DOI https://doi.org/10.30525/978-9934-26-223-4-116

КІБЕРБЕЗПЕКА УКРАЇНИ В УМОВАХ ГІБРИДНОЇ АГРЕСІЇ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ ПРОТИ УКРАЇНИ (ЛЮТИЙ – КВІТЕНЬ 2022 Р.)

Козьміних А. В.

Вступ

Одним з головних інструментів політики, міжнародної політики зокрема, є – інформація. Спотворення інформації посилює напруженість, особливо в умовах гібридних війн та змінюють сприйняття фактів відповідно до уподобань акторів, які прагнуть вплинути. Варто відзначити, що досягнення в галузі цифрових медіа, скасування інформаційних меж, залишають країни відкритими та вразливими для втручання у їхній політичний та інформаційний простір з боку інших держав[1]. Інформаційний простір впливає на економічні, політичні та культурні процеси, на розвиток військової справи та технології. З прискореним переходом на цифрові системи управління зросла загроза кібербезпеці, адже Україна завжди була серед стратегічних цілей зовнішньої політики Росії серед інших країн, тому прагнемо забезпечити кібербезпеку.

Постановка проблеми. Кібербезпека в умовах гібридної війни набуває особливої важливості, оскільки сьогодні вже практично неможливо уявити собі жоден об'єкт технологічної інфраструктури, який не був би оснащений різними програмними комплексами, багато з яких мають вихід у мережу Інтернет, що несе серйозні ризики.

Кібератаки можуть бути використані як допоміжний засіб у рамках інформаційної війни, з метою злому закритих даних та їх опублікування або «вкидання» фейкової інформації, в т. ч. з посиланням на джерела, що вселяють довіру. Все це змушує по-новому дивитися на проблему кібербезпеки, особливо коли йдеться про небезпечні об'єкти чи системи забезпечення життєдіяльності.

Можливий досить широкий спектр наслідків негативного впливу за допомогою сучасних інформаційних технологій на функціонування об'єктів інфраструктури – від окремих людських жертв (наприклад, внаслідок впливу на автоматизовану систему управління транспортною інфраструктурою, на систему управління електропостачання тощо) до значних руйнувань (вплив на автоматизовані системи управління гідро-, електро- та атомних станцій тощо) і порушення функціонування всієї інфраструктури як економічної основи існування держави. Зловмисне використання інформаційних технологій завдати шкоди, порівняно із застосуванням традиційної зброї, і навіть з використанням зброї масового ураження. Актуальність дослідження зумовлена тим, що сучасне суспільство практично повністю залежить від стану захищеності інформації та кіберінфраструктури у всіх сферах. Можливість використовувати як інформаційні, так і кібертехнології, а також інформаційно-комунікаційні мережі для досягнення своєї мети мають не лише державні структури країн, а й кримінальні та терористичні організації. Тому забезпечення кібербезпеки критично важливої інфраструктури держави стало вирішальною умовою для забезпечення обороноздатності України.

Аналіз останніх досліджень і публікацій. Проблемами окремих аспектів кібербезпеки займалась велика кількість закордонних та українських науковців, які у своїх напрацюваннях та прикладних дослідженнях висвітлювали різні аспекти даного питання від безпекових особливостей інформаційних технологій і кіберзлочинів до кібернетичних війн.

Виділення невирішених раніше частин загальної проблеми. Кібербезпека є найважливішим аспектом національної безпеки в умовах російської агресії проти України, тому для протидії та запобігання кібернетичній активності, яка може завдати шкоди інтересам суспільства та держави, одного використання технічних засобів та механізмів контролю та захисту інформації недостатньо, необхідна інтеграція різних потенціалів, включаючи проведення систематичної розвідувальної діяльності, профілактичне застосування правоохоронних інструментів, використання медійних та соціально-мережевих ресурсів, залучення важелів фінансово-економічного впливу, налагодження міжнародного співробітництва в сфері кібербезпеки.

