УДК 004:355.01 :32:316.476(100) https://doi.org/10.31470/2306-546X-2019-40-70-76

КІБЕРЗАГРОЗИ В УКРАЇНІ ЯК ПРОБЛЕМА В УМОВАХ ГЕОПОЛІТИЧНОГО СУПЕРНИЦТВА

Шимченко Л. А.

Предметом дослідження *виступають кіберзагрози як інструмент геополітичного суперництва.*

Метою *написання статті є дослідження проявів кіберзагроз для українського суспільства в умовах геополітичного суперництва.*

Завдання дослідження: *розглянути формат термінологічної невизначеності кіберзагрозливої проблематики на національному рівні; дослідити прояви різнопланових кіберзагроз для українського суспільства і держави; закцентувати увагу на пропонованих механізмах боротьби проти наростаючих кібезагроз в умовах геополітичного суперництва.*

Методи дослідження. *У процесі написання статті були використані такі методи дослідження: системний підхід, пошуковий метод, синтезу та узагальнення, аналогічний метод.*

Методологічною базою дослідження стали наукові праці вітчизняних вчених, аналітичні матеріали.

Результати роботи. *Проведено дослідження проблематики геостратегічного суперництва, де основну увагу звернуто на кіберборотьбу. Встановлено, що кібербезпекова проблематика дедалі більше стає проблемою і національного рівня, що простежується в швидкості прийняття нормативно-правових рішень з узаконеними механізмами протидії кіберзагрозам, в створенні спеціальних кіберпідрозділів для забезпечення кіберпротистояння та ін. Акцентовано увагу на тих кіберзагрозах, що були найбільш резонансними в останні роки для українського суспільства і держави та звернуто увагу на застосовуваних владою механізмах протидії.*

Галузь застосування результатів. *Отримані результати дослідження можуть бути використані при викладанні у ВНЗ України таких курсів як: Національна безпека, Інформаційна безпека, Соціально-економічна безпека та ін.*

Висновки. *Кіберзлочини, кібератаки, кібервійни – це все породженням становлення інформаційної цивілізації, що не лише дає змогу будувати більш ефективне та успішне суспільство, а й формує нові загрози національній безпеці, призводить до геополітичного суперництва. Найбільше протиборство розгортається в площині кіберпростору, тому держава більшу увагу повинна приділяти системі формування інформаційної політики у всіх її проявах: забезпечити термінологічну визначеність; сприяти створенню належної координації діяльності різноманітних інформаційних відомств, діяльність яких пов'язана з кіберпросторовими можливостями; створити ефективну систему підготовки кадрів для спеціальних структурних кіберпідрозділів; налагодити співпрацю з міжнародними структурами, що намагаються забезпечувати кібербезпеку в світовому просторі.*

Ключові слова: *кіберпростір, кіберзагрози, кібератаки, кібервійни, хактивізм, геополітичне суперництво, кібершпигунство, кібердиверсії, держава, суспільство, інформаційні технології.*

КИБЕРУГРОЗЫ В УКРАИНЕ КАК ПРОБЛЕМА В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОГО СОПЕРНИЧЕСТВА

Шимченко Л. А.

Предметом исследования *выступают киберугрозы как инструмент геополитического соперничества.*

Целью *написания статьи является исследование проявлений киберугроз для украинского общества в условиях геополитического соперничества.*

Задачи исследования: *рассмотреть формат терминологической неопределенности киберугрожающей проблематики на национальном уровне; исследовать проявления разноплановых киберугроз для украинского общества и государства; акцентировать внимание на предлагаемых механизмах борьбы против нарастающих киберугроз в условиях геополитического соперничества.*

Методы исследования*. В процессе написания статьи были использованы следующие методы исследования: системный подход, поисковый метод, синтеза и обобщения, аналогичный метод.*

Методологической базой исследования стали научные труды отечественных ученых, аналитические материалы.

Результаты работы*. Проведено исследование проблематики геостратегического соперничества, где основное внимание обращено на киберборьбу. Установлено, что проблематика кибербезопасности все больше становится проблемой и национального уровня, прослеживается в скорости принятия нормативно-правовых решений с утверждёнными механизмами противодействия киберугрозам, в создании специальных киберподразделений для обеспечения киберпротивостояния и др. Акцентировано внимание на тех киберугрозах, которые были наиболее резонансными в последние годы для украинского общества и государства, а также обращено внимание на применяемых властью механизмах противодействия.*

Область применения результатов. *Полученные результаты исследования могут быть использованы при преподавании в вузах Украины таких курсов как: Национальная безопасность, Информационная безопасность, Социально-экономическая безопасность и др.*

