути спрямована безпосередньо на передбачувану функціональність програмного забезпечення, перенаправляти трафік, видаючи себе за підроблений веб-сайт, або використовувати об'ємну атаку з великим обсягом даних, що заповнюють сервер [2].

DoS (DDoS) атака трактується також як «напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена; 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» [3].

В цілому, суть DDoS-атаки полягає в масовому надсиланні на атакований комп'ютер або мережеве обладнання великої кількості зовнішніх запитів. Вони можуть не мати сенсу або бути сформульованими некоректно лише заради того, щоб ціль прийняла запит і почала його обробляти. І через те, що атаковане устаткування в короткий проміжок часу намагається опрацьовувати занадто велику кількість запитів, то його робота значно уповільнюється або повністю припиняється.

Основні класи атак на сьогодні є досить детально вивчені, однак, попри це, існують різні підходи їх класифікації. Наприклад, у звіті Prolexic Technologies пропонується класифікувати DDoS-атаки на три основні типи атак: 1) targeted attacks (використовують недоліки в протоколах, прикладних програмах); 2) consumption attacks (поглинання ресурсів системи); 3) exploitative attacks (використовують вразливості, помилки кода) [4].

Також пропонується атаки класифікувати згідно з протоколами, за якими вони здійснюються, на основі чого DDoS-атаки поділяють на: «SYN flood, TCP reset, ICMP flood, UDP flood, DNS request, CGI request, Mail bomb, ARP storm і атаки на алгоритмічну складність» [5].

В цілому прийнято розділяти розподілені атаки на відмову (за способом реалізації і об'єкту дії) на два класи: поглинання ресурсів мережі, що полягає в пересилці великої кількості пакетів в мережу жертви, що зменшує пропускну здатність для законних користувачів, та поглинання ресурсів вузла (полягає в пересилці «важких» або некоректних запитів жертві).

Як слушно підмічають Ф. Тайхман, С. Бруно та С. Віттман, «за хакерською атакою стоїть намір. У цьому контексті хакерів також називають акторами загроз. Це може бути будь-хто: від незадоволеного колишнього співробітника до вороже налаштованих національних держав та політичних вандалів з явною метою нападу. Розумно припустити, що є не тільки намір викликати хаос, хоча це не є строго необхідним» [2].

Наприклад, останніми із наймасовіших DDoS-атак проти банківського сектору, офіційних сайтів органів влади, енергетичного блоку та порталу «Дія» в Україні мала місце в ніч з 13 на 14 січня та 15 лютого 2022 року.

Крім того, часто метою DDoS-атак є викрадення персональних даних. Зауважується, що

«наявність етичних проблем щодо захисту даних стає все більш очевидною в міжнародному законодавстві. Загалом 137 країн ухвалили закони, які забезпечують захист даних та конфіденційності. У світлі цих нормативних змін, що сприяють чіткішому етичному розмежуванню, серйозність наслідків DDoS-атак для захисту даних зростає» [2].

Урядовцями відмічається, що «завдяки сучасним антиDDoS-інструментам була змога оперативно відбити атаку на портал «Дія», відбувалася фільтрація іноземного трафіку, вимкнення та відновлення роботи» [6]. Обидві атаки були добре скоординовані й схожі за своєю потужністю, зухвалістю та безпрецедентністю.

У травні 2022 року хакери здійснили масштабну DDoS-атаку на сайти провідних телекомунікаційних компаній України, що було направлено на виведення з ладу інфраструктури мережі операторів, під час якої спостерігалася часткова недоступність веб-сайтів та деяке погіршення якості доступу до мережі Інтернет. Однак, відповідні спеціалісти таких компаній вдало та швидко відбили кібернаступ за допомогою налаштованої ефективної системи кіберзахисту.

Окремо варто відмітити активність DDos-атак, направлених проти роботи енергетичної структури в Україні, так за перші місяці військової агресії НЕК «Укренерго» зазнало 10-кратне збільшення подібних атак, а ніж в попередні п’ять років [7].

