УДК 004.056.53

Даценко А. В., здобувач вищої освіти;
Яворська Т. М., доцент, доцент кафедри інформаційних систем управління;
Донецький національний університет імені Василя Стуса

КІБЕРБОРОТЬБА Й КІБЕРЗАХИСТ ЯК ОДНІ З КЛЮЧОВИХ ЕЛЕМЕНТІВ ГІБРИДНОЇ ВІЙНИ

Ключові слова: кіберборотьба, кіберзахист, гібридна війна, кібервійська, кіберкомандування.

Вступ. У воєнний час життєво актуальним є завдання щодо розвитку національної системи кіберзахисту держави, адже ворог проводить активні деструктивні дії не тільки у фізичному, а й у кібер- та інформаційному просторах. Кіберзахист та кіберборотьба наразі вважаються одними із головних складників гібридної війни. Україна є учасником гібридної війни, і відповідно кібервійни. Скоординовані зусилля наших військових, спецслужб, вітчизняної кіберспільноти, фахівців з протидії дезінформації сприятимуть зміцненню кіберзахисту нашої держави.

Актуальність. Поняття кіберборотьби існувало в українському інформаційному просторі завжди. Від початку повномасштабного вторгнення цей аспект набув ширшого свого застосування та актуальності. Ще до 2022 року росія активно здійснювала кібератаки на інфраструктуру, держоргани, інформаційно-комунікаційні мережі України.

Кіберборотьба та кіберзахист вважаються ключовими складниками гібридної війни через їх потенційну здатність вплинути на інформаційні системи, економіку, інфраструктуру та загальний порядок у країні або регіоні. Ці методи можуть використовуватися для впливу на суспільство, збурення стабільності та порушення нормального функціонування країни чи регіону.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України»: «кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем» [1].

Гібридна війна (англ. *hybrid warfare*) – це різновид ескалації конфліктів, властивий для XXI століття, що поєднує застосування державних та недержавних, традиційних і нетрадиційних стратегій, ресурсів, засобів, методів підривної діяльності, механізмів кібервійни з метою досягнення певних політичних цілей [2].

Кібервійна (англ. *cyberwarefare*) – це комп’ютерне протистояння у просторі інтернету [3].

Від моменту повномасштабного вторгнення попит на удосконалення знань із такого сектору, як-от кібербезпека, неймовірно зріс. В Україні період 2022–

2023 років характеризується появою рекордної кількості навчальних проєктів і можливостей, створених відповідно для українців будь-якої вікової категорії.

У березні 2022 року Міністерство цифрової трансформації України започаткувало освітній процес **re/start in cyber.** Ця програма складається з двох етапів:

1. Проходження онлайн-курсу з основ кібербезпеки на базі Toronto Metropolitan University, що забезпечуватиме набуття теоретичних знань та практичних навичок.

2. Підготовка до майбутнього працевлаштування за участі рекрутингової компанії BazaIT, під час якої учасники матимуть змогу ознайомитися з правилами написання CV (професійного резюме) та проходження співбесіди з роботодавцями [4].

Учасники цієї програми отримують всесвітньо визнаний сертифікат Foundational Cybersecurity Technologies (GFACT). Тобто зі впровадженням усе більшої кількості освітніх програм у сфері кіберпростору поповнюється надзвичайно важливий інтелектуально-технологічний складник нашої держави, який сприяє розвитку інформаційного фронту.

Українські кібервійська (ЗСУ) беруть початок своєї активної діяльності у кіберпросторі з 2010 року. В Україні була ратифікована Конвенція про кіберзлочинність. Натомість, у США вже було чинне кіберкомандування як окремий сектор їх збройних сил.

Під час структурування поняття кіберборотьби на її відповідні підвиди було виокремлено три окремі напрями: **кіберрозвідка (кібердорозвідка), кібервплив і кіберзахист.** Ці сектори тісно взаємопов'язані між собою, але кожен з них має свою мету, напрями вивчення, застосування.

Усі складники всередині кіберкомандування повинні взаємодіяти між собою. Кожне управління має на меті контролювати виконання завдань, що стосуються напряму, підлягає під критерії їх діяльності (рис. 1).

Рисунок 1 – Класифікація кіберкомандування [5]

Метою діяльності кіберсил Збройних Сил України є захист суверенітету держави та відсіч збройній агресії в кіберпросторі, проведення оборонних і наступальних операцій у кіберпросторі.

Основними функціями кібервійськ є:

- ведення кіберрозвідки, кібердорозвідки;
- планування та проведення оборонних і наступальних кібероперацій (операцій у кіберпросторі);
- підтримка інформаційних, психологічних операцій у кіберпросторі;
- організація виконання в межах компетенції заходів з підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони), координація виконання завдань з підготовки до кібероборони органами виконавчої влади, органами місцевого самоврядування та іншими складниками сил оборони [5].

Висновки

Наразі Україна перебуває на інформаційній передовій кібервійни. Досвід, який ми отримуємо під час боротьби з ворогом, робить наших кіберспеціалістів лідерами на світовому ринку, збільшується попит на українські освітні проєкти серед фахівців за кордоном. Можемо зробити висновок, що галузі кіберборотьби й кіберзахисту в Україні й надалі активно розвиватимуться, розширюватимуться й залучатимуть нові таланти задля безпеки країни.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України: Закон України № 2163-VIII 2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 11.11.2023).

2. Гібридна війна. *Велика Українська Енциклопедія: вебсайт.* URL: https://vue.gov.ua/Гібридна_війна (дата звернення 11.11.2023).

3. Актуальна тема – інтерв'ю. На часі створення дієвої системи кібероборони держави – Олександр Федієнко. *АрміяInform: вебсайт.* URL: https://armyinform.com.ua/2022/10/21/na-chasi-stvorennya-diyevoyi-systemy-kiberoborony-derzhavy-oleksandr-fediyenko/ (дата звернення 13.11.2023).

4. Кіберпезпека в Україні: шляхи розвитку та можливості. *Мультимедійна платформа іномовлення України. Укрінформ: вебсайт.* URL: https://www.ukrinform.ua/amp/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення 12.11.2023).

5. Володимир Павленко, Вадим Лєднєй – пост (інтерв'ю): вебсайт. URL: https://lb.ua/news/2023/01/31/544318_vadim_liedniey_metoyu_diyalnosti.html (дата звернення 13.11.2023).