Выводы. *Киберпреступления, кибератаки, кибервойны – это всё порождение становления информационной цивилизации, что не только позволяет строить более эффективное и успешное общество, но и формирует новые угрозы национальной безопасности, приводит к геополитическому соперничеству. Больше всего противоборство разворачивается в плоскости киберпространства, поэтому государство больше внимания должно уделять системе формирования информационной политики во всех ее проявлениях: обеспечить терминологическую определенность; способствовать созданию надлежащей координации деятельности различных информационных ведомств, деятельность которых связана с киберпространственными возможностями; создать эффективную систему подготовки кадров для специальных структурных киберподразделений; наладить сотрудничество с международными структурами, которые пытаются обеспечивать кибербезопасность в мировом пространстве.*

Ключевые слова: *киберпространство, киберугрозы, кибератаки, кибервойны, хактивизм, геополитическое соперничество, кибершпионаж, кибердиверсии, государство, общество, информационные технологии.*

CYBER-THREATS IN UKRAINE AS A PROBLEM IN CONDITIONS OF GEOPOLITICAL RIVALRY

Shymchenko L. A.

The subject of research *is cyber-threats as an instrument of geopolitical rivalry.*

The goal of research *is to study the impact of cyber-threats on Ukrainian society in conditions of geopolitical rivalry.*

The research target *is to consider the format of the terminological uncertainty of the cyber-threatening problem at a national level; to study the impact of diverse cyber-threats on Ukrainian society and the state; to focus attention on the proposed control mechanisms against the growing cyber-threats in the conditions of geopolitical rivalry.*

Research methods. *In the process of the study, the following research methods were used: a system approach, a search method, synthesis and generalization, an analogical method.*

Methodological basis of research were the Ukrainian scientists' works and analytical materials.

The results of work*. Researching the issue of geostrategic rivalry, the most of the focus is on cyber-struggle. It is found that cyber-security problems increasingly become a problem of the national level, which is traced at the speed of adoption of normative legal decisions with legitimate mechanisms of counteraction to cyber-threats, in the creation of special cyber units to secure cyber resistance and others. The article emphasizes cyber-threats that were the most resonance for the Ukrainian society and the state over recent years, and also attention was paid to the mechanisms used by the authorities to counteract.*

The field of application of results*. The results of this research can be applied in higher educational establishments of Ukraine to teach such disciplines as National Security, Information Security, Socioeconomic Security, etc.*

Conclusions. *Cybercrime, cyberattacks, cyberwar are a result of the formation of an information civilization that not only enables to build a more efficient and successful society, but also forms new threats to national security, leads to geopolitical rivalry. The greatest controversy unfolds in regard to cyberspace, so the state should pay more attention to the system of formation of information policy in all its aspects: to provide terminological definiteness; to promote the formation of the proper coordination of activities of various information departments related to cyberspace opportunities; to create an effective training system for special structural cyber units; to cooperate with international agencies trying to provide cybersecurity in the world.*

Key words: *cyberspace, cyber-threats, cyberattacks, cyberwar, hacktivism, geopolitical rivalry, cyberespionage, cyberdiversion, state, society, information technology.*

JEL Classification: E 29, L86, M15

Постановка проблеми. За останні 5 років українське суспільство все більше стало відчувати на собі наслідки впливу інформаційних технологій – як позитивних, так і негативних. До останніх слід віднести кіберзагрози у вигляді шахрайств, здирництва, несанкціонованого доступу до персональної інформації та ін. Це пов'язано з матеріальними та моральними втратами певних громадян чи юридичних осіб. Але все частіше суспільство відчуває і більш загрозливіші впливи, що можуть привезти до небезпек цілих регіонів, великої кількості людей чи статків і функціонування юридичних осіб. Особливо коли кіберзагрози стосуються об'єктів критичної інфраструктури. В контексті цього вважаємо, що необхідно прослідкувати сучасні кіберзагрози для українського суспільства та вивчити, в подальшому, дії держави по убезпеченню від можливого негативу у всіх його проявах.

Аналіз основних досліджень і публікацій. Вагомий внесок у дослідження проблеми кіберзагроз зробили як зарубіжні вчені, так і українські науковці. Проблему кіберзагроз дедалі активніше досліджують наукові структури, громадські організації, окремі науковці. Дослідження з проблематики кіберзагроз знайшли відображення у працях Дж. Ліпмана, Ф.Крамера Д. Фахренкурга, Л. Вентца, Дж. Льюїса, М. Лібіцкі, Д.Куела, С.Бейделмана, Л. Жанчевскі, А. Коларіка, М. Каветлі. Віддали належне цій тематиці й вітчизняні дослідники: О. Порфимович, А. Марченко, Ю.Федорова, М.Погорецький, В. Шеломенцев, О. Манжай, В. Петров, М.Ожеван, В. Пилипчук. Незважаючи на значні дослідження даної сфери, проблема забезпечення кібербезпеки залишається і потребує подальшого дослідження, особливо в рік президентських та парламентських виборів, коли найбільше загострюється геополітичне суперництво.

