ІВАЩЕНКО Сергій Миколайович
доцент кафедри права Національної безпеки та правової роботи Військово-юридичного інституту Національного юридичного університету імені Ярослава Мудрого,полковник м. Харків

КАЛІБЕРДА Олександр Денисович
Військово-юридичний інститут Національного юридичного університету імені Ярослава Мудрого м. Харків

КІБЕРПЕЗПЕКА У КОНТЕКСТІ ГІБРИДНОЇ ВІЙНИ: АНАЛІЗ ДІЙ ПРОТИВНИКА ТА ЕФЕКТИВНІСТЬ ЗАХИСТУ

У сучасних умовах ведення гібридної війни кіберпростір перетворився на одне з ключових полів бойових дій, де інформаційна атака, злам критичної інфраструктури або дестабілізація державного управління можуть мати наслідки, не менш руйнівні, ніж традиційні військові дії. Україна з 2014 року перебуває в умовах постійної кіберзагрози з боку держави-агресора, а з початку повномасштабного вторгнення 2022 року ці загрози набули системного й масштабного характеру. Кібератаки, кампанії з дезінформації, навмисне знищення або зміна цифрових даних - все це перетворилось на складову агресивної політики ворога. З огляду на це, питання кібербезпеки стає надзвичайно важливим, як для охорони державного суверенітету, так і для безперебійної роботи всіх галузей суспільного життя.

Актуальність дослідження зумовлена необхідністю глибшого аналізу тактики дій противника в кіберпросторі та оцінки ефективності існуючих

механізмів кіберзахисту. Це дозволить визначити напрями вдосконалення національної системи безпеки в умовах постійної гібридної загрози.

Нормативно-правова база України визнає кібербезпеку важливою складовою національної безпеки. Згідно із Законом України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 року № 2163-VIII [1], до основних загроз у кіберпросторі віднесено спроби порушення стабільності функціонування об’єктів критичної інфраструктури, органів державної влади та систем зв’язку. Особливу увагу до кіберзагроз приділяє також Закон України від 21.06.2018 року № 2469-VIII «Про національну безпеку України» [2], де зазначено, що кіберзагрози є складовою загроз національній безпеці, а забезпечення кібербезпеки - однією з функцій сектору безпеки і оборони. Визначено також необхідність міжвідомчої взаємодії між суб’єктами безпеки для протидії гібридним формам впливу, зокрема у кіберпросторі.

Гібридна війна як форма сучасного конфлікту охоплює широкий спектр методів впливу, поєднуючи традиційні військові дії з нетрадиційними інструментами - політичними, економічними, інформаційними, психологічними та кібероперaціями. Водночас, гібридна війна передбачає скоординоване використання відкритих і прихованих дій, спрямованих на дестабілізацію держави-жертви, підрив її національної безпеки та зниження оборонного потенціалу без формального оголошення війни. Одним із ключових чинників гібридної боротьби беззаперечно є кіберкомпонент, що охоплює хакерські наступи на державні та військові інформаційні мережі, проникнення в інфраструктурні об'єкти, поширення неправдивої інформації, втручання у канали зв'язку та намагання вплинути на погляди населення.

Кібероперації в умовах гібридної війни виконують не лише допоміжну функцію, а часто є самостійним інструментом впливу, який дозволяє завдати шкоди противнику без фізичного вторгнення. Особливістю кіберзагроз є їхня складність для ідентифікації, висока швидкість реалізації, глобальний масштаб і можливість збереження анонімності виконавців. Кіберпростір стає ареною постійного прихованого протистояння, де атаки на критичну інфраструктуру,

банківську систему, системи зв'язку та органи державної влади виступають потужним інструментом стратегічного тиску. У період повномасштабної агресії з 2022 року кількість кібератак зросла в рази. Зокрема, у лютому 2022 р. російські хакери здійснили численні кібератаки на Україну, які здебільшого полягали в атаках середнього та малого масштабу і включали шпигунство, інформаційно-психологічні операції та гібридну війну, яка поєднує цілеспрямовані кібератаки з кінетичними військовими ударами по землі [3, с. 122]. Також, було зафіксовано масштабні DDoS-атаки на сайти Міністерства оборони, Збройних Сил України, державних банків. У березні-квітні активно використовувалися програми-стирачі даних - HermeticWiper, IsaacWiper, CaddyWiper, що були спрямовані на знищення даних у державних і комерційних структурах. Ці атаки супроводжувалися інформаційно-психологічними операціями, дезінформацією та спробами вплинути на громадську думку.

Проблеми кіберзахисту України зумовлені низкою причин. Головні з них - розрізненість законів, недостатня координація між суб'єктами національної системи кібербезпеки, брак потрібної техніки та спеціалістів, плюс обмежена участь у світових системах протидії кіберзагрозам. Суттєвим викликом є невисокий рівень обізнаності з кібербезпекою серед держслужбовців та громадян. Для підвищення ефективності кіберзахисту необхідно удосконалити законодавствао з акцентом на чітке визначення повноважень усіх суб'єктів, розвиток технічної інфраструктури, запровадження системи підготовки фахівців з кібербезпеки, створення оперативних центрів реагування на кіберінциденти та розширити міжнародну співпрацю у сфері кібероборони.

Таким чином, кібербезпека в умовах гібридної війни набуває стратегічного значення як один із ключових елементів національної безпеки. Кібероперації стали потужним інструментом агресії, здатним паралізувати функціонування державних інституцій, підірвати довіру до влади та створити хаос у суспільстві без застосування фізичної сили. Аналіз вітчизняного законодавства свідчить про наявність основ для побудови ефективної системи кіберзахисту, однак на практиці вона потребує суттєвого вдосконалення - як у нормативно-правовому,

так і в організаційному вимірах. Підвищення спроможностей держави у сфері кібербезпеки має базуватися на міжвідомчій взаємодії, технічній модернізації, підготовці фахівців та посиленні міжнародного співробітництва, що дозволить ефективно протидіяти гібридним загрозам у цифровому просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII (з наступ. змін. та доповн.). URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20250403#Text.

2. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII (з наступ. змін. та доповн.). URL: https://zakon.rada.gov.ua/laws/show/2469-19/ed20240809#Text.