Влітку 2022 року було атаковано сайти Державної служби України з безпеки на транспорті, які забезпечують роботу прикордонної інфраструктури, сервера системи «Шлях» й електронної пошти та документообігу, через що рух пасажирського та вантажного транспорту здійснювався без доступу до цих ресурсів [8]. З метою протидії вказаної DDoS-атакам представниками Укртрансбезпеки було вжиту цілу низку заходів протидії, однак все ж були змушені закрити систему «Шлях», базу даних заявок на перетин кордону водіями певних категорій, реєстри Ліцензіатів та МС, реєстр дозволів на міжнародні перевезення та реєстр поїздок Європейської Конференції Міністрів Транспорту. Таке рішення все ж призвело до тимчасового ускладнення руху автотранспорту на міжнародних пунктах пропуску.

12 грудня 2023 року мобільний оператор «Київстар» заявив про масштабний збій в роботі через хакерську атаку на ядро мережі, що призвело як до відсутності роботи самої мережі, так і до неможливості абонентів перейти до інших операторів. В цей же час подібним атакам була банківську систему Монобанк та додаток Vodafon. Під загрозою персональні дані абонентів. Окрім того, виникає потреба відшкодування завданих збитків абонентам та клієнтам через відсутність можливості скористатися послугами та сервісами операторів. Відповідно такі ситуації вимагають як технічного забезпечення та відновлення, так і належної правової оцінки із застосуванням заходів правового впливу.

На сьогодні, сучасний арсенал засобів та методів протидії DDoS-атакам в Україні є досить значним та ефективним, що демонструється на практиці, особливо в умовах гібридної війни та постійних посягань в інформаційному просторі.

Загалом, можливо поділити підходи протидії DDoS-атакам на технічні та правові. Серед перших виокремлюють пасивні та активні, а також на превентивні та реакційні.

Звісно, першочергово варто використовувати весь профілактичний арсенал можливих заходів протидії, що є найбільш ефективною тактикою захисту від кібератак. Звісно, профілактичний метод є управлінським, тим не менш аналіз можливих причин імовірних DDoS-атак є першим кроком до зменшення їх руйнівних наслідків.

Відмічається ефективність «методів фільтрації за списками ACL (Access Control List) та використання мережевих екранів, що дає можливість зменшити та зупинити атаку, перенаправивши трафік на атакуючі комп’ютерні системи, таку тактику ще називають «ботнет»

(використання заражених комп'ютерних систем)» [9].

Також, із технічних методів протидії DDoS-атакам «не менш діючим є механізм оновлення системного та прикладного програмного забезпечення з можливістю повернення до попередньої версії, оскільки адже виявлення та виправлення недоліків серед цього класу програмного забезпечення проходить достатню кількість перевірок фахівцями різного рівня та спеціалізацій» [10].

У науково-технічній літературі звертається увага на доцільність використання систем розподіленого захисту як одного із ефективних комплексних методів протидії аналізованим видам кібератак. З метою впровадження даного захисту необхідне обладнання встановлюється у магістральних операторів, і якщо аналізатор атак фіксує напад на хост, або сервер, що захищається, він моментально транслює адреси атакуючих хостів іншим вузлам по всій мережі, і мережа починає працювати проти атакуючих хостів. Подібна система здатна відбити DDoS-атаки великої потужності. Що часто використовується для захисту владних інформаційних ресурсів в Україні.

Найбільш високопродуктивним і ефективним вважається застосування апаратних систем розподіленого захисту [11]. Наприклад, A10 Networks Thunder Threat Protection System володіє такими характеристиками як: «автоматичний розрахунок фільтрів блокування та аналіз без попереднього налаштування або ручного втручання з подальшим блокуванням аномальної поведінки; 5-рівнева адаптивна ескалація політики, захист на основі машинного навчання; інтелектуальне виявлення сервісів з автоматичним призначенням політики пом'якшення наслідків; захист застосунків від DDoS-атак, що не вимагає спеціальної підготовки для застосунків і серверів; понад чотири десятки джерел інформації про загрози безпеки для миттєвого розпізнавання і блокування шкідливого трафіку».