Метою написання статті є дослідження проявів кіберзагроз для українського суспільства в умовах геополітичного суперництва.

Об'єктом дослідження стало геополітичне суперництво, що в даний час має яскраво виражений войовничий характер.

Предметом дослідження виступають кіберзагрози як інструмент геополітичного суперництва.

Виклад основного матеріалу. Широкому загалу українців поняття кіберпростір, кібератака, кіберзагроза, кібервійна стали більш-менш бути зрозумілими після початку гібридної війни на Сході України, ще більше – після інформації ЗМІ про втручання у виборчу компанію США російських кіберспецслужб. В даний час, перед президентськими та парламентськими виборами в Україні, думаюча частина українського суспільства стала акцентувати свою увагу на кібербезпеці виборчого майбутнього процесу. Немає таємниці в тому, що в умовах геополітичного суперництва, яке нині триває на світовому рівні і де Україна є безпосереднім учасником (переважно як об'єкт), будуть використовуватись всі методи боротьби – і кіберборотьби в тому ж числі.

Якщо звернутися до теоретичних досліджень процесу забезпечення кібербезпеки, то помічаємо, що, незважаючи на значну кількість наукових дискусій з приводу необхідності забезпечення кібербезпеки держав, понятійний апарат є вкрай нечітким. Частіше зустрічається публіцистичний стиль викладу змісту понять. І лише не в значній частині спеціалізованої літератури чи нормативних державних документах останнього часу зустрічаються певні пояснення. Оскільки цими проблемами стали цікавитися і пересічні громадяни, тому є необхідністю на змістовому аспекті проблем кібербезпеки сконцентрувати більше уваги науковцям-фахівцям.

Відносячи себе до пересічних громадян, які цікавляться кібербезпековими проблемами, акцентуємо увагу на тому, що більше інформації можна отримати з міжнародних джерел, ніж з вітчизняних. Якщо американські науковці орієнтують переважно на можливість використання визначень у суто практичній діяльності, то вітчизняні дослідження здебільшого загальнотеоретичні або уточнюючі. Зарубіжна інформація по кіберпростору, кібербезпеці більше у формі пропонованих стратегій національної безпеки, доктрин, певних документів для силових структур від дій яких і залежить забезпечення такої специфічної безпеки. Серед вітчизняних науковців не помічено широкої фахової дискусії щодо термінологічних проблем у сфері кібербезпеки, що ускладнює науковий супровід прийняття державних рішень та висвітлення певних безпекових проблем тими, хто намагається їх показати і пояснити студентам, учням, широкій громадськості.

Взагалі, кіберзагрози державі чи суспільству умовно можна розділити на: «класичні» – в змістовому наповненні оригінальні, або звичні, що потребують лише сучасних інформаційних технологій (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків та ін.) та злочини, що можуть вплинути на політичне становище держави чи суспільства (хактивізм, кібершпигунство, кібердиверсії).

Більшість науковців стверджують, що в Україні в повному обсязі присутні всі «класичні» кіберзлочини і щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисяч. У 2017 році, як стверджує керівник Кіберполіції С. Демидюк, супроводжували близько 7 тис. кримінальних проваджень, з них 4,5 тис. – винятково кіберзлочини. За одинадцять місяців 2017 року направили до суду обвинувальні акти щодо 726 осіб [9].

Найчастіше сьогодні «класичні» кіберзлочини пов'язані з простою схемою. Шахрай дзвонить жертві як поліцейський. Зазвичай він повідомляє про затримання сина за підозрою у зберіганні наркотиків. Жертва починає хвилюватися, і тоді інший шахрай – «син» – жалісливим голосом просить переказати велику суму на картку за «вирішення питання». За 77 епізодами із січня 2016 року по травень 2017 року група вкрала у 41 особи 1,16 млн. грн. «Середній чек» становив 28,4 тис. грн., максимальний – 175 тис. грн. [9].

Стрімко зростає кількість шахрайств, здійснюваних за допомогою високих інформаційних технологій – використання фішингових сайтів та клонів сайтів великих компаній. Кібершахрайство передбачає викрадення невеликих сум з якомога більшої кількості користувачів. Поліція розслідує лише ті випадки, про які громадяни повідомляють до правоохоронних органів. Проте дуже багато громадян з різних причин – через невеликі збитки, завдані кіберзлочинцями, або через недовіру до кіберполіції, – не звертаються до правоохоронців із заявами [4].

