Яструбецька Леся Сергіївна
доктор економічних наук, професор кафедри фінансів, грошового обігу і кредиту
Львівського національного університету імені Івана Франка
Голиш Софія Сергіївна
здобувач першого (бакалаврського) рівня вищої освіти
Львівського національного університету імені Івана Франка

DOI: https://doi.org/10.36059/978-966-397-335-7-31

ВИКОРИСТАННЯ КІБЕРАТАК В РОСІЙСЬКІЙ ГІБРИДНІЙ ВІЙНІ ТА ЇХ ВПЛИВ НА ФІНАНСОВУ БЕЗПЕКУ УКРАЇНИ

Гібридна агресія росії в Україні набула глибинного і довгострокового характеру, перейшовши у лютому 2022 року в гостру фазу – повномасштабне військове вторгнення. Її наслідки виявляються у масштабних людських, територіальних й економічних втратах. Російський режим використав й продовжує застосовувати в Україні широкий арсенал гібридних засобів – економічних, енергетичних, інформаційних тощо. Промислове шпигунство, корупція, диверсії та провокації, вчинені агресором, спрямовані на порушення безпеки інформаційно-технічної інфраструктури України, дискредитацію державних структур, зниження рівня фінансової безпеки країни.

Дослідженню особливостей гібридних конфліктів присвятили свої праці вітчизняні й іноземні вчені, зокрема такі: О. Базалук, В. Бірчак, В. Горбулін, Р. Додонов, Є. Магда, М. Нікіфоров, С. Рябенко, Р. Бернсбі, Е. Броу, К. Каунерт, Дж.А. Ларсен, Г. Лассвелл, Г. Ласконьяріас, В. Мічлін-Шапір, Е. Фолі та інші. Водночас, гібридні протистояння постійно еволюціонують у формах свого виявлення, особливо це стосується інформаційних інструментів агресії, що найбільше підлягають впливу стрімкого

технологічного розвитку. Відтак, застосування росією гібридних методів в інформаційній сфері, зокрема кіберзлочинів, потребує поглибленого вивчення та аналізу з метою напрацювання засобів протидії.

Впродовж останніх років чимало кібератак було вчинено на інформаційно-технічну інфраструктуру України, web-сторінки банківських установ та підприємств. Водночас перед початком війни рівень кіберзлочинності суттєво зріс, що може свідчити про використання агресором втручання в інформаційний простір держави з метою підготовки до повномасштабного вторгнення. Аналіз кібер-активності росії в Україні в цей період, дав змогу виявити кібер-атаки, які становили найбільшу загрозу:

– кібер-атака, реалізована росією 14 січня 2022 р., внаслідок якої зазнали зловмисного інформаційного втручання близько 70 державних веб-сайтів, серед яких web-сторінки Міністерства оборони України, Міністерства закордонних справ України, Державної служби України з надзвичайних ситуацій тощо;

– кібер-атака, вчинена росією 15-16 лютого 2022 р., що була спрямована на сайти органів державної влади України та банківські установи, серед яких – АТ КБ «ПриватБанк», АТ «Державний ощадний банк України»;

– кібер-атака, здійснена росією 23 лютого 2022 р., метою якої було дестабілізувати сайти державних установ України та банки, серед яких – сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Міністерства з питань стратегічних галузей промисловості України, Міністерства інфраструктури України, Міністерства аграрної політики України;

– кібер-атака, реалізована росією 24 лютого 2023 року, внаслідок якої зазнав деструктивного впливу сайт Київської ОДА, а також Державною службою спеціального зв’язку та захисту інформації України було виявлено масові e-mail листи з фішинговими посиланнями на приватні адреси українських військових і пов’язаних осіб.

На початку війни росії проти України було виявлено кібер-атаки на системи зв'язку газети «Kyiv Post», супутникову мережу «KA-SAT», урядові веб-сайти, пункт прикордонного контролю з метою перешкоджання виїзду біженців до Румунії, атаки на цифрову інфраструктуру України, що призвело до блокування доступу до фінансових послуг та енергетичних ресурсів. У березні 2022 р. продовжилися кібератаки з використанням шкідливого програмного забезпечення на урядові сайти й web-сторінки фінансових установ, а також на неурядові, благодійні організації, що перешкоджало розповсюдженню необхідних продуктів, медикаментів та інших видів гуманітарної допомоги. Крім того, здійснювалися фішингові атаки на громадян України, державні служби, а також кібер-атаки на постачальників електронних комунікаційних мереж та/або послуг, що призводило до порушення функціонування українських мереж.

Кібер-атаки, реалізовані росією в Україні впродовж березня 2022 р., спричинили також отримання несанкціонованого доступу до облікових даних українських громадян та організацій. У квітні 2022 р. російськими хакерами за допомогою троянської програми й шахрайського опитування через сторінки в соціальних мережах було перехоплено конфіденційну інформацію й окремі облікові дані уряду України, банківські та платіжні дані громадян. Також було реалізовано спробу перешкодити роботі електростанцій і припинити постачання електроенергії населенню України [2].

Початок війни в Україні характеризувався також зростанням дезінформаційних потоків в суспільстві, зокрема в березні 2022 року в ефірі одного з українських телеканалів з'явилося неправдиве повідомлення щодо заклику Президента України Володимира Зеленського до капітуляції [2].

Кіберзлочинність завдає вагомих фінансових і репутаційних втрат державі, суб'єктам господарювання та громадянам, суттєво знижуючи рівень їхньої фінансової безпеки. Водночас, кібер-атаки, що використовуються зловмисниками як інструменти гібридної війни, можуть спричинити глобальні наслідки для захисту національних інтересів країн та глобальної безпеки загалом. Відтак,

в цілях протидії російській агресії Україною було реалізовано комплекс заходів разом із урядами інших держав, зокрема 22 лютого 2022 р. до команди швидкого реагування на російські кібер-атаки було залучено 12 експертів з шести країн ЄС (Литва, Естонія, Хорватія, Польща, Нідерланди та Румунія).

Висновки. Спільні дії України й країн-союзниць дадуть змогу сформувати комплексні стратегічні підходи у протидії російській гібридній агресії, створити гнучкі та ефективні механізми реагування на кібер-загрози, що, своєю чергою, забезпечить зміцнення фінансової безпеки держави і суб'єктів підприємництва й підвищить оборонний потенціал у триваючій війні.

Література:

1. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua (дата звернення: 11.10.2023).

2. Пшетачник Я., Тарпова С. Війна Росії проти України: хронологія кібератак. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf (дата звернення: 29.10.2023).

3. Сайти банків та органів влади зазнали масової DDoS-атаки. URL: https://www.ukrinform.ua/ (дата звернення: 12.11.2023).