У контексті зазначено варто звернутися до зарубіжного досвіду, особливо в частині дослідження переваг, проблем та юридичних аспектів тестування на проникнення та використання «червоної команди». За своєю технічною природою, дана тактика захисту від DDoS-атак включає в себе тестування на проникнення, імітацію атаки. Ретельне тестування є основою гарного проєктування безпеки. Тестування – це тактична форма перевірки, щоб переконатися, що елементи керування працюють належним чином. Тестування також є запобіжним способом виявлення вразливостей у системі. «Червона команда» – спосіб тестування кібербезпеки того чи іншого суб'єкта за умови, що експерти з безпеки, які не входять до IT-відділів або команд додатків суб'єкта перевірки стану та якості забезпечення перевірки, проводять тестування на проникнення або тестування. Вони аналізують систему так, як зловмисники область напрямку атаки. Їхня мета знайти прогалини в безпеці, збираючи інформацію, аналізуючи вразливості та повідомляючи результати.

Слід зауважити, що «хоча «червона команда» та тестування на проникнення схожі за своїми кінцевими результатами, організаціям важливо вибрати правильну оцінку для правильної мети, беручи до уваги, на якому етапі процесу забезпечення безпеки знаходиться організація». У контексті вказаного, предметним буде дослідження на тему «The compliance implications of cyberattack: a distributed denial of service (DDoS) attack explored» [2], у якому зроблено спробу допомогти організаціям вибрати найкращі методи та інструменти оцінки безпеки, показати, як тестування на проникнення та червона команда повинні працювати разом, забезпечити краще розуміння того, як зміцнити стан безпеки організації та, отже, виявити шлях для майбутніх досліджень. Наслідки незаконного отримання даних є величезними і обіцяють зрости відповідно до нових правил захисту даних. Оскільки тенденція регулювання вказує на суворість вимог до дотримання кібербезпеки та захисту даних, що зростає, це залишається плідним починанням

для вчених. Вкрай важливо визнати, що для того, щоб бути ефективним, дотримання вимог має бути вбудоване в організаційну структуру корпорації. Практична значущість цього підходу для корпорацій є очевидною. Цінність практичного аналізу ризиків кібербезпеки, включаючи здатність співробітників виявляти кіберзагрози та повідомляти про них, а також постійний моніторинг кіберактивності, має основне значення. Зусилля щодо забезпечення відповідності повинні демонструвати активну ініціативу боротьби з агресією зловмисників, які здійснюють ретельно продумані DDoS-атаки. Суб'єкт (державна установа чи приватна структура), яка залишає свою кібербезпеку вразливою і не має плану дій у надзвичайних ситуаціях, повинна очікувати наступних позовів щодо недбалості, особливо з урахуванням зростаючої сфери застосування правил захисту даних.

На основі короткого огляду основних технічних підходів протидії DDoS-атакам приходимо до висновку, що сучасні захисні рішення, в першу чергу, направлені на забезпечення моніторингу трафіку, його фільтрацію, що зумовлюється потребою виявлення мережевих DDoS-атак різного типу. За допомогою таких технічних рішень видається можливим блокувати шкідливі пакети у трафіку, не перешкоджаючи доступу реальних користувачів, відстежувати наявність аномалій та сигналізувати про останні хостера. Отже, саме використання дієвого програмно-апаратного комплексу дозволяє вчасно та ефективно протидіяти DDoS-атакам.

Як вже відмічалося, DDoS-атаки несуть в собі безліч загроз як для інтересів приватних структур, так і в контексті посягання на національні інтереси та завдання значних матеріальних збитків, що, у свою чергу, вимагає відповідної реакції з боку законодавця.

Міжнародна спільнота визнає DDoS-атаки як посягання, яке вимагає кримінального покарання, що підтверджується Настановами Комітету Конвенції Європейського Союзу з питань [12].