В Україні стрімко ростуть статки кібершахраїв, які крадуть гроші з банківських карток. У 2017 році злочинці вкрали 670 млн. грн., у 2016 майже удвічі менше – 339 млн. грн. [10]. Велика частина таких злочинів взагалі не розкривається, так як для збереження власного іміджу банківські установи взагалі не повідомляють про випадки викрадення коштів – компенсують з власних заощаджень. Значна кількість потерпілих можуть тривалий час і не знати про те, що їх обікрали, і тоді на виявлення факту «зламу» витрачаються, а то й роки. Таким чином можна констатувати, що далеко не завжди держава реально обізнана з масштабами кіберзлочинності. І ця проблема наявна не лише в Україні, а й у всіх державах, де кіберзлочинність набирає обертів. Значними за обсягами та збитками залишаються злочини, пов'язані з поширенням порнографії, порушенням авторських прав.

Злочини, віднесені до групи геополітичних чи міждержавних механізмів боротьби (хактивізм, кібершпигунство, кібердиверсії), масштабно збільшуються. Україна вже активно залучається у протистояння хактивістів, в окремих випадках стає об'єктом кібершпигунських акцій. Хактивізм пов'язаний з проведенням інформаційних атак, які негативно впливають на об'єкта впливу. Атаки в мережі протікають настільки швидко, що просто не вистачить часу, щоб прийняти відповідне рішення і привести його у виконання. Так само існуючі технології фільтрації не дозволяють заблокувати окрему сторінку, відфільтрований буде весь сайт цілком. Що у випадку з платформами-гігантами, такими як Facebook або Google, призведе до катастрофи [8].

Як стверджує Д. В. Дубов, першим масованим випадком хактивізму, з яким зіткнулася Україна, були події довкола закриття файлообмінного сервісу ex.ua. Ідеться про масовані DDoS-атаки на ресурси органів

державної влади, здійснювані різноманітними суб'єктами, переважно громадянами України. Після спроб правоохоронних органів втрутитися в роботу файлообмінного сервісу було здійснено DDoS-атаки на понад 10 інтернет-сайтів органів державної влади, зокрема на сайт Президента України та сайт Міністерства внутрішніх справ України (символічно, що сайт інституції, яка має опікуватися питаннями кіберзлочинності, виявився одним з найменш стійких до кібератак). Атака розпочалася після того, як правоохоронні органи за позовом компаній Microsoft, Adobe, а також телеканалу «1+1» спочатку заблокували домен, а потім заарештували частину серверів компанії. Уже ввечері того ж дня внаслідок масштабних DDoS-атак було заблоковано роботу офіційних сайтів Президента України, уряду, Верховної Ради, СБУ, Національного банку України, Антимонопольного комітету, Державної податкової служби, Партії регіонів, Міністерства внутрішніх справ України [5, 212 с.]. Лише 3 лютого ex.ua став доступним для користувачів. Прямого економічного збитку державні органи від цих атак не зазнали, але стало зрозуміло, що держава не готова ані ідеологічно, ані технічно до подібних атак.

В період Євромайдану (жовтень 2013 р. – лютий 2014 р.) невідомі особи почали масово використовувати нетботи з метою засмічення інформаційного поля, введення людей в оману та поширення чуток [1]. У Twitter десятки нетботів вкидали різноманітне інфосміття, було «зламано» електронну пошту, аккаунт прес-секретаря Ю. Луценка Л. Сарган, аккаунти В. Кличка, офіційний сайт партії «УДАР», поштову скриньку й аккаунт на Facebook прес-секретаря Ю. Тимошенко М. Сороки. Постраждали й електронні ЗМІ, які були головними інформаційними майданчиками, а заразом і рушійними силами акцій протесту. Кілька днів поспіль хакерських атак зазнавав сайт «Української правди» та «Главкому». Сайт інтернет-видання «Цензор нет» було знищено хакерами [2].

З березня 2014 року декілька груп і окремих активістів розпочали захист держави в інформаційному та кіберпросторі. Їх функції були як супротив діям «Кіберберкуту» (Cyberberkut – віртуальній структурі, що не визнає української влади, сформованої після лютого 2014 р.). Саме «Кіберберкут» взяв на себе відповідальність за атаки на сайти структур НАТО 15 березня 2014 року – було здійснено напади на офіційний сайт НАТО, а також на сайти Центру кіберзахисту НАТО в м.Таллінні (The NATO Cooperative Cyber Defence Centre of Excellence – CCD COE) та Парламентської асамблеї НАТО [5, 215 с.].

