

3. FAO. The importance of Ukraine and the Russian Federation for global agricultural markets and the risks associated with the current conflict. URL: https://www.fao.org/fileadmin/user_upload/faoweb/2022/Info-Note-Ukraine-Russian-Federation.pdf

4. UNCTAD. The impact on trade and development of the war in Ukraine. URL: https://unctad.org/system/files/official-document/osginf2022d1_en.pdf

5. Чалюк Ю.О. Глобальні соціально-економічні наслідки російсько-української війни. Економіка та суспільство, 2022. Вип. 37. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/1224/1179>

Завгородня Ю.В.,
доцент кафедри політичних теорій,
кандидат політичних наук, доцент,
Національного університету «Одеська
юридична академія», м. Одеса

КІБЕРНЕТИЧНІ ЗАГРОЗИ У ВІЙСЬКОВО-ПОЛІТИЧНОМУ ПРОЦЕСІ СУЧАСНОЇ УКРАЇНИ

В умовах повномасштабного вторгнення військових країни агресора на територію України виникла чітка загроза територіальній цілісності суверенної та незалежної держави визнаної на міжнародному рівні. Оскільки, процес протистояння відбувається не лише на полі бою військових, тому виникає потреба в аналізі сучасної методики впливу, такої як кіберпротиборство. Тому, російсько-українські протиборства сформовані з комплексу заходів впливу сторін один на одного, тому варто акцентувати увагу на сучасні форми впливу, які застосовується у протистоянні та виходить за фактичні межі розповсюдження військових дій.

Кіберзагрози розповсюджуються не лише на країну, яку намагаються окупувати, а й на країни, які публічно оголошують підтримку Україні, щоб дестабілізувати процеси в середині політичної системи та порушити постачання різних видів підтримки (гуманітарної чи військової). Проте, наслідки такої

діяльності є ще більшою ознакою протиправних дій агресора та більшою потребою підтримки України, яка відстоює межі своєї країни. Оскільки, окупація в сучасному світі це ознака варварства та беззаконня, порушення світового порядку розвитку та взаємодії, а також порушення міжнародного права.

Масштаби кіберзагроз в сучасному суспільстві збільшуються та глобалізуються навіть під час регіонального протиборства. Тому, успішна атака хакерів може призводити до знеструмлення окремих регіонів чи навіть країн, викрадення баз даних, списання коштів з банківських рахунків чи знищення успішної організації. Так, до прикладу після початку військової агресії у 2015 році з рахунків окремих підприємств України хакерам вдалось украсти близько 100 млн. грн., що деморалізує суспільство та економічно робить бідними звичайних громадян [1].

В свою чергу, на офіційному урядовому порталі Держспецзв'язку подало офіційну статистику щодо кібератак за перші чотири місяці повномасштабної війни. Автори зазначають, що «ворожі хакери продовжують атакувати Україну. Інтенсивність кібератак від початку повномасштабного воєнного вторгнення росії не зменшується, хоча їхня якість – знижується. Найбільше, атакують Уряд і місцеві органи влади, оборонний, фінансовий, енергетичний сектори. Залишаються у полі зору кіберзловмисників також транспортна інфраструктура та телеком-галузь»[2].

Загальна кількість кібератак за перші чотири місяці повномасштабної війни 796 атак. Найпоширеніші методи кібератак, це: збір інформації зловмисником (242), шкідливий програмний код (192), втручання (92), спроби втручання (82), порушення доступності (56), інше (132)[2].

Тому враховуючи усі процеси впливу на політично-правову систему суспільства варто розтлумачити поняття «кібернетичної загрози». Так, на думку Діордіца І. «кібернетична загроза (кіберзагроза) – наявні й потенційно можливі явища та чинники, що створюють небезпеку інтересам людини, суспільства й держави через порушення доступності, повноти, цілісності, достовірності,

автентичності режиму доступу до інформації, яка циркулює в критичних об'єктах національної інформаційної інфраструктури»[1].

Оскільки, в умовах війни російсько-українського протистояння основним завдання агресора є повалення української державності, то кіберзагрози та їх застосування є ваговою складовою впливу на політичний процес та його дестабілізація. Разом з тим, українська держава також здійснює ряд заходів щодо кібербезпеки України. Так, «у листопаді вперше українську сторону було запрошено до навчань кіберкомандуванням ЗС США Cyber Flag. Наразі український підрозділ готується до схожих навчань Locked Shields 2022 за планом Агентства оборонних інформаційних систем Міністерства оборони США. Українські представники вже працюють у складі групи з аналізу кіберзагроз Регіонального центру кібербезпеки, який створено в Каунасі (Литовська Республіка). Достатньо значна кількість українських військовослужбовців завершила або продовжує навчання у відповідному профільному коледжі Національного університету оборони США, інших військових навчальних закладах держав-партнерів»[3].

Тому, українське суспільство і держава розуміють небезпеку та негативні наслідки, які несуть кіберзагрози, для цього створюють кібервійська, які мають відповідну форму підготовки для протидії агресору в кіберпросторі. Метою діяльності українських кібер військ загалом є перемога над агресором та звільнення окупованих територій. Тому, потенціал дій направлений на кіберпростір також формує методику контр впливу на російську інформаційну систему задля дестабілізації внутрішніх процесів у країні агресора.

Варто відзначити, що усі дії у кіберпросторі виходять за правові межі поведінки. Нормативних процедур впливу сторін один на одного в кіберпросторі не існує, що відповідно не обмежує сторони у використанні різних форм атак. А тому, попередження кіберзагроз у сучасній війні є складним процесом.

Список використаної літератури

1. Діордіца І. Поняття і зміст кіберзагроз на сучасному етапі. Підприємство, господарство і право. №4. 2017. URL: <http://pgp-journal.kiev.ua/archive/2017/4/22.pdf>
2. Держспецзв'язку: Статистика кібератак за чотири місяці війни. Урядовий портал. 30.06.2022. URL: <https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni>
3. Протистояння кіберзагрозам спільно. АрміяINFORM. 05.02.2022.URL: <https://armyinform.com.ua/2022/02/05/protystoyaty-kiberzagrozam-spilno/>

Ковальова Н.А.,
професор, доктор історичних наук, доцент,
ДВНЗ «Український державний
хіміко-технологічний університет»,
кафедра філософії та українознавства

«ЧЕРЕЗ КИЇВ ДО ЛЬВОВА!»: БОРОТЬБА СІЧОВИХ СТРІЛЬЦІВ ЗА СОБОРНУ УКРАЇНУ НАПРИКІНЦІ 1917 – НА ПОЧАТКУ 1918 рр.

З падінням Російської імперії у полонених галичан-українців (у Наддніпрянщині їх звали «австрійцями») відновилися сподівання на здобуття власної державності. До гуртування навколо Центральної Ради їх ніхто не змушував. Переважно це була молодь, діями якої керувало бажання слугувати українській справі – відродженню державності. Зокрема, двадцятип'ятирічний Роман Дашкевич Великдень 1917 р. у Забайкаллі зустрічав з мрією подолати тисячі кілометрів і якнайскоріше дістатися України, бо вояк має служити в українському війську і підтримати національну революцію [4, с. 289]. Одноосібно чи групами втікачі з російського полону намагалися добратися до Києва з різних куточків Росії, долаючи численні перешкоди, зокрема, шлях Івана Вислоцького з Уфи до Києва тривав пів року, а його брат Олександр добирався