Мета та завдання. Мета дослідження полягає у висвітленні проблеми кібербезпеки в світлі повномасштабного вторгнення Росії в Україну (з 24 лютого 2022 р.). Для реалізації означеної теми передбачено здійснити аналіз шляхів розвитку кібербезпеки України з урахуванням останніх подій в умовах гібридної війни.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію

[1] Melykh O., Korbut, A. Entertainment media in the context of hybrid war in the post-Soviet countries: the case of Ukraine. *Economic Annals-XXI*. 2020. Vol. 182(3-4). P. 27. doi: https://doi.org/10.21003/ea.V182-03

кібербезпеки України»« було затверджено Стратегію кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни[2]. Стратегія кібербезпеки України 2021 (далі – Стратегія 2021) визначила проблемні аспекти попередньої стратегії (2016 рік): недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною; заплановані заходи не завжди корелювалися із визначеними нею завданнями; відсутність цілісного бачення (програми) розвитку спроможностей основних суб'єктів національної системи кібербезпеки, обмеженість ресурсного забезпечення функціонування цієї системи, відсутністю належної державної підтримки розвитку її інституційного забезпечення; не були розроблені індикатори виконання Стратегії кібербезпеки України, що ускладнило процес оцінки її результативності та виокремлення незавершених завдань. Участь у реалізації названої Стратегії переважно брали суб'єкти сектору безпеки і оборони, недостатньо залучалися інші державні органи, наукові установи, громадськість. До виконання завдань із розвитку наукового потенціалу та поширення кіберграмотності недостатньо залучалися заклади освіти та наукові установи.

Також не сформовано перелік об'єктів критичної інформаційної інфраструктури, не створено модель державно-приватного партнерства. Розвиток цифрової грамотності здійснювався без чіткої програми, кібернавчання проводились епізодично[3].

Нова Стратегія кібербезпеки України враховує попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав – членів ЄС та держав – членів НАТО[4]. Варто відзначити, що кібератаки використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення та дискредитації української державності. Протягом двох місяців війни СБУ нейтралізувала понад 250 кібератак, знешкодила ботоферми і заблокувала понад 50 тис. акаунтів у соціальних мережах[5]. 24 лютого з початку повномасштабного вторгнення Україна зазнала DDOS-атаки – поклали сайти Кабінету Міністрів, Міністерства закордонних справ, Служби безпеки України[6]. 3 березня на сайти декількох ОВА здійснили кібератаку і розмістили «заяву» Зеленського про «мирний договір з Росією»[7].

Служба безпеки Microsoft відзначає, що Росія використовує різноманітні методи отримання початкового доступу до своїх цілей, в т.ч. фішингові кампанії з використанням невиправлених уразливостей локальні сервери *Exchange* і компрометація *upstream.* Це дозволяє її проводити операції зі знищення, вилучення даних і збереження для довготривалого шпигунства та спостереження.

Також Росією за весь період повномасштабного вторгнення використовувалось деструктивне зловмисне програмне забезпечення *wiper*.

З 23 лютого по 8 квітня було здійснено майже 40 дискретних деструктивних атак[8], які постійно знищували файли в сотнях систем у десятках державних установ в Україні.

Якщо характеризувати кібератаки на Україну, то слід відзначити, що більше 40% руйнівних атак були спрямовані на організації критичної інфраструктури, які могли негативно впливати на уряд, військових, економіку, люди. 32% руйнівних інцидентів торкнулися українських державних організацій на національному, регіональному та міському рівнях[9].

Служба безпеки Microsoft також відзначила, що в українських мережах було розгорнуто щонайменше вісім руйнівного зловмисного програмного забезпечення, у тому числі *ICS*, призначене для промислових систем контролю[10]. Якщо агресор зможе підтримувати поточний темп розробки та розгортання, очікувано, що впродовж війни буде виявлено більш руйнівне зловмисне програмне забезпечення.

З початком російського вторгнення в Україну 24 лютого Microsoft спостерігала, як російські групи кіберзагроз виконують дії на підтримку стратегічних і тактичних цілей своїх військових. Хронологія військових ударів і кібервторгнень показує кілька прикладів операцій комп'ютерної мережі та військових операцій, які, здається, працюють у тандемі проти спільного набору цілей, хоча незрозуміло, чи є координація, централізовані завдання чи просто загаль-

[2] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. Офіційний сайт Верховної Ради України: https://zakon.rada.gov.ua/laws/show/447/2021#Text

[3] Там само.

[4] Там само.

