ВИКЛИКИ ТА ОРГАНІЗАЦІЙНО-ПРАВОВІ ЧИННИКИ УБЕЗПЕЧЕННЯ КІБЕРСФЕРИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ПІД ЧАС ПОВНОМАСШТАБНОЇ АГРЕСІЇ

Олександр Геннадійович ДЕМИДКО,

здобувач другого рівня вищої освіти гр. 756 юм Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Науковий керівник: *Шинкаренко І. Р., канд. юрид. наук, професор, професор кафедри права Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»*

«Скоординована та руйнівна кібератака Росії перед вторгненням в Україну показує, що кібератаки активно і стратегічно використовуються у сучасній війні, навіть якщо загроза та наслідки кібератаки не завжди видно громадськості. Кіберзагроза постійна і розвивається. Кібератаки можуть завдати великої шкоди нашій критичній інфраструктурі з фатальними наслідками» (міністр оборони Данії Мортен Бедсков)

Війна стала періодом випробування надійності організаційно-правового механізму захисту безпеки кіберпростору України та всього демократичного суспільства світу. Хроніка подій свідчить, що: атака на Україну російських хакерів почалася за кілька хвилин до масованого вторгнення армії; за інформацією Reuters, США, Велика Британія та ЄС офіційно звинуватили РФ у здійсненні масової кібератаки 24 лютого 2022 року, яка призвела до збою в роботі супутникового інтернет-сервісу Viasat за годину до початку війна. Це спричинило знищення «десятків тисяч» супутникових терміналів; на кінець листопада 2022 р. кількість кібератак на об'єкти енергосектору критичної інфраструктури склала понад 1,2 млн [1, с. 101-105; 2].

В той же час напередодні війни ще14 січня 2021 року після відомої кібератаки на сайти державних органів, виникла реальна потреба в термінових змінах на рівні українського законодавства щодо залучення сторонніх спеціалістів для пошуку помилок та вразливостей у програмних продуктах, інформаційно-комунікаційних системах.

За період 2022-2023 роки кібер інциденти у країнах світу нагадують фронтові сводки: Королівська пошта Великобританії стала жертвою ransomware; Міністерство громадських робіт і транспорту Коста-Рики постраждало; Угрупування Dark Pink атакує урядові та військові організації в Азії та Європі; Кібератака на постачальника послуг з обробки державних електронних даних торкнулася багатьох округів США; Серйозний недолік мобільного застосунку розкрив дані мільйонів індійських студентів [3].

© Демидко О. Г., 2023

Зроблений нами у грудні 2022 році аналіз думок науковців та практичних працівників у сфері національної безпеки взагалі та кібернетичної, зокрема, дозволяє визначити низку чинників, що створюють загрозу кібернетичній безпеці у сфері критичної інфраструктури: недостатній рівень координації зусиль різних установ та відомств, секторальних уповноважених органів щодо формування захисту, необхідного для протистояння загрозам у сфері кібербезпеки критичної інфраструктури; непрозорість розподілу обов'язків між певними відомствами, правоохоронними органами і силовими структурами України, що спеціалізуються на проблемах кіберзахисту та їх незадовільне кадрове забезпечення кваліфікованими фахівцями з цих питань; відсутність ефективної системи підготовки фахівців не тільки для правоохоронних органів, ф й служб кібербезпеки всіх суб'єктів господарювання; відсутність єдиного на законодавчому рівні понятійно-термінологічного поля кібербезпеки України, як головної складової інформаційної безпеки, а також системних нормативно-правових документів, які б регламентували діяльність служб кібербезпеки відомств, а також правоохоронних і силових структур у сфері кібернетичного захисту тощо [4, с. 168-171; 5, с. 206-217].

Зростаюча кількість кіберзлочинної діяльності на підприємствах, постійне вдосконалення інформаційних технологій і нові можливості «вдосконалення» інструментів реалізації злочинних задумів у сфері інформаційної та кібернетичної безпеки створюють економічні загрози для глобальних інформаційних мереж.

Підвищення рівня актуальності кіберзагроз різноманітним об'єктам визначається тим, що в умовах сьогодення низка безпекових чинників у щодо формування кримінально активного середовища у кіберпросторі: недостатньо ефективна нормативна база та система управління кібербезпекою на рівні об'єкт-фірма-регіон-держава; не завжди відповідність вимогам війни готовність реагувати на кібератаки; гальмування галузевими суб'єктами у сфері кібербезбеки залучення професійної спільноти щодо трансформації їх діяльності; нерегулярність моніторингу формування кіберзагроз конкретним об'єктам і як наслідок реактивність всієї системи кібербезпеки.