Хакерськими структурами, що підтримували нову українську владу, було здійснено кібератаки проти веб-сайту «Кремлін.Ру», сайтів Центробанку Росії, Міністерства іноземних справ РФ, Russia Today (RT), «Російської газети», було «зламано» сторінки деяких депутатів російської Думи, голови Комітету з транспорту. В 2015 році з груп українських ІТ-активістів було створено Український Кіберальянс, дії якого стають гласними лише на 10%. У травні 2016 Український Кіберальянс провів низку операцій щодо зламу мережі ресурсів окупаційної влади Криму, окупованих районів Луганської та Донецької областей. На ресурсах були розміщені відеозвернення хактивістів. У червні 2016 Кіберальянс передав волонтерам міжнародної спільноти InformNapalm масив даних, добутих зі зламаних поштових листувань і хмарних сховищ російських журналістів і пропагандистів. За твердженням InformNapalm, було оприлюднено листування російських пропагандистів щодо теми MH17, про обстріли української території, спроби інформаційного впливу росіян, спрямованого не тільки проти України, але і США [7].

У листопаді 2016 року Українська група хакерів опублікувала нові листи, які, як вони стверджують, мають стосунок до помічника російського президента Володимира Путіна Владислава Суркова. Листи містять плани, які показують, як соратники Суркова розробляли сценарій з дестабілізації Харківської області, досліджували українських політиків, намагаючись використати політичні розбіжності в Україні, і допомогли встановити керівництво сепаратистських груп у частині Донецької і Луганської областей. Перша партія листів із «пошти Суркова», за словами аналітиків, свідчить про ретельне планування влади Росії напередодні анексії Криму і про пряму роль Москви в розпалюванні конфлікту на сході України [7].

Як стверджують фахівці, що Росія проти України застосовувала навіть троянські програми – вірус Snake, відому також під назвами Turla і Uroboros. Цей вірус, яким було охоплено в серпні 2014 року 60 комп'ютерів в офісі прем'єр-міністра України Яценюка, пробравшись на чужий комп'ютер, перехоплює мережевий трафік, дає іншій особі можливість отримати віддалений доступ до підключеного до Інтернету комп'ютера [12]. Досить активним було використання троянських програм в 2014-2016 роках, з 2017 року активність зменшилась.

З 2015 по 2017 рік відбулось кілька масштабних кібератак, які демонстрували системні проблеми у комунікативній реакції органів влади або атакованих установ. 23 грудня 2015 р. кібератаці було піддано «Прикарпаттяобленерго» – вважається, що початок атаки припадає на приблизно на 15:30. Механізмом атаки стали фішингові листи, які містили віруси BlackEnergy. Внаслідок реалізації кібератаки перерва в електропостачанні склала від 1 до 3,5 годин, а без світла залишилось 225 тис. споживачів. Відома міжнародна компанія ESET, яка займається кібербезпекою, повідомила, що аварія на «Прикарпаттяобленерго» стала результатом зовнішньої хакерської атаки. В офіційній заяві з посиланням на власне розслідування вказується, що атака стала частиною глобальнішої хакерської діяльності проти підприємств України та Польщі [14].

Крім безпосередньо атаки на об'єкт енергетичної інфраструктури, організатори атаки спробували вивести з ладу і систему колл-центру – телефонні системи центру були забиті тисячами фіктивних дзвінків, які, як пізніше виявилося, йшли з Москви, для того, щоб ніхто інший не міг додзвонитися. Тим самим хакери намагались зменшити можливості для вчасного реагування та надання вчасної інформації на звернення громадян.

18 грудня 2016 р. відбулась ще одна атака на роботу енергомереж України – в ніч з 17 на 18 число на підстанції «Північна» НАК «Укренерго» відбувся збій в автоматиці керування. Електропостачання вдалось швидко відновити (щоправда в окремих районах світло зникло на 6 годин)[3]. Найбільш оперативно подію коментував очільник Укренерго В. Ковальчук – він в 11:34 18-го грудня зробив відповідну заяву на своїй сторінці ФБ. З його ж повідомлення можна дізнатись, що одразу розпочала роботу команда з аналізу кіберінциденту. 21-го грудня з посиланням на заяву пана Ковальчука, Reuters повідомив, що Україна розпочала розслідування.

Ще одним кіберінцидентом який потребував ефективного комунікування з боку органів державної влади – атака вірусу NotPetya. 27 червня 2017 р. було виявлено кіберінцидент, пов'язаний із функціонуванням вірусу NotPetya. Згідно з даними Департаменту кіберполіції Національної поліції України, під час масованої хакерської атаки в Україні були інфіковані понад 12,5 тисяч комп'ютерів. За дві доби 1508 юридичних і фізичних осіб подали скарги до кіберполіції про блокування комп'ютерів вірусом Petya A, який шифрував дані на комп'ютері та вимагав гроші. Обрушилася робота сайтів «Укренерго», «Київенерго», «Укртелекому», «Нової пошти», «Ощадбанку», «Укргазбанку», «ОТП Банку» та ін. Загальні збитки обраховуються в 1,2 млрд. дол. [13].