Кримінально-правова практика на сучасному етапі свого становлення будується шляхом кваліфікації DDoS-атак в рамках діючих статей 361 та 361-1 КК України. В умовах воєнного стану зазначені норми зазнали змін. Так, Законом України «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX від 24 березня 2022 року [13] до вказаних статей КК України, які передбачають кримінальну відповідальність за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) внесено зміни, які полягають у новій їх редакції, яку спрямовано на розв'язання принаймні трьох завдань: 1) приведення термінології, що вживається у зазначених статтях, у відповідність до Закону України «Про електронні комунікації» від 16 грудня 2020 року № 1089-IX [14], а також вимог іншого законодавства України у сфері кібербезпеки; 2) диференціації у ст. 361 КК України ступеня відповідальності за несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж з урахуванням наслідків, що настали через це, з відповідним посиленням санкцій за вчинення подібного втручання; 3) доповнення статті новою частиною п'ятою, якою передбачається відповідальність за вчинення аналізованих дій під час дії воєнного стану.

Однак по при це, чинне кримінальне законодавство все одно прямо не визначає DDoS-атаки ні як спосіб, ні як знаряддя кримінального правопорушення, ні як окремий склад, водночас і кримінально-правова доктрина не надає однозначної оцінки щодо правової природи такої протиправної практики. Не міститься й визначення суб'єктного складу такого діяння, його предмету, не вирішене питання розмежу-

вання між адміністративною та кримінальною відповідальністю за такі дії, так само відсутній механізм виявлення та доведення факту скоєння описаного вище правопорушення та механізм захисту, відновлення порушеного права. Окрім того, чинне національне законодавство навіть не закріплює поняття «DoS (DDoS) атака», що суттєво ускладнює можливості кримінально правового впливу на суб'єктів, які вчинили чи були причетними до проведення DDoS-атак. Підсумовуючи викладене вище, слід відзначити, що існуюча ситуація вимагає негайної реакції та відповідних змін на законодавчому рівні з метою запровадження кримінально-правових санкцій у національній правовій системі за проведення DDOS-атак, особливо враховуючи можливі завдані збитки та характер шкоди.

Анотація

Стаття присвячена дослідженню особливостей національного досвіду протидії DDoS-атакам. Проаналізовано поняття DoS(DDoS)-атаки під явищем чого пропонується розуміти напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Надано основні характеристики DDoS-атак та їх класифікації. Визначено, що основу організаційної протидії DDoS-атакам в Україні становить робота кіберполіції та Держспецзв'язку як одного із з основних суб'єктів кібербезпеки України, відповідального за кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури, за координацію діяльності суб'єктів забезпечення кібербезпеки щодо кіберзахисту.

Окреслено найбільші DDoS-атаки на українські владні портали, інформаційні ресурси, банківські платформи та об'єкти критичної інформаційної інфраструктури. Звернено увагу на те, що сучасний арсенал засобів та методів протидії DDoS-атакам в Україні є досить значним та ефективним, що демонструється на практиці, особливо в умовах гібридної війни та постійних посягань в інформаційному просторі.

Зауважено, що чинне кримінальне законодавство прямо не визначає DDoS-атаки ні як спосіб, ні як знаряддя кримінального правопорушення, ні як окремий склад, водночас і кримінально-правова доктрина не надає однозначної оцінки щодо правової природи такої протиправної практики. А сучасна практика кримінально-правової кваліфікації будується на основі приписів нині чинних ст.ст. 361 та 361-1 КК України, що не дозволяє повною мірою використовувати потенціал кримінально-правових механізмів та вимагає відповідної реакції законодавця.

Ключові слова: кібератака, DDoS-атака, кібербезпека, протидія DDoS-атакам, організаційно-правові основи протидії DDoS-атакам, кримінальна відповідальність.

