Гуленко Д.Б.,
здобувач освітньо-наукового рівня доктор філософії
за спеціальністю D4 «Публічне управління та адміністрування»
Науковий керівник: **Супрунова І. В.,**
д. н. держ. упр., професор кафедри національної безпеки, публічного управління та адміністрування
Державний університет "Житомирська політехніка"

ТРАНСФОРМАЦІЯ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ: ВИКЛИКИ ВОЄННОГО СТАНУ ТА ЄВРОІНТЕГРАЦІЙНІ ПРОЦЕСИ

Повномасштабна військова агресія російської федерації проти України стала каталізатором фундаментальних змін у глобальній архітектурі безпеки, остаточно закріпивши кіберпростір як повноцінний п'ятий домен ведення бойових дій. Якщо до 2022 року кіберзагрози розглядалися переважно в контексті шпигунства або фінансових збитків, то сучасна війна продемонструвала їхню деструктивну спроможність впливати на кінетичні операції та життєдіяльність держави. Стратегія кібербезпеки України, яка затверджувалася в умовах «гібридного миру», зіткнулася з безпрецедентними викликами, що вимагали миттєвої адаптації нормативно-правової бази, технічної інфраструктури та організаційних підходів.

Моніторинг кіберпростору 2022-2025 років засвідчує структурну мутацію ворожих стратегій. Якщо на початку вторгнення превалювали деструктивні кампанії з використанням вайперів для паралічу інфраструктури, то нині пріоритетом агресора стало приховане шпигунство та компрометація ланцюгів постачання [1]. Зафіксований CERT-UA ріст кількості інцидентів на 36% (2023 рік) та їх безпосередня координація спецслужбами рф змушує Україну відходити від класичного захисту на користь доктрини «активної оборони».

Вагомим аспектом забезпечення стійкості стала децентралізація обробки даних. Нормативне врегулювання цього процесу через Закон «Про хмарні послуги» та Постанову КМУ № 263 створило правове підґрунтя для розміщення державних інформаційних ресурсів за межами країни [2]. Залучення потужностей глобальних хмарних провайдерів (зокрема екосистем Amazon Web Services та Microsoft) дозволило нівелювати загрозу втрати інформації внаслідок кібернетичних атак на фізичні дата-центри. Зазначена модель «цифрового

суверенітету» без фізичної прив'язки до території наразі розглядається міжнародними партнерами як еталонна практика для збереження керованості державою в умовах війни.

Головне, що зараз формує нашу систему кіберзахисту - це необхідність нормативної конвергенції з правом ЄС. Статус кандидата на вступ до Євросоюзу поставив перед нами завдання впровадити Директиви NIS2 (Network and Information Security Directive), яка докорінно змінює філософію захисту критичних об'єктів. На відміну від попередніх регуляторних актів, ця директива не лише охоплює ширше коло галузей (зокрема хімічну промисловість, поштові сервіси, утилізацію відходів), але й запроваджує імперативні норми щодо оперативного звітування про кіберінциденти [3].

Відповідно, процес адаптації українського законодавства до стандартів NIS2 вимагає розв'язання комплексу завдань:

- ✓ уніфікація управління ризиками (впровадження обов'язкових стандартів кіберзахисту для керівників підприємств критичної інфраструктури із запровадженням персональної відповідальності за їх порушення);
- ✓ швидкість реагування (Директива вимагає надання раннього попередження про значний інцидент протягом 24 годин, що потребує повної автоматизації процесів обміну інформацією між суб'єктами кібербезпеки та державними центрами реагування (CERT-UA, НКЦК));
- ✓ захист ланцюжків постачання (організації зобов'язані враховувати ризики, пов'язані з їхніми підрядниками та постачальниками ПЗ, що є критично важливим в умовах використання ворогом вразливостей стороннього софту).

Співпраця з західними партнерами вийшла на зовсім інший рівень. Зокрема, ініціювання «Талліннського механізму» (грудень 2023 року) дозволило трансформувати розрізнену донорську допомогу в системну стратегію посилення українських кіберспроможностей [4]. Паралельно з цим,

інтенсифікація діалогу з Брюсселем прискорює входження України до європейського простору кібербезпеки та Єдиного цифрового ринку.

Не менш гостро постає проблема кадрового голоду, ускладнена стрімкою експансією штучного інтелекту. Технології ШІ сьогодні виступають як засобом масштабування ворожих кампаній (автоматизований фішинг, генерація експлойтів), так і безальтернативним інструментом аналітиків SOC-центрів для роботи з Big Data. Ця суперечність змушує нас повністю переосмислити освітніх підходів: пріоритетом має стати підготовка фахівців, здатних ефективно протидіяти саме алгоритмічним загрозам.

Наша майбутня безпека залежить від того, як ми поєднаємо три ключові елементи: замість ситуативного реагування сформовано модель превентивної протидії. Архітектура стійкості майбутнього залежатиме від синергії трьох компонентів: повної нормативної інтеграції з ЄС (стандарти NIS2), поглиблення технологічної децентралізації та інвестування в інтелектуальний потенціал галузі. Сьогодні Україна фактично еволюціонує зі статусу споживача безпекової допомоги у ключового експортера унікального бойового досвіду для всієї європейської спільноти.

Список використаних джерел

1. Російські хакери змінили тактику атак на Україну – звіт Держспецзв'язку за І півріччя 2024 року. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/news/russian-hackers-adopting-new-tactics-ssscip-report
2. Про деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану: Постанова Кабінету Міністрів України від 12.03.2022 р. № 263. *Урядовий портал*. URL: https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263

3. Директива (ЄС) 2022/2555 Європейського Парламенту і Ради від 14 грудня 2022 року про заходи високого спільного рівня кібербезпеки в межах Союзу (NIS2 Directive). *Official Journal of the European Union*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

4. Талліннський механізм: Україна та країни-партнери підписали спільну заяву щодо посилення кіберпідтримки. *Державна служба спеціального зв'язку та захисту інформації України*. URL: https://mfa.gov.ua/news/tallinnskij-mehanizm-ukrayina-ta-mizhnarodni-partneri-zapochatkuvali-novij-instrument-spivpraci-u-kiberprostori