Основним каналом розповсюдження вірусу стало програмне забезпечення M.E.Doc, сервери якої було зламана задовго до самої атаки. Незважаючи на те, що вірус маскувався під дію віруса-здирника його цілями були шпигунство та подальше знищення атакованих систем.

Більшість даних вказують на те, що активна фаза атаки розпочалась приблизно о 10:30-11:00 27 червня 2017 р. При цьому перші офіційні реакції розпочались лише о 16:40. Відтак публічне комунікативне реагування відбулося із суттєвим запізненням, відносно вимоги реакції протягом першої години. На момент заяв вже декілька годин випуски новин на телебаченні, повідомлення в медіа, обговорення в соціальних мережах були зосереджені довкола кібератак. Висловлювалися різні версії події, окремі розгорнуті інтерв'ю почали з'являтись вже за 2 місяці після кібератаки, але вони не дають громадянам цілісного уявлення про те, що відбулось, хто постраждав, як держава планує цього уникати в майбутньому, та що для цього робиться.

Кінець 2017 р. відмітився декількома випадками кіберінцидентів. Ключовий з них – атака вірусу BadRabbit. 24 жовтня 2017 р. за допомогою цього вірусу було атаковано київський метрополітен (призвело до збоїв у оплаті проїзду платіжними картками) та Одеський аеропорт (були уражені окремі інформаційні системи аеропорту). Крім того, з метою попередження атаки на інформаційні ресурси Міністерства транспорту було відключено їх офіційний сайт. Першою реакцією (о 14:36) було повідомлення прес-служби Мінтрансу, що сайт відключено у зв'язку із можливими атаками. Майже одночасно (о 16:30) на ситуацію відреагували твіттер-аккаунт Київського метро (жодної інформації про суть події – лише повідомлення про те, що не працюють окремі функції) та Одеського аеропорту (повідомлення містить інформацію про суть проблеми, про поточний стан, але не вказано жодних відомостей щодо того, що робиться для її вирішення) [11].

Перше повідомлення на сайті Департаменту кіберполіції – лише 25-го жовтня з розгорнутими показниками ураження, механізму реалізації ураження та рекомендаціями для попередження ураження систем (для технічних спеціалістів). Загалом реакція як організацій що були уражені вірусом, так і суб'єктів протидії кібератакам була достатньо оперативною. Водночас не можна не відмітити хаотичність повідомлень, часто – низьку інформативність (або повне ігнорування причин виникнення кризової ситуації) та відсутність зрозумілих пояснень для громадськості щодо суті події (найбільш повним та адекватним ситуації в цьому сенсі було повідомлення СБУ).

Другий випадок, який вимагав активного інформаційного позиціонування державних структур, пов'язаний із діяльністю українського співтовариства хактивістів «Ukrainian Cyber Alliance», які у листопаді 2017 р. розпочали акцію (флешмоб) під загальним хештегом #F*ckResponsibleDisclosure. За словами організаторів його мета – «громадська акція для підвищення рівня IT-гігієни» (за суттю акція є формою краудсорсингового пен-тесту державних інформаційних систем) [6].

У межах «флешмобу» були протестовані уразливості наступних структур: Національне агентство з питань попередження корупції, Комунальна наукова-дослідна установа «Науково-дослідний інститут соціально-економічного розвитку міста», Міністерство внутрішніх справ, Департамент кіберполіції Національної поліції України, Херсонська обласна рада, Судова влада України, Державна служба фінансового моніторингу України, Енергоатом, Головне управління Національної поліції в Київській області, Київводоканал, ОАО «Запорожсталь», Державна служба з надзвичайних ситуацій, Комунальний концерн «Центр комунального сервісу», Укртелеком, Закарпатський військомат, низка регіональних Центрів зайнятості, Міністерство охорони здоров'я України, Міністерство юстиції України, Міністерство оборони України, Запорізька АЕС, Інститут електрозварювання НАН України, Міністерство освіти України та НАН України.

З 23 державних установ (міністерств, їх підрозділів чи об'єктів критичної інфраструктури), лише 3 (Національне агентство з питань попередження корупції, Херсонська обласна рада та Енергоатом) публічно відреагували на ситуацію. У більшості своїй це були спростування загального характеру, в яких йшлося про те, що, незважаючи на спроби кібератак, активістам не вдалось отримати доступ до внутрішніх мереж, інформації з обмеженим доступом чи порушити роботу підприємств. Найбільш жорстким публічне протистояння виявилось між ініціаторами флешмобу та компанією «Енергоатом», які спочатку взагалі відмовлялись визнавати наявність уразливості, але в подальшому спробували залучити організаторів до їх усунення [6].

