9. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text Офіційний вісник України, 26.09.2014 р., № 75, том 1, с. 83, стаття 2125.

10. Ярмощук Т. Угода про асоціацію для українців символізує цивілізаційний вибір – експерт. Радіо Свобода. 20 листопада 2016 р. URL: https://www.radiosvoboda.org/a/28126929.html

11. Найем М. Френсіс Фукуяма: Путін робить рівно те саме, що робив Гітлер. *Українська правда*. 27 серпня 2014 р. URL: https://www.pravda.com.ua/articles/2014/08/27/7035903/

12. Johann B. Opinion: Revolution of dignity in Ukraine. *Deutsche Welle.* URL: https://www.dw.com/en/opinion-revolution-of-dignity-in-ukraine/a-18077223

УДК 327

ПРІОРИТЕТ ДЕРЖАВИ У КІБЕРПРОСТОРІ: АТАКА ЧИ ЗАХИСТ?

А. В. Савчук, Ю. В. Котик

Анотація: стаття присвячена проблематиці кібербезпеки в політиці держави та визначенню впливу агресивної поведінки у кіберпросторі на міждержавні відносини на прикладі Російської Федерації. Окреслено вплив сучасних технологій на державну політику та національну безпеку, охарактеризовано основні переваги та недоліки активного використання кібер-можливостей держави у контексті нападу.

Ключові слова: кібербезпека, технології, національна безпека, міждержавні відносини, Російська Федерація.

Стрімкий розвиток технологій вплинув на розширення інформаційного поля та кіберпростору. Активна людська діяльність не лише сприяє розширенню спектру загроз, а змінює тактику кібератак. Кібербезпека є важливим аспектом життя сучасної людини, оскільки вона захищає невід'ємну від її життєдіяльності категорію «власності». Вона передбачає збереження конфіденційних даних щодо кожної особистості, захист інформації про здоров'я людини та інтелектуальну власність, і що важливо, забезпечує охорону державних та галузевих інформаційних систем. Особливого значення ця проблематика має для України, яка стала полігоном для випробувань новітніх технологій та зрештою від яких значно постраждала.

Метою статті є аналіз конкретної моделі поведінки держави у кіберпросторі – Російської Федерації, спрогнозувати її вплив на відносини з іншими акторами міжнародних відносин, а також визначити, яка саме поведінка в кіберпросторі є прийнятною для держави в сучасних умовах.

Росія – одна з тих держав, яка найчастіше згадується у повідомленнях засобів масової інформації про вчинені кібератаки, викрадення даних та втручання у виборчі кампанії інших країн. Особливо кричущими випадками можна згадати її зусилля вплинути на вибори президента США у 2016. У 2020 році ситуація була схожою [1]. В обох випадках російські цілі полягали в тому, щоб підірвати віру суспільства в демократичний процес США, очорнити невигідних російській адміністрації кандидатів і завдати шкоди їх виборності та потенційному президентству. У виборчій кампанії 2020 року американські слідчі виявили, що хакери російської військової розвідки проникли в численні державні та місцеві виборчі бюро, заявивши, що крадіжки включають конфіденційну інформацію про близько 500 000 виборців [2]. Одночасно федеральні чиновники також заявили, що не мають жодних ознак того, що хакерство змінило результати або втрутилося у вибори.

Дії Російської Федерації дуже добре відомі міжнародній спільноті, зокрема і в кіберпросторі, хоча усе, як це притаманно адміністрації цієї держави, заперечується. Той факт, що РФ не надто переймається з приводу відвертої брехні щодо агресивної поведінки, має свої наслідки [3]. В першу чергу, така активність і «відкритість» в кіберпросторі відчутно впливає на відносини між державами. Через постійну фіксацію спеціалістами

кібератак з боку РФ, а також Китайської Народної Республіки, країни Європейського Союзу та більшою мірою США постійно розширюють та продовжують дію санкцій проти цих держав [4]. ЄС запровадив свої перші в історії санкції у відповідь на кібератаки в липні 2020 року, спрямовані проти російських, китайських та північнокорейських хакерів, залучених до серйозних інцидентів у попередні роки, один з яких пов'язаний з спалахом NotPetya у 2017 році, що був спрямований на територію України. Санкції заключаються в заморожуванні активів, заборону на подорожі та проведення будь-яких фінансових операцій іноземним хакерам, що причетні до інформаційних диверсій [5].

