Вісник Національного університету "Львівська політехніка". Серія: "Юридичні науки"
№ 3 (27), 2020

УДК 336.7:340.5:347.7

Ірина Жаровська
Національний університет "Львівська політехніка",
доктор юридичних наук,
професор кафедри теорії, історії та філософії права
irazhar@ukr.net,
ORCID 0000-0003-3821-8120

НАЦІОНАЛЬНА ТА ІНФОРМАЦІЙНА БЕЗПЕКА (АКТУАЛІЗАЦІЯ В СУЧАСНИХ УМОВАХ)

http://doi.org/10.23939/law2020.27.056

Увага зосереджена на питаннях інформаційної безпеки. Кіберзагрози в глобалізаційному суспільстві є завжди, проте в час певних світових чи державницьких проблем та труднощів їх вплив відчувається особливо гостро.

Констатовано, що нині світ зустрівся з новою проблемою – новою хворобою, від якої не має лікування та попередження у вигляді вакцинації. Комплекс заходів, які вживають на державному рівні, зумовлює послаблення державного та недержавного секторів економіки та стосується всіх сфер життєдіяльності як окремої людини, так і держави та міжнародних інституцій. В той же час питання інформаційної безпеки привертається з новою силою, оскільки активізувалися кібератаки різного рівня.

За нашим аналізом вони мають вибірковий характер, та спрямовані саме на ті інституції, які особливо задіяні в протидії пандемії. Від початку пандемії COVID-19 ВООЗ зафіксувала різке збільшення кількості кібератак, спрямованих на її співробітників, та афер по електронній пошті, що стосуються громадськості в цілому.

У висновках зазначено, що проблема інформаційної безпеки стосується комплексу національних інтересів. Кібератаки активізувалися у час боротьби зі світовою пандемією, що зумовлена поширенням COVID-19 та стосуються як міжнародних інституцій, діяльність яких направлена на спеціалізовану боротьбу з цією кризою, так і на національні державні органи публічної влади. Ці кібератаки проводять не тільки через економічний інтерес, але й з метою поширення панічних настроїв та страху серед населення, підбурювання та інші масові девальвації. Національна державна стратегія та Стратегія кібербезпеки має мати комплексний характер та стосуватися як превентивних заходів, так і заходів відповідальності за протиправні діяння.

Ключові слова: інформаційна безпека, національна безпека, кібератаки, COVID-19

Постановка проблеми. Національна безпека в останній час, у зв'язку з викликами глобалізації, кризовими явищами сучасного суспільства та трансформацією інформаційного простору, отримала нову актуалізацію.

Класичні форми міжнародної співпраці, зокрема міжнародні нормативні гарантії захисту та функціонування колективної безпеки нині не можуть повністю задовільнити потреби суспільства та держави. Тому додатковими викликами для держави є питання забезпечення інформаційної безпеки.

Аналіз дослідження проблеми. Проблеми інформаційної безпеки широко досліджували у вітчизняній науковій доктрині, особливо фахівці в галузі адміністративного права. Серед дослід-

ників, які внесли значну роль у розвиток досліджуваного предмету варто вказати таких: А. Андреєв, Б. Бессонов, А. Венгеров, А. Вікторов, А. Горбулін, К. Делекаров, О. Дзьобань, В. Ліпкан, Я. Малик, Т. Ткачук, В. Радецький, Т. Розова, С. Самигін, Г. Ситник, тощо.

Проте питання правового регулювання інформаційної безпеки не є повністю вичерпане. Нові загрози породжують потребу подальшого наукового аналізу, зокрема у світлі нових національних викликів, породжених COVID 19.

Метою статті є аналіз питань національної та інформаційної безпеки в сучасних кризових умовах, пов'язаних зі збільшенням кібератак.

Виклад основного матеріалу. Прояви інформаційної загрози можуть загрожувати як органам публічної влади й міжнародним інституціям, так і приватному сектору та сфері бізнесу. Вказане безпосередньо стосується національної безпеки, національних цілей, стратегій та векторів розвитку.