[5] Протягом двох місяців війни СБУ нейтралізувала понад 250 кібератак, знешкодила ботоферми. UNN. 21 квітня 2022 р. URL: https://www.unn.com.ua/uk/news/1973434-za-dva-misyatsi-viyni-sbu-neytralizuvala-ponad-250-potuzhnikh-kiberatak

[6] Знову кібератака на Україну: лежать сайти уряду, МЗС, Служби безпеки. *24 канал.* URL: https://24tv.ua/znovu-kiberataka-ukrayinu-lezhat-sayti-uryadu-mzs-sluzhbi-bezpeki_n1876055

[7] https://24tv.ua/rosiya-napala-ukrayinu-24-lyutogo-2022-hronologiya-podiy_n1876131

[8] Microsoft: Россия координирует кибератаки с нанесением ударов по Украине. URL: https://www.golosameriki.com/a/russia-coordinates-cyberattacks-with-military-strikes-in-ukraine/6547892.html

[9] Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Digital Security Unit April 27, 2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[10] Там само.

ний набір зрозумілих пріоритетів кореляція[11]. Іноді атаки на комп'ютерні мережі безпосередньо передували військовій атаці, але з нашої точки зору, такі випадки були рідкісними. Поки що кібероперації узгоджувалися з діями, спрямованими на порушення або дискредитацію українських урядових, військових та економічних функцій, убезпечення опорних пунктів у критичній інфраструктурі та зменшення доступу українського населення до інформації.

Цілком імовірно, що спільні зусилля Microsoft, США та багатьох інших країн і компаній щодо посилення кіберзахисту як в Україні, так і за її межами, безсумнівно, допомогли зменшити шкоду, завдану цими зусиллями. Але якби Росія дійсно мала під рукою запас раніше невиявлених уразливостей і складного шкідливого програмного забезпечення, призначеного для їх використання, цих ліній оборони просто було б недостатньо, щоб запобігти значній шкоді та зриву. Оновлення мереж і систем критичної інфраструктури є повільною, дорогою та складною роботою, і неможливо, щоб кожна потенційна ціль була загартована до такої міри, щоб вона більше не була вразливою для російських кібератак, якщо тільки ці кібератаки ніколи не були настільки вражаючими.

Більше того, багато ранніх теорій про те, чому Росія могла добровільно утриматися від більш серйозних кібератак, виглядають дедалі більш неправдоподібними, оскільки конфлікт триває тривалий період. Наприклад, одне з пояснень, чому Росія залишила українські електророзподільні та комунікаційні мережі недоторканими, полягало в тому, що путін хотів, щоб решта світу побачила швидку, вирішальну перемогу Росії в Україні через постійний потік зображень і відео, яким могла б перешкодити така напад. Але оскільки стає все більш очевидним, що швидкої, вирішальної перемоги не буде, стає все менш сенсу, що Росія продовжуватиме залишати цю інфраструктуру недоторканою, якщо вона справді не зможе її знищити. Ця інтерпретація, здається, додатково підкріплюється рішенням Росії завдати удару по телевежі в Києві, замість того, щоб намагатися порушити засоби масової інформації та комунікаційні системи більш ефективно та менш насильно за допомогою кібер-можливостей.

Враховуючи попередню готовність Росії розгортати кібератаки з далекосяжними руйнівними наслідками, було б помилкою переоцінювати їхні кіберспроможності лише тому, що вони досі не вражали. І майже неможливо довести відсутність кіберзброї в арсеналі агресора[12]. Варто відзначити, що Росія використовувала хакерські кампанії для підтримки свого повномасштабного вторгнення в Україну, поєднуючи шкідливе програмне забезпечення з ракетами в кількох атаках, у тому числі на телевізійні станції та державні установи.

Нагадаємо, що «Стратегія 2021» визначила основні загрози кібербезпеки: «гібридна агресія Російської Федерації проти України у кіберпросторі. Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки Російської Федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності; кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат. Набуває поширення використання кіберпростору для вчинення злочинів проти основ національної безпеки України, а також кримінальних правопорушень, пов'язаних із легалізацією доходів, одержаних злочинним шляхом, торгівлею людьми, незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним обігом наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інших предметів і речовин, які загрожують життю та здоров'ю людей тощо; організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності. Особливостями таких кібератак є їх тривалість, складність та прихований характер, що ускладнює їх попередження, виявлення та нейтралізацію; використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності»[13]. Отже, визначивши осо-

[11] Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine. Digital Security Unit April 27, 2022. URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

[12] Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine. URL: https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/

[13] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 року № 447/2021. Офіційний сайт Верховної Ради України: https://zakon.rada.gov.ua/laws/show/447/2021#Text

бливості та характер російських кібератак можна говорити про реальність та серйозність вразливості у кіберпросторі. Об'єкти інфраструктури особливої важливості, розвідка, комунікації, командування та контроль, логістика, ліквідація наслідків та готовність до надзвичайних ситуацій повністю залежать від ІТ-систем, об'єднаних у мережі[14].