Крім того, невідповідність слів держави та її дій значно шкодить іміджу держави. Саме до такого прийому невідповідності вдається Російська Федерація, формуючи свою агресивну поведінку у кіберпросторі. Підтвердженням цього є події в ООН навесні 2021 року. Організацією Об'єднаних Націй було розроблено пакет добровільних «норм», які визначають дозволені та заборонені дії держав у кіберпросторі. Угода по суті підтвердила та розширила комплекс зобов'язань, вперше проголошених у 2015 році [6]. Росія схвалила ці норми разом із США та 23 іншими країнами. Але, погоджуючись з ними, РФ не планувала насправді їх дотримуватися. Зокрема, норми зобов'язували Росію заборонити окремим інформаційним угрупуванням працювати на її території, а російські правоохоронні органи видати злочинців, які блокують комп'ютери жертв і вимагають виплати за їх розблокування, для подальшого судового розслідування над ними до потерпілих країн. Однак Росія нехтує правилами: дозволяє злочинним угрупуванням безкарно проводити свої операції, адже, фактично, уряд сам замовляє їхні послуги, як це було з вірусом NotPetya в 2017 році. [7] Таке легковажне ставлення до міжнародних домовленостей і їх недотримання створює образ держави, дії якої надто важко передбачити, а звідси випливає потенційна загроза міжнародній безпеці.

Водночас, завдяки таким діям Російська Федерація отримала для себе значно потужнішого і сильнішого опонента у сфері кібернетики. Це добре підтверджується з огляду на Глобальний індекс кібербезпеки (GCI) та Національний індекс кібербезпеки (NCSI). Різниця між цими рейтингами полягає в тому, що перший вимірює на глобальному рівні, як уряди виконують зобов'язання щодо кібербезпеки у вигляді підвищення обізнаності про її важливість та різні проблеми, що виникають. Другий оцінює готовність країн запобігати кіберзагрозам та керувати кіберінцидентами в межах своїх кордонів [8]. Більш показовим тут все таки є Національний індекс, адже за рівнем можливостей самозахисту США займає 17 сходинку у 2021 році, а РФ – 33 [9]. Звідси виникає питання «Хто може вдарити сильніше?», тим паче, що у показниках Індексу розвитку інформаційно-комунікаційних технологій теж чималий відрив. За ними Сполучені Штати знаходяться на 16 місці, а РФ – аж на 45 [10].

Але бажання Росії розмовляти з міжнародною спільнотою з позиції сили втілює особисто сам Президент РФ. Так 1 вересня 2017 року В. Путін, даючи відкритий урок «Росія спрямована в майбутнє», висловив своє ставлення до розвитку штучного інтелекту: «Искусственный интеллект – будущее не только России, это будущее всего человечества. Здесь колоссальные возможности и трудно прогнозируемые сегодня угрозы. Тот, кто станет лидером в этой сфере, будет властелином мира» [11]. Схожа позиція у Китайської Народної Республіки, яка поставила собі за мету до 2030 року стати світовим лідером у галузі досліджень штучного інтелекту [12]. Але, беручи до уваги імперські настрої РФ, у своєму президентському зверненні до Думи В. Путін оголосив, що випробування однієї з нових технологій завершені і незабаром розпочнеться її виробництво.

Але, володіючи новітніми технологіями, треба пам'ятати, що медаль має дві сторони. До моменту відокремлення кіберпростору як поля бою, технології активно використовувалися для досягнення цілей у класичних військових діях. Прикладом цього є найдовша американська операція в Афганістані під назвою «Нескорена свобода», що розпочалась 2001 року внаслідок атак «Аль-Каїди» 11 вересня 2001 р., адже саме вони

подали мотив для швидкого просування військової техніки [13]. За рахунок великого фінансування сфери освіти та досліджень, розробки, випробувань та оцінки нових та вдосконалених технологій, на що було витрачено близько 2 мільярдів доларів, американська армія була технологічно найкраще озброєна. Більшість технологій Сполучених Штатів були невідомими для командирів, солдатів, авіаторів інших країн на той момент, тому розбити талібів їм вдалося за лічені дні. Звідси можна зробити висновок, що під час атаки, в тому числі у кіберпросторі, володіння унікальними технологіями вигідно за той рахунок, що противнику важко визначити стратегію нападу.