Означені чинники та кібератаки призводять до наступного: блокування систем управління критичною інфраструктурою; виведення з ладу критично важливих систем держави та бізнесу (веб-сайти, електронні державні сервіси для громадян та бізнесу, інтернет-магазини, акаунти ключових менеджерів тощо); втрата особистої, корпоративної та конфіденційної інформації; крадіжка персональних та фінансових даних, що призводить до виведення коштів; шкода діловій репутації компанії та втрата клієнтів як наслідок; матеріальні витрати на ліквідацію наслідків кіберінцидентів тощо.

Визнаючи той факт, що кіберзлочинність – основна загроза національній безпеці України та те, що вона особливо впливає на соціогуманітарну сферу та критичну інфраструктуру, підтримаємо пропозиції щодо:

Заходів на нормативно-творчому рівні: підготовка та виконання Плану заходів із реалізації Стратегії кібербезпеки на 2023 рік, на період воєнного стану, на період післявоєнної відбудови (першочергові дії-термін рік (стабілізаційні), дії створення сталої системи кібербезпеки (5 років), формування довгострокових інноваційних заходів правового, організаційного

© Демидко О. Г., 2023

та техніко-програмного змісту); продовження адаптації законодавства України до світових стандартів убезпечення кіберпростора за рахунок імплементації правових норм законодавства ЄС у сфері кібербезпеки тощо; визначити на нормативному рівні вимогу регулярного адаптування політику захисту кіберсфери на рівні держава-галузь-регон-«суб'єктита-об'єкти господарювання»-громадяни.

Заходів на організаційному рівні: посилення взаємодії між основними суб'єктами національної системи кібербезпеки України, налагоджувати конструктивне і швидке співробітництво; формування ефективної системи координації та міжнародної співпраці у сфері протидії кібербезагрозам; створення ефективної системи моніторингу, аналізу, інформування про нові загрози на рівні держава-галузь-регон-«суб'єктита-об'єкти господарювання»-громадяни; регулярне адаптування політику захисту кіберсфери на рівні держава-галузь-регіон-«суб'єкти-об'єкти господарювання»-громадяни; розробка системних організаційно-правових механізмів виявлення загроз кібербезпеці на ґрунті сучасної нормативної бази європейських стандартів, адміністративно-правових методик та іноваційних засобів та заходів реалізації державної політики у сфері забезпечення багаторівневої національної безпеки; забезпечення кібербезпеки, як складових елементу національної безпеки України; формування системи інформування державних органи, у випадках виявлення ознак потенційних кіберінцендентів.

Заходів на науково-освітньому рівні: з метою мінімізація збитків від кібератак, важливо побудувати систему наукового забезпечення виявлення та нейтралізації інцидентів на рівні галузевих, міжгалузевих лабораторій та ін; активізація співпраці та координації досліджень не тільки у технічній сфері а й з правового забезпечення убезпечення кіберпросторі на плятформі Національного Кластеру Кібербезпеки.

Список використаних джерел:

1. Загальна характеристика особливостей та проблем кібербезпеки в сучасній Україні. *Актуальні проблеми політики. 2022. Вип. 70. С. 101-105.* DOI https://doi.org/10.32782/app.v70.2022.16.

2. Війна Росії проти України почалася з кібер нападу на супутники. за годину до вторгнення були знищені «десятки тисяч» терміналів Viasat-itc.ua. *ITC.ua.* URL: https://itc.ua/ua/novini/vijna-rosiyi-protiukrayini-pochalasya-z-kibernapadu-na-suputniki-za-godinu-do-vtorgnennya-buli-nishheni-desyatkitisyach-terminaliv-viasat/

3. Огляд подій у сфері кібербезпеки. Січень 2023.URL: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_ 2023_ fin.pdf.

4. Демидко О. Г. Окремі аспекти забезпечення кібернетичної безпеки критичної інфраструктури України. *Протидія організованій злочинності: проблеми теорії та практики: Матеріали всеукраїнського науково-практичного семінару (м. Дніпро, 09 грудня 2022 р.).* Дніпро: Дніпроп. держ. ун-т внутр. справ. 2022. с. 168-171.

5. Mykola Nechyporuk, Volodymyr Pavlikov, Nataliia Filipenko, Hanna Spitsyna, Ihor Shynkarenko Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. Conference on Integrated Computer Technologies in Mechanical Engineering–Synergetic Engineering ICTM 2020: Integrated Computer Technologies in Mechanical Engineering. 2020 pp 206-217(Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago More information about this series at. URL: http://www.springer.com/series/15179 https://doi.org/10.1007/978-3-030-66717-7.

© Демидко О. Г., 2023