УДК 004.056

Радецька А. О.
Куперштейн Л. М.

КІБЕРЗБРОЯ ЯК ЕФЕКТИВНИЙ НЕВІД'ЄМНИЙ ІНСТРУМЕНТ ВІЙСЬКОВОГО КОНФЛІКТУ

Анотація
Робота присвячена дослідженню використання кіберзброї в умовах військової агресії. Проаналізовано основні напрямки її застосування та наслідки, спричинені цим.
Ключові слова: кіберзброя, кібератаки, військова агресія.

Abstract
The work is devoted to the study of the use of cyber weapons in conditions of military aggression. The main directions of its application and the consequences caused by it are analyzed.
Keywords: cyber weapons, cyber attacks, military aggression.

Вступ

Кожен з історичних етапів розвитку людства супроводжувався і певним розвитком технологій. Наслідком цього було, відповідно, і постійне оновлення видів озброєння. Сьогодні людство остаточно увійшло в нову еру, яку вже з упевненістю можна назвати мережевою.

Відповідно до сучасного стану розвитку технологій з'являються і нові засоби ведення війни. Серед інших можна виділити також такі, що застосовуються у кіберпросторі. Засобами є нові види озброєнь, що спираються на використання інформаційно-комп'ютерних технологій.

Результати дослідження

Єдиного визначення поняття кіберзброя на даний період часу ще не запропоновано. Однак, проаналізувавши наявні найбільш поширені визначення, можна виділити окремі ознаки та створити загальне поняття.

У Оксфордському словнику поняття кіберзброя представлено як певну частину комп'ютерного програмного забезпечення або апаратного забезпечення, що використовується для ведення кібервійни [1].

У словнику Макмілана подається наступне визначення терміну кіберзброя: шкідливе програмне забезпечення, що використовується однією країною проти іншої для політичних, військових або розвідувальних цілей [2].

Компанія Heimdal Security, напрямком роботи якої є забезпечення та надання послуг із кіберзахисту, надає наступне визначення: термін «кіберзброя» означає просунутий і складний фрагмент коду, який можна використовувати для військових або розвідувальних цілей. Компанія стверджує, що термін нещодавно з'явився з військової галузі, щоб назвати шкідливе програмне забезпечення, яке можна використовувати для доступу до комп'ютерних мереж супротивника [3].

П. Паганіні визначає кіберзброю як певний комп'ютерний код, який використовується або призначений для використання з метою загрози або заподіяння фізичної, функціональної або психічної шкоди і структурам, системам або живим істотам [4].

Отже, після аналізу вище наведених визначень, можна зробити висновок, що під терміном «кіберзброя» можна вважати певне програмне забезпечення або сукупність програм, які створені та/або використовуються з метою завдання певної шкоди супротивнику та/або отримання певної військової переваги, наприклад, як встановлення контролю над інформаційними ресурсами (телебачення, радіо, інтернет тощо), безпілотними апаратами, виведення з ладу апаратури супротивника, знищення або заміна важливої інформації і т.п.

Після дослідження та аналізу відомі випадків і прецедентів застосування кіберзброї під час ведення військових дій, було визначено основні напрямки та види кібератак з використанням кіберзброї. Наслідки використання кіберзброї можуть бути найрізноманітнішими і привести до важких деструктивних результатів.

Вандалізм – паплюження інтернет сторінок, заміни їх змісту образливими чи пропагандистськими зображеннями. Наслідком є завдання удару по авторитету держави як у світі, так і серед населення. Яскравим прикладом можна вважати атаку на низку державних сайтів України в січні 2022 року, коли при спробі їх відкриття відображався не вміст сайту, а картинка з попередженням українською,

російською та польською мовами про покарання українців за діяння ОУН УПА [5].

Пропаганда – розсилка звернень пропагандистського характеру або вставка пропаганди в зміст інших інтернет сторінок, розповсюдження фейкових новин. Наслідком є просування вигідної точки зору на певні події з боку ворога, а також дезорієнтації населення [6].

Збір інформації – зламування приватних сторінок чи серверів для отримання інформації чи її заміни на фальшиву. Наслідком є отримання доступу до важливої інформації, оприлюднення якої здатне нанести значну шкоду противнику. Прикладом є злом баз даних Роскомнагляду та Центробанку Росії в березні 2022 [7-8].

Відмова сервісу – атаки на різноманітні сайти, сервіси та системи, основна мета яких порушення чи унеможливлення їх коректної роботи. Яскравим прикладом є організовані масові DDoS-атаки українськими кібервійськом на державні, медіа та фінансові сервіси противника протягом усього військового вторгнення російської федерації в Україну [8].

Атаки на об'єкти критичної інфраструктури – атаки на системи, які забезпечують життєдіяльність міст, їх інфраструктури, таких як телефонні та банківські системи, водопостачання, електроенергії, пожежної охорони, транспорту тощо. Наслідками є порушення функціонування важливих систем, організацій та структур, що може призвести до колапсу та масової паніки серед населення. Прикладом є регулярні атаки на українські банківські сервіси, мобільні оператори та провайдери з боку ворога від самого початку повномасштабних військових дій [8].

Висновки

В результаті аналізу випадків застосування кіберзброї під час ведення військових дій було встановлено, що її використання є надзвичайно дієвим засобом боротьби із ворогом. Застосування кіберзброї не несе за собою жодних прямих людських втрат з боку атакуючого, однак може завдати значних руйнувань супротивнику чи дестабілізувати його. Кожна країна повинна бути забезпечена сучасною кіберзброєю як наступального так і оборонного характеру, оскільки супротивника не потрібна недооцінювати і потрібно вміти ефективно захищатися.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. English Oxford Living Dictionaries. [Electronic resource]. – Access mode : https://en.oxforddictionaries.com/definition/cyberweapon
2. Macmillan Dictionary. [Electronic resource]. – Access mode : http://www.macmillandictionary.com/dictionary/british/cyber-weapon
3. Heimdal Security. [Electronic resource]. – Access mode : https://heimdalsecurity.com/glossary/ cyber-weapon.
4. Pierluigi Paganini. Cyber Weapons. – April 3, 2012. [Electronic resource]. – Access mode : http://securit
5. Сайти Дія, МЗС, ДСНС, МОУ зламали хакери URL: https://ilounge.ua/ua/blog/ sajty-diya-vzlomali-hakery
6. На сайтах українських громад опублікували фейкове звернення Зеленського. URL:https://zaxid.net/na _ofitsiynih_saytah_otg_opublikuvali_feykove_zvernennya_zelenskogo_n1537449
7. Зламали Роскомнагляд і злили дані в мережу URL: https://www.unian.ua/world/anonymous-zlamali-roskomnaglyad-i-zlili-dani-vme rezhu-novini-svitu11738668.html?utm_source=unian&utm_medium=read_more _news&utm_ca aign=read_more_news_in_post
8. Кібервійна проти Росії: як з окупантами борються в мережі URL: https://rayon.in.ua/news/491247-internet-sanktsii-dlya-rosii-onovlyuetsya.yaffairs.co/wordpress/3896/intelligence/ cyber-weapons.html.

Радецька Анастасія Олександрівна — студентка групи 1БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м.Вінниця, e-mai: an.radetska@gmail.com

Куперштейн Леонід Михайлович к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця email: kupershtein.lm@gmail.com

Radetska Anastasiia O. — Student of Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, e-mail: an.radetska@gmail.com

Kupershtein Leonid M. — PhD, Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, email: kupershtein.lm@gmail.com