Загрози в кіберпросторі є найбільш серйозними для національної безпеки України. Кібербезпека зараз ключова проблема в економічному, політичному, соціальному та військовому аспектах. Тим не менш, вона залишається найменш зрозумілою та найбільш недооціненою загрозою. Тому потрібно розуміти, що кіберпростір в даний час є найважливішим театром бойових дій. Боротьба за кібер-домінування – і відповідно здатність протистояти кібератакам – означає нову еру військових відносин, яка суттєво змінить природу та структуру збройних сил. Також слід відзначити, що кібербезпеки не можна досягти на рівні держави. Вона потребує інтеграції зусиль і приватного сектору, і підприємств, міжнародної координації та співпраці у безпрецедентних масштабах.

Більше того, кіберпростір є ідеальним полем для асиметричної війни. Окремих людей чи групи залучають дуже низька вартість і щодо низький рівень технічної підготовки, необхідний проведення атак на важливі урядові, економічні, фінансові та військові об'єкти. У 2008 році, напередодні нападу Росії на Грузію із застосуванням звичайної зброї, серія кібератак вивела з ладу грузинські урядові, медійні та військові об'єкти, показавши «обличчя майбутніх війн»[15].

Висновки

Отже, російсько-українська війна з початку повномасштабного вторгнення продемонструвала, що кібератаки агресора співпадають з воєнними діями, тобто захопленням або руйнуванням об'єктів критичної інфраструктури. Відзначимо, що Росія використовувала хакерські кампанії для підтримки свого повномасштабного наступу на Україну, поєднуючи шкідливе програмне забезпечення з ракетами в кількох атаках, у тому числі на телевізійні станції та державні установи.

Вважаємо, що важливу роль у створенні ефективної системи кібербезпеки має підготовка відповідних фахівців у нашому випадку у військовій, політичній, промисловій сферах, адже однією з головних проблем забезпечення кібербезпеки в Україні є недостатній професіоналізм – навіть за наявності передових технологій країна досі відчуває брак відповідних спеціалістів. З огляду на ситуацію України важко протистояти кібератакам, які застосовує Росія. Так завдяки активній діяльності проєвропейських сил та за конструктивної підтримки зовнішніх гравців Україні вдається протистояти РФ.

На даний момент потрібно більше зосереджувати увагу на: підвищення захищеності критичної інформаційної інфраструктури та стійкості її функціонування, розвиток механізмів виявлення та попередження кіберзагроз та ліквідації наслідків їх прояву, підвищення захищеності громадян та територій від наслідків надзвичайних ситуацій, спричинених інформаційно-технічним чи військовим впливом на об'єкти критичної інформаційної інфраструктури. Певна річ, захист критичних галузей, які функціонують на базі широко розповсюджених інформаційних систем, наприклад телекомунікацій або охорони здоров'я, також має приділятися значна увага, але, на нашу думку, сучасні засоби забезпечення кібербезпеки при грамотному їх використанні здатні значно знизити ризики, що виходять від самих різних загроз: починаючи від звичайних шкідливих програм і до складних таргетованих атак. У промислових інформаційних системах ці методи просто непридатні через безліч причин.

[14] Шрайер Ф., Викс Б., Винклер Т.Х. Кибербезопасность: дорога, которую предстоит пройти. DCAF Horizon. 2015. Working Paper No. 4.RU.

[15] Шрайер Ф., Викс Б., Винклер Т.Х. Вказ праця.

Інформація про автора:
Козьміних Альона Віталіївна,
кандидат політичних наук, доцент,
доцент кафедри політичних теорій
Національний університет «Одеська юридична академія»
23, Фонтанська дорога, Одеса, 65009, Україна

Information about author:
Kozminykh Alona Vitaliivna,
PhD in Political Science, Associate Professor,
Associate Professor at the Department of Political Theories
National University "Odesa Law Academy"
23, Fontanska road, Odesa, 65009, Ukraine