Зважаючи на те, що акція отримала розголос у ЗМІ, ігнорування проблеми (відсутність повідомлень та жорсткі спростування) видається малоефективним механізмом у реагуванні на подібні ситуації. Навіть у тих

випадках, коли спростування наводились, вони часто запізнювались у часі й були надто загальними. Крім того, із них залишалось незрозумілим якісь заходи були вжиті.

Висновки. Кіберзлочини, кібератаки, кібервійни – це все є породженням становлення інформаційної цивілізації, що не лише дає змогу будувати більш ефективне та успішне суспільство, а й формує нові загрози національній безпеці, призводить до геополітичного суперництва. Найбільше протиборство розгортається в площині кіберпростору, тому держава більшу увагу повинна приділяти системі формування інформаційної політики у всіх її проявах: забезпечити термінологічну визначеність; сприяти створенню належної координації діяльності різноманітних інформаційних відомств, діяльність яких пов'язана з кіберпросторовими можливостями; створити ефективну систему підготовки кадрів для спеціальних структурних кіберпідрозділів; налагодити співпрацю з міжнародними структурами, що намагаються забезпечувати кібербезпеку в світовому просторі.

Список використаних джерел

1. Боти намагаються засмічувати інформаційне поле #євромайдан – як з цим боротись. URL: http://v-n-zb.livejournal.com/6379558.html

2. Булгак П. Кібервійна та Євромайдан: репетиція 2015. URL: http://www.pravda.com. ua/articles/2013/11/27/7003178/

3. В «Укренерго» назвали причину нічного «знеструмлення» Києва та області. URL: https://www.epravda.com.ua/news/2016/12/18/614928/

4. Демидюк С. Сьогодні кіберполіція близько 80% злочинів, пов'язаних із кібершахрайством. URL: http://mvs.gov.ua/ua/news/13720_Sogodni_kiberpoliciya_rozkriva_blizko_80_zlochiniv_povyazanih_iz_kibershahraystvom__Sergiy_Demedyuk_FOTO.htm

5. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ : НІСД, 2014. 328 с.

6. Дубов Д. В. Проблемні питання комунікування кібератак в Україні: можливі шляхи вирішення. URL: http://www.niss.gov.ua/content/articles/files/CyberCommunication-e06b5.pdf

7. Кіберальянс заявляє, що у 2016 році український хактивізм вийшов на світовий рівень. URL: https://detector.media/infospace/article/122787/2017-02-02-kiberalyans-zayavlyae-shcho-u-2016-rotsi-ukrainskii-khaktivizm-viishov-na-svitovii-riven/

8. Мазур Є. Хактивіст про кібербезпеку України: не можна підвищити ефективність порожнечі. URL: https://24tv.ua/ukrayina_tag1119

9. Некрасов В. Голова Кіберполіції: «Ваш син у поліції» приносить шахраям на «зоні» мільйони гривень на добу URL: https://www.epravda.com.ua/publications/2018/01/15/633003/

10. Некрасов В. Українці збагатили кібершахраїв на півмільярда: як не стати жертвою. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu

11. Rad Rabdit – новый вирус-шифровальщик, атаковавший Украину. URL: https://24tv.ua/ru/novaja_kiberataka_v_ukraine_stalo_izvestno_kakoj_imenno_virus_zablokiroval_kompjutery_gospredpr_n880875

12. Російська програма-шпигун знайдена на комп'ютерах в офісі Яценюка. URL: https:// www.unian.ua/science/ 948970

13. США звинуватили Росію в атаці вірусу Not Petya і обіцяли наслідки. URL: https:// www.unian.ua/ politics/10009301

14. Червоненко В. Чи була кібератака на обленерго? URL: https://www.bbc.com/ukrainian/society/ 2016/01/160106

References

1. Boty namahaiutsia zasmichuvaty informatsiine pole #ievromaidan – yak z tsym borotys [Bots are trying to clutter the information field #EuroMaidan – how to fight it]. URL: http://v-n-zb.livejournal.com/6379558.html [in Ukr.].

2. Bulhak, P. (2013). Kiberviina ta Yevromaidan: repetytsiia 2015 [Cyberwar and EuroMaidan: rehearsal 2015]. URL: http://www.pravda.com. ua/articles/2013/11/27/7003178 [in Ukr.].

3. V «Ukrenerho» nazvaly prychynu nichnoho «znestrumlennia» Kyieva ta oblasti [In «Ukrenergo» was named the reason of nightly «blackouts» of Kyiv and region]. URL: https://www.epravda.com.ua/news/2016/12/18/614928 [in Ukr.].