Треба погодитися з Т. Ткачуком в тому, що до національних цілей в інформаційній сфері варто віднести такі: а) покласти край спотворенням поглядів людей на навколишній світ і самих себе (духовна безпека); б) забезпечити впровадження інформаційних технологій у військову сферу та забезпечити їх захист (воєнна безпека); в) прискорити розробку та впровадження новітніх ІКТ у суспільно-економічну сферу (економічна безпека); г) досягти належного рівня культури інформаційних відносин (соціальна безпека); ґ) створити загальнодержавні інформаційні системи для постійного моніторингу стану навколишнього середовища (екологічна безпека); д) сприяти інтеграції національної інформаційної інфраструктури зі світовою інфраструктурою; е) посилити захист інформаційних прав людини; є) вжити термінових заходів для створення позитивного іміджу держави в умовах інформаційної глобалізації" [1, с. 386].

Інформаційні загрози, інформаційні атаки можуть виступати і засобом військових дій. Поки наша нація покладається на комп'ютерні мережі як фундамент військової та економічної сили, наша національна та економічна безпека отримує загрозу через кіберсферу. Кібератаки на будь-яку державу, навіть з найсильнішим інформаційним захистом, промисловістю та державними системами сильно впливають на нашу економіку та можливості протидіяти сучасній мережево-орієнтованій війні.

Т. Маккензі доводить, що такі атаки суттєво впливають навіть на США, яка має найпотужнішу армію світу. "Стримування в кібердомені різко відрізняється і набагато складніше, ніж у інших військових областях (повітря, суша, море та космос). Кіберзброя та кібертехніка порівняно недорогі і їх можна легко отримати або розробити. Кількість груп противника, здатних атакувати американські мережі, велика, і наша здатність стримувати кожну групу буде залежати від її мотивів та рівнів толерантності до ризику. Ефективна стратегія кібер-стримування має бути багатошаровою і використовувати всі інструменти національної сили США" [2, с. 1].

Понятійно-категоріальний апарат у сфері інформаційного суспільства на нормативному рівні не відрізняється чіткістю та узгодженістю. Так, є багато дефініцій, які ще чекають свого обґрунтування. Вказане пов'язане з відносною новизною та стрімким розвитком проблеми.

Все таки, виправити ситуацію на нормативному рівні спробували законотворці. В кінці 2017 року був прийнятий закон "Про основні засади забезпечення кібербезпеки України", який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Цей закон надає широку дефініцію поняттю кібератаки: “ Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту” [3]

Вужче, але інформативніше розуміння знаходимо в допоміжних джерелах. У своєму коментарі до National Interest А. Панайотіс використовує визначення кібератаки як кібероперації, будь то наступальна чи оборонна, що, як очікується, спричинить травму чи загибель людей або пошкодження або знищення предметів [4].

В аналітичній записці Національного інституту стратегічних досліджень при Президентові України під кібератакою запропоновано розуміти “цілеспрямовані дії, які реалізуються в кіберпросторі (або за допомогою його технічних можливостей), що призводять (можуть призвести) до досягнення несанкціонованих цілей” [5].

Кіберзагрози в глобалізаційному суспільстві є завжди, проте в час певних світових чи державницьких проблем та труднощів їх вплив відчувається особливо гостро.

Нині світ зустрівся з новою проблемою – новою хворобою, від якої не має лікування та попередження у вигляді вакцинації. Комплекс заходів, які вживають на державному рівні, зумовлює послаблення державного та недержавного секторів економіки та стосується всіх сфер життєдіяльності як окремої людини, так і держави і міжнародних інституцій. В той же час питання інформаційної безпеки привертається з новою силою, оскільки активізувалися кібератаки різного рівня.

За нашим аналізом вони мають вибірковий характер, та спрямовані саме на ті інституції, які особливо задіяні в протидії пандемії.

З моменту початку пандемії COVID-19 ВООЗ зафіксувала різке збільшення кількості кібератак, спрямованих на її співробітників, та афери по електронній пошті, що стосуються громадськості в цілому. Тільки за один тиждень квітня 2020 і близько 450 активних електронних адрес та паролів ВООЗ та осіб, які працюють над новим коронавірусним реагуванням, стали доступними в мережі.