Військові чиновники визнають достоїнства програмного забезпечення в бою, але кажучи про іншу сторону високого рівня розвитку, необхідно мати на увазі бажання інших країн володіти подібними технологіями [14]. Тому, США як технологічний лідер стали більш вразливими для кібератак, ніж інші, адже все більше даних з різних областей діяльності держави зберігаються у цифровому просторі, що сприяє зростанню можливостей супротивника отримати доступ до стратегічно важливої інформації та вплинути на перебіг певних подій [15]. Окрім цього, володіння розвинутими технологіями окремими державами кидає виклик іншим у контексті збереження їх національної безпеки і міжнародного миру. Тому логічним є наступний висновок: просунутість в ІТ є перевагою, коли ти атакуєш; натомість часто це є недоліком і зоною вразливості, що збільшується, коли атакують тебе.

Глобальна геополітична напруженість зростає, а життя у XXI столітті активно спрямовується у цифровий простір. Все більше країн вважають ІТ-технології пріоритетними для національної безпеки, адже вони мають вирішальне значення для економічного зростання та соціальної стабільності [16]. Водночас, всеосяжна економічна інтеграція держав означає, що наслідки технологічних ушкоджень можуть бути негативними далеко не для однієї держави. Тому відповідаючи на питання «Захист чи оборона?», будуть різні відповіді. З технологічної точки зору, безперечно, вигідніше атакувати першим, адже опонент не завжди готовий до удару, або готовий недостатньо, або не може передбачити потужностей, що будуть використані [17].

З точки зору геополітики, успіх чи провал атаки залежить від обраного опонента. Лише за останні три-чотири роки посилилась актуальність спільних регіональних та глобальних реакцій для створення безпечного, надійного та сумісного кіберпростору. Тому у скорому майбутньому утворення міцної системи кібербезпеки буде здійснюватися на рівні регіональних організацій. Наприклад, АСЕАН перша у 2018 році прийняла рішення виконувати 11 добровільних, необов'язкових норм прийнятих ООН у 2015 рік для регулювання міждержавних відносин у кіберполітиці [18].

З моральної та етичної точки зору, будь-яка кібератака тягне за собою втручання, викрадення або пошкодження часто приватної та конфіденційної інформації користувачів та чутливої інформації для державних служб. Тому обмеження доступності інформації та основоположної її інфраструктури, наприклад, у формі зупинки мережі, в наслідок направлених кібератак, порушує широкий спектр прав: необґрунтоване обмеження доступу до інформації та можливостей людей висловлюватись та мирно спілкуватися, користуватися цілим рядом економічних, соціальних та культурних благ [19]. У свою чергу, для держави-замовника кібератаки подібні дії можуть призвести до зниження рівня довіри міжнародної спільноти, та утвердженню репутації, як актора, що дестабілізує міжнародне безпекове середовище.

Високорозвинена держава не може дозволити собі відступати від цифрової технології або уникати використання цих технологій через кіберзагрози. На разі нові технології стають даністю і тоді залишається лише розробити способи управління ризиками. Використовуючи аналогію з фізичного світу, не уникнути покупки автомобіля через ризик його викрадення. Швидше, можна знайти способи захисту майна. Ця ж концепція повинна застосовуватися і в кіберпросторі. Тому

найприйнятнішим шляхом у цифровому просторі для держави є відслідковування тенденцій розвитку технологій, аби мати уявлення, з чим є потенційна можливість стикнутися, та намагання підтримувати системи захисту “up-to-date”.

Аннотация. Статья посвящена проблематике кибербезопасности в политике государства и определению влияния агрессивного поведения в киберпространстве на межгосударственные отношения на примере Российской Федерации. Определено влияние современных технологий на государственную политику и национальную безопасность, охарактеризованы основные преимущества и недостатки активного использования кибер-возможностей государства в контексте нападения.