4. Demydiuk, S. (2018). Sohodni kiberpolitsiia blyzko 80% zlochyniv, pov'iazanykh iz kibershakhraistvom [Today, cyberpolice solve about 80% crimes of cybercrime]. URL: http://mvs.gov.ua/ua/news/13720_Sogodni_kiberpoliciya_rozkriva_blizko_80_zlochiniv_povyazanih_iz_kibershahraystvom__Sergiy_Demedyuk_FOTO.htm [in Ukr.].

5. Dubov, D. V. (2014). Kiberprostir yak novyi vymir heopolitychnoho supernytstva [Cyber space as a new dimension of geopolitical rivalry]: monohrafiia. Kyiv : NISD, 328 p. [in Ukr.].

6. Dubov, D. V. (2018). Problemni pytannia komunikuvannia kiberatak v Ukraini: mozhlyvi shliakhy vyrishennia [Problematic issues of communicating cyberattacks in Ukraine: possible ways to solve the problem]. URL: http://www.niss.gov.ua/content/articles/files/CyberCommunication-e06b5.pdf [in Ukr.].

7. Kiberalians zaiavliaie, shcho u 2016 rotsi ukrainskyi khaktyvizm vyishov na svitovyi riven [Cyberalians inform that in 2016, Ukrainian hacktivism came to the world level]. URL: https://detector.media/infospace/article/122787/2017-02-02-kiberalyans-zayavlyae-shcho-u-2016-rotsi-ukrainskii-khaktivizm-viishov-na-svitovii-riven [in Ukr.].

8. Mazur, Ye. Khaktyvist pro kiberbezpeku Ukrainy: ne mozhna pidvyshchyty efektyvnist porozhnechi [Haktivist about the cyber security of Ukraine: it is impossible to increase the efficiency of emptiness]. URL: https://24tv.ua/ukrayina_tag1119 [in Ukr.].

9. Nekrasov V. (2018). Holova Kiberpolitsii: «Vash syn u politsii» prynosyt shakhraiam na «zoni» miliony hryven na dobu [The head of Cyberpolice: «Your son in the police» brings swindlers in «prison» millions of hryvnias per day]. URL: https://www.epravda.com.ua/publications/2018/01/15/633003 [in Ukr.].

10. Nekrasov, V. (2018). Ukraintsi zbahatyly kibershakhraiv na pivmiliarda: yak ne staty zhertvoiu [Ukrainians enriched cybersecurity about half a billion: how not to become a victim]. URL: https://news.finance.ua/ua/news/-/419603/ukrayintsi-zbagatyly-kibershahrayiv-na-pivmilyarda-yak-ne-staty-zhertvoyu [in Ukr.].

11. Rad Rabdit – novyi virus-shifrovalshchik, atakovavshyi Ukrainu [Rad Rabdit – a new virus-coder, which attacked of Ukraine]. URL: https://24tv.ua/ru/novaja_kiberataka_v_ukraine_stalo_izvestno_kakoj_imenno_virus_zablokiroval_kompjutery_gospredpr_n880875 [in Rus.].

12. Rosiiska prohrama-shpyhun znaidena na komp'iuterakh v ofisi Yatseniuka [The Russian spyware program was found on computers in the Yatsenyuk office]. URL: https:// www.unian.ua/science/ 948970 [in Ukr.].

13. SShA zvynuvatyly Rosiiu v atatsi virusu NotPetya i obitsialy naslidky [US blamed Russia for the virus of NotPetya and promised consequences]. URL: https:// www.unian.ua/politics/10009301 [in Ukr.].

14. Chervonenko, V. (2016). Chy bula kiberataka na oblenerho? [Was there a cyberattack on regional power distribution company (Oblenergo)?]. URL: https://www.bbc.com/ukrainian/society/2016/01/160106 [in Ukr.].

ВІДОМОСТІ ПРО АВТОРА

Шимченко Людмила Анатоліївна, кандидат філософських наук, доцент кафедри документознавства ДВНЗ «Переяслав-Хмельницький ДПУ імені Григорія Сковороди».
e-mail: ShymchenkoL@ukr.net
orcid.org/0000-0002-2165-1377

СВЕДЕНИЯ ОБ АВТОРЕ

Шимченко Людмила Анатольевна, кандидат философских наук, доцент кафедры документоведения ГВУЗ «Переяслав-Хмельницкий ГПУ имени Григория Сковороды».
e-mail: ShymchenkoL@ukr.net

INFORMATION ABOUT AUTHOR

Ljudmila Shimchenko, candidate of philosophical sciences, associate professor of scientific discipline of documentation
Pereiaslav-Khmelnytskyi Hryhorii Skovoroda State Pedagogical University
e-mail: ShymchenkoL@ukr.net