Шахраї, що представляють ВООЗ в електронних листах, також все частіше орієнтуються на широку громадськість з метою направлення пожертв на вигаданий фонд, а не на справжній фонд солідарного реагування COVID-19. Кількість кібератак зараз більше, ніж у п’ять разів перевищує кількість, спрямованих на Організацію за аналогічний період минулого року [6].

Фахівці американської корпорації Google вважають, що поширенням коронавірусної інфекції у світі активно користуються хакери, зокрема ті, яких таємно підтримує влада в різних країнах. “У компанії відзначили, що кіберзлочинці намагаються скористатися стурбованістю людей через пандемію для здійснення фішингових атак і різних видів шахрайства: від імітації збору пожертвувань для благодійних та неурядових організацій, до відправки працюючим з дому співробітникам фальшивих повідомлень, нібито від роботодавця, і до підроблених сайтів, схожих на офіційні сторінки влади або управлінь охорони здоров’я”. За місяць ця корпорація фіксувала відправку через її поштовий сервіс Gmail приблизно 18 млн електронних листів кожного дня, які стосуються теми коронавірусу та мають шкідливе програмне забезпечення [7]. Однак, це не просто економічні атаки. Злочинні групи підтримує влада, як зазначають фахівці корпорації.

Тільки в нашій державі Державна служба спеціального зв’язку та захисту інформації України у період з 3 по 10 квітня зареєструвала 1174 кіберінциденти [8].

Тому на державному рівні цивілізовані держави розробляють комплексний підхід, який, зазвичай, репрезентують у вигляді державних стратегій.

Позитивно оцінюємо рішення України, яка створила стратегію, яка предметно стосується інформаційної сфери. Рішенням Ради національної безпеки і оборони України від 27.01.16 р. введено в дію Стратегію кібербезпеки України. Метою Стратегії є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідними є: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері; забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура) [10].

Проте, як і в більшості інших сфер правового регулювання, виникає проблема в реалізації норм права. Як вказують фахівці "виконання окремих важливих рішень РНБО України, присвячених кібербезпековим технологіям, відбувається повільно, із значним порушенням визначених термінів виконання. Законопроекти, пов'язані з питаннями захисту кіберпростору держави, не розглядаються Верховною Радою України протягом багатьох місяців, а то й років. Крім того, законодавство щодо кібербезпеки країни також не є досконалим. Зокрема, в Україні на сьогодні законодавчо, на жаль, не визначено сфер відповідальності між різними державними та правоохоронними органами" [11, с. 109].

Вважаємо, що в контексті кібератак Україна має значну увагу зосередити на можливостях їх стримування.

Параметри стримування можуть бути пасивними або активними. У своїй книзі "Кіберстримування та кібервійна" Мартін Лібіцький описує ці варіанти, як (1) "стримування запереченням (здатність відривати атаки)" або пасивне стримування та (2) "стримування за допомогою покарання (загроза відплати)" або активне стримування. З кіберточки зору, пасивне стримування включає ті дії, що вживаються для захисту наших мереж від атак або побудови стійких мереж, що мінімізують наслідки нападу. Ці дії – це важлива частина хорошої інженерії та доктрини системи безпеки, що відіграє допоміжну роль у активному стримуванні кібератак. Вони чинять стримувальний ефект, заперечуючи противника будь-яких значущих наслідків для систем, мереж або операцій [12].

Наполягаємо на тому, що поєднання пасивних та активних дій є запорукою побудови успішної стратегії. Саме пасивне кіберстримування (стримування запереченням) не спричинить необхідного страху в противника, щоб запобігти нападам. Має бути справжня загроза ввести небажаний набір заходів покарання (активне стримування), щоб стратегія була успішна та ефективна.

Один з найбільших бар'єрів для ефективного кіберстримування – це поняття атрибуції. Знаходження в кібердомені можливо, але в деяких обставинах це може бути важким і трудомістким.

Складна структура Інтернету, незріла політична та правова політика, і глобальна природа кібердомену дозволяє працювати анонімно. Противники можуть використовувати будь-яку кількість вразливих систем або протоколів, приховувати або підробляти їх місцезнаходження та працювати майже з будь-якого фізичного місця. Чим досконаліший нападник, тим складніше стає атрибуція. Ці зловмисники вживатимуть дій, щоб приховати своє справжнє місцеположення та зробити його не тільки хибним, але й таким, що відверне від них увагу шляхом підозри інших суб'єктів. Крім того, правові та політичні перешкоди можуть зробити атрибуцію важкою і трудомісткою особливо, коли міжнародна співпраця між різними організаціями, агенції та уряди зобов'язані визначити джерело нападу.