Ключевые слова: кибербезопасность, технологии, национальная безопасность, межгосударственные отношения, Российская Федерация.

Abstract. The article is devoted to the issue of cybersecurity in state policy and determining the impact of aggressive behavior in cyberspace on interstate relations on the example of the Russian Federation. The impact of modern technologies on public policy and national security is outlined, the main advantages and disadvantages of active use of cyber capabilities of the state in the context of the attack are described.

Key words: cybersecurity, technologies, national security, interstate relations, Russian Federation.

СПИСОК ЛІТЕРАТУРИ

1. Biden vows US action over Russian cyber-attacks. BBC News. 09.07.2021. URL: https://www.bbc.com/news/world-us-canada-57786302
2. Factbox: U.S. intel report on Russian cyber attacks in 2016 election. Reuters. 07.01.2017. URL: https://www.reuters.com/article/us-usa-russia-cyber-intel-factbox-idUSKBN14Q2HH
3. US imposes new Russia sanctions over cyber-attacks. BBC News. 11.06.2018. URL: https://www.bbc.com/news/world-us-canada-44446449
4. Cerulus L. EU countries extend sanctions against Russian, Chinese hackers. Politico. 17.05.2021. URL: https://www.politico.eu/article/eu-council-cyber-sanctions-russia-china-hackers/
5. ЄС готує санкції проти Росії і Китаю за кібератаки – Bloomberg. Європейська Правда. 27.02.2020. URL: https://www.eurointegration.com.ua/news/2020/02/27/7106845/
6. Hogeveen B. Six years in the making: UN reaches global cyberspace consensus. ASPI: The Strategist. 26.03.2021. URL: https://www.aspistrategist.org.au/six-years-in-the-making-un-reaches-global-cyberspace-consensus/
7. Marks J. The Cybersecurity 202: Russia agrees to cyber rules and violates them at the same time. The Washington Post. 14.06.2021. URL: https://www.washingtonpost.com/politics/2021/06/14/cybersecurity-202-russia-agrees-cyber-rules-violates-them-same-time/
8. National cyber security index. 2021. URL: https://ncsi.ega.ee/ncsi-index/
9. Global Cybersecurity Index 2020. International Telecommunication Union: Switzerland, Geneva. 2021. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
10. ICT Development Index 2017. International Telecommunication Union. URL: https://www.itu.int/net4/ITU-D/idi/2017/index.html
11. Стенографический отчёт о Всероссийском открытом уроке «Россия, устремлённая в будущее». Президент России. 01.09.2017. URL: http://kremlin.ru
12. Vincent J. Putin says the nation that leads in AI ‘will be the ruler of the world’. The Verge. 04.09.2017. URL: https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world
13. Brustein J. A rare military tech unicorn looks past Afghanistan War. Bloomberg. 24.08.2021. URL: https://www.bloomberg.com/news/articles/2021-08-24/afghanistan-war-turns-u-s-military-drone-startup-shield-into-unicorn
14. Greenemeier L. Post-9/11 Technology Brings Exoskeletons, Laser Cannons to 21st-Century U.S. Military. Scientific American. 06.09.2011. URL: https://www.scientificamerican.com/article/post-911-military-technology/
15. Kavanagh C. New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses? Carnegie. 28.08.2019. URL: https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736
16. High Technology Affects National Security. China Economic Times. 12.06.2000. URL: http://www.china.org.cn/english/GS-e/668.htm
17. Missiroli A. Game of drones? How new technologies affect deterrence, defence and security. NATO Review. 05.05.2020.
18. Koh D. The Geopolitics of Cybersecurity. The Diplomat. 09.12.2020. URL: https://thediplomat.com/2020/12/the-geopolitics-of-cybersecurity/
19. Vallor S., Rewak W. An Introduction to Cybersecurity Ethics. 2019. 65 p. P. 7–13. URL: https://www.scu.edu/media/ethics-center/technology-ethics/IntroToCybersecurityEthics.pdf