Horshkova O.O., Taikhmann Fabian. Experience in countering DDoS attacks in Ukraine: some legal aspects

The article is devoted to the study of the peculiarities of national experience in countering DDoS attacks. The author analyzes the concept of (DoS) DDoS attacks, under which it is proposed to understand an attack on a computer system with the intention of making computer resources inaccessible to users for whom the computer system was intended. The main characteristics of DDoS attacks and their classification are provided. It is determined that the basis of organizational counteraction to DDoS attacks in Ukraine is the work of the cyber police and the State Special Communications Service of Ukraine as one of the main subjects of cybersecurity of Ukraine responsible for cyber protection of State information resources and critical information infrastructure, for coordinating the activities of cybersecurity entities in terms of cyber protection.

The author outlines the largest DDoS attacks on Ukrainian government portals, information resources, banking platforms and critical information infrastructure facilities. The author emphasizes that the current arsenal of means and methods of countering DDoS attacks in Ukraine is quite significant and effective, which is demonstrated in practice, especially in the context of hybrid warfare and constant encroachments in the information space.

It is noted that current criminal law does not explicitly define DDoS attacks either as a method or as an instrument of a criminal offense, or as a separate corpus delicti, and at the same time, the criminal law doctrine does not provide an unambiguous assessment of the legal nature of such an unlawful practice. And the current practice of criminal law qualification is based on the provisions of the currently effective Articles 361 and 361-1 of the Criminal Code of Ukraine, which does not allow to fully utilize the potential of criminal law mechanisms and requires an appropriate legislative response.

Key words: cyberattack, DDoS attack, cybersecurity, counteraction to DDoS attacks, organizational and legal framework for counteraction to DDoS attacks, criminal liability.

Список використаних джерел:

1. Захаров М. Як компаніям захиститися від DDoS-атак: пояснюють кіберексперти. З технічного боку. URL: https://cutt.ly/QHdBV0J
2. Teichmann F., Bruno S. Sergi, Wittmann C. The compliance implications of cyberattack: a distributed denial of service (DDoS) attack explored. *International Cybersecurity Law Review*. Volume 4, Issue 4. С. 291–298.
3. Коваленко Я.І. Необхідність упровадження на законодавчому рівні засобів захисту права на доменне ім'я від DoS (DDoS) атак в Україні. *Юридичний науковий електронний журнал*. № 1. 2021. С. 84–87. URL: http://www.lsej.org.ua/1_2021/20.pdf
4. Андон П.І., Ігнатенко О.П. Протидія атакам на відмову в мережі Інтернет: концепція підходу. *Проблеми програмування*. 2008. № 2–3. С. 564–574.
5. Xiang Y., Zhou W., Chowdhury M. A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. Technical Report, TR C04/02, *School of Information Technology, Deakin University*, Australia, March 2004.
6. Україна змогла відбити найбільшу за всю історію країни кібератаку. URL: https://www.kmu.gov.ua/news/mihajlo-fedorov-ukrayina-zmogla-vidbiti-najbilshu-za-vsyu-istoriyu-krayini-kiberataku
7. Кібервійна за український Інтернет-простір: як протидіяти DDoS-атакам. URL: https://hub.kyivstar.ua/news/kibervijna-za-ukrayinskyj-internet-prostir-yak-protydiyaty-ddos-atakam/
8. Укртрансбезпека» заявляє про атаку російських хакерів і плани відновити роботу найближчим часом. URL: https://interfax.com.ua/news/general/842355.html
9. Величко С.В. Засоби та механізми протидії DDoS-атакам. URL: http://dspace.onua.edu.ua/bitstream/handle/ %BC.pdf?sequence=1&isAllowed=y
10. Вільне та відкрите програмне забезпечення. URL: https://cutt.ly/uHdKnu4
11. A10 THUNDER TPS. URL: https://iitd.com.ua/tag/zashchita-ot-ddos-atak/
12. Конвенція про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575
13. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 р. № 2149-IX. *Урядовий кур'єр*. 2022. 5 квітня № 78.
14. Про електронні комунікації: Закон України від 16 грудня 2020 р. № 1089-IX. *Офіційний вісник України*. 2021. 26 січня № 6. Ст. 306.