Висновок. Проблема інформаційної безпеки стосується комплексу національних інтересів. Кібератаки активізувалися у час боротьби зі світовою пандемією, що зумовлена поширенням COVID-19 та стосуються як міжнародних інституцій, діяльність яких направлена на спеціалізовану боротьбу з цією кризою, так і на національні державні органи публічної влади. Ці кібератаки проводять не тільки через економічний інтерес, але й з метою поширення панічних настроїв та страху серед населення, підбурювання та інші масові девальвації. Національна державна стратегія та Стратегія кібербезпеки має мати комплексний характер та стосуватися як превентивних заходів, так і заходів відповідальності за протиправні діяння.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України: дис. на здобуття кандидата юрид. наук, ДВНЗ «Ужгородський національний університет», Ужгород. С. 397. 2. McKenzie T. M. (2014) Is Cyber Deterrence Possible? Colonel, USAF CPP–4 Air University Press Air Force Research Institute Maxwell Air Force Base, Alabama. 20 c. 3. Про основні засади забезпечення кібербезпеки України: закон України від 05.10.2017. № 2163-VIII. *Відомості Верховної Ради.* 2017. № 45, ст. 403. 4. Panayotis A. Ya., Lowther A. B. (2014) Conflict and Cooperation in Cyberspace: The Challenge to National Security. Boca Raton: Taylor and Francis Group. 5. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка. Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/454/. 6. WHO reports fivefold increase in cyber attacks, urges vigilance (2020) URL: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance. 7. У Google повідомили, що тема пандемії активно використовується для кібератак по всьому світу (2020) URL: https://www.unn.com.ua/uk/news/1865331-u-google-povidomili-scho-tema-pandemiyi-aktivno-vikoristovuyetsya-dlya-kiberatak-po-vsomu-svitu. 8. У Держспецзв'язку зафіксували на початку квітня понад 1 тис. DDoS-атак та кіберінцидентів (2020) URL: =https://www.unn.com.ua/uk/news/1863743-u-derzhspetszvyazku-zafiksuvali-ponad-1-tis-ddos-atak-ta-kiberintsidentiv. 9. White House. National Security Strategy. Washington, DC: White House, May 2010. URL: http://www.whitehouse.gov/sites/default/files/rss_viewer/national _security_strategy.pdf. 10. Про рішення Ради національної безпеки і оборони України від 27.01.16 р. "Про Стратегію кібербезпеки України": Указ Президента України від 05.05.16 р. № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016. 11. Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам *Інформація і право*. № 3. С. 105–110. 12. Libicki M. C. Cyber Deterrence and Cyberwar. Santa Monica, CA: RAND Corporation.

REFERENCES

1. Tkachuk T. Yu. ***Pravove zabezpechennya informacijnoyi bezpeky` v umovax yevrointegraciyi Ukrayiny`*** [Legal provision of information security in the conditions of European integration of Ukraine]. Dy`s. na zdobuttya kandy`data yury`d. nauk, DVNZ «Uzhgorods`ky`j nacional`ny`j universy`tet», Uzhgorod. P. 397. 2. McKenzie T. M. ***Is Cyber Deterrence Possible?*** Colonel, USAF CPP–4 Air University Press Air Force Research Institute Maxwell Air Force Base, Alabama. 20 p. 3. ***Pro osnovni zasady` zabezpechennya kiberbezpeky` Ukrayiny`*** (05.10.2017) [On the basic principles of ensuring cybersecurity of Ukraine] No. 2163-VIII. Vidomosti Verxovnoyi Rady` [Vidomosti Verxovnoyi Rady`]. 2017. # 45, p. 403. [inUkrainian]. 4. Panayotis A. Ya., Lowther A. B. ***Conflict and Cooperation in Cyberspace***: The Challenge to National Security. Boca Raton: Taylor and Francis Group. 5. ***Problemy` chy`nnoyi vitchy`znyanoyi normaty`vno-pravovoyi bazy` u sferi borot`by` iz kiberzlochy`nnistyu: osnovni napryamy` reformuvannya*** [Problems of the current domestic regulatory framework in the field of combating cybercrime: main directions of reform]. Anality`chna zapy`ska. Nacional`ny`j insty`tut strategichny`x doslidzhen`. Retrieved from:: http://www.niss.gov.ua/articles/454/ (accessed 25.04.2020). [inUkrainian]. 6. ***WHO reports fivefold increase in cyber attacks, urges vigilance***. Retrieved from:: https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (accessed 25.04.2020). 7. ***U Google povidomy`ly`, shho tema pandemiyi akty`vno vy`kory`stovuyet`sya dlya kiberatak po vs`omu svitu*** [Google has been informed that a pandemic is being used extensively for cyber attacks around the world]. Retrieved from:: https://www.unn.com.ua/uk/news/1865331-u-google-povidomili-scho-tema-pandemiyi-aktivno-vikoristovuyetsya-dlya-kiberatak-po-vsomu-svitu (accessed 25.04. 2020). 8. ***U Derzhspeczzv'yazku zafiksuvaly` na pochatku kvitnya ponad 1 ty`s. DDoS-atak ta kiberincy`dentiv*** [In the beginning of April over 1 thousand DDoS attacks and cyber incidents were recorded in the State Secretariat of Communications]. 2020. Retrieved from:: https://www.unn.com.ua/uk/news/1863743-u-derzhspetszvyazku-

zafiksuvali-ponad-1-tis-ddos-atak-ta-kiberintsidentiv (accessed 25.04.2020). 9. White House. ***National Security Strategy***. Washington, DC: White House, May 2010. Retrieved from: http://www.whitehouse. gov/sites/default/files/rss_viewer/national _security_strategy.pdf. 10. Pro rishennya Rady` nacional`noyi bezpeky` i oborony` Ukrayiny` "***Pro Strategiyu kiberbezpeky***` Ukrayiny`(05.05.16) [About Ukraine's Cybersecurity Strategy] No. 96/2016. Retrieved from:: https://zakon.rada.gov.ua/laws/show/96/2016 (accessed 25.04.2020). 11. Gavlovs`ky`j V. D. ***Zaxy`st informaciyi shlyaxom posy`lennya efekty`vnosti proty`diyi kiberatakam*** [Protecting information by enhancing the effectiveness of counteracting cyber attacks] Informaciya i pravo. [Information and law.]# 3. P. 105–110. [inUkrainian]. 12. Libicki M. C. ***Cyber Deterrence and Cyberwar***. Santa Monica, CA: RAND Corporation.

Дата надходження: 10.07.2020 р.

Irina Zharovskaya
Lviv Polytechnic National University,
Department of Theory, History and Philosophy of Law,
Doctor of Law, Professor

NATIONAL AND INFORMATION SECURITY (CURRENT UPDATE)

The focus is on information security issues. There are always cyber threats in a globalized society, but in times of certain world or state problems and difficulties, their impact is particularly acute.

It is stated that the world now is facing a new problem – a new disease whose treatment does not have treatment and prevention in the form of vaccination. The set of measures taken at the state level causes the weakening of the state and non-state sectors of the economy and applies to all spheres of life of both individuals and the state and international institutions. At the same time, the issue of information security is coming back with renewed vigor as cyberattacks of various levels have intensified.

According to our analysis, they are selective in nature and are aimed at those institutions that are particularly involved in the pandemic response. Since the launch of the COVID-19 pandemic, WHO has seen a sharp increase in the number of cyberattacks targeted at its employees and e-mail scams affecting the public at large.

The conclusions stated that the problem of information security concerns a complex of national interests. Cyberattacks have intensified during the fight against the global pandemic caused by the spread of COVID-19 and affect both international institutions that are dedicated to the specialized fight against this crisis and national public authorities. They have not only economic interest, but also causing panic among the population, incitement, fear and other mass devaluations. National State Strategy and Cybersecurity Strategy must be comprehensive in nature and to address both preventative and criminal liability measures.

Key words: information security, national security, cyber-attacks, COVID-19.