УДК [004.946.056:355.01](043.2)

В. О. Безруков

Кіберзагрози як новий вимір ведення війни

Вінницький національний технічний університет

Анотація:

У статті розглядається феномен кіберзагроз як нового виміру ведення війни в умовах сучасного технологічного розвитку. Аналізуються основні види кіберзагроз, включаючи атаки на критичну інфраструктуру, кібершпигунство, дезінформаційні кампанії та використання шкідливого програмного забезпечення. Досліджуються наслідки таких атак для національної безпеки, економіки та суспільства. Окрема увага приділяється стратегіям кібероборони, міжнародному співробітництву та механізмам протидії кіберзагрозам у воєнний час.

Ключові слова: кіберзагрози, кібербезпека, інформаційна війна, кібератаки, критична інфраструктура, кібершпигунство, дезінформація, кібервійна, національна безпека, цифрові технології.

Abstract:

The article examines the phenomenon of cyber threats as a new dimension of warfare in the context of modern technological development. The main types of cyber threats are analyzed, including attacks on critical infrastructure, cyber espionage, disinformation campaigns, and the use of malicious software. The consequences of such attacks for national security, the economy, and society are explored. Special attention is given to cyber defense strategies, international cooperation, and mechanisms for countering cyber threats in wartime.

Keywords: cyber threats, cybersecurity, information warfare, cyber attacks, critical infrastructure, cyber espionage, disinformation, cyber war, national security, digital technologies.

Вступ

Сучасний світ дедалі більше залежить від цифрових технологій, що створює нові виклики у сфері безпеки. Одним із таких викликів є кіберзагрози, які набули особливого значення в умовах гібридних конфліктів та сучасної воєнної стратегії. Традиційні війни вже не обмежуються фізичними бойовими діями – поряд із ними активно розгортається кібернетичне протистояння, яке охоплює атаки на критичну інфраструктуру, інформаційні війни, кібершпигунство та деструктивні дії у віртуальному просторі

Кібератаки дозволяють завдавати значних збитків державам та організаціям без безпосереднього використання зброї, що робить їх ефективним інструментом у веденні сучасної війни. Крім того, технологічний розвиток сприяє зростанню складності таких атак, що ускладнює їх виявлення та протидію. У зв’язку з цим виникає необхідність розробки ефективних механізмів кіберзахисту, міжнародного співробітництва у сфері кібербезпеки та адаптації військових стратегій до нових викликів цифрової епохи.

Мета цього дослідження – проаналізувати основні види кіберзагроз, їх вплив на безпеку держави та методи протидії їм у контексті сучасної війни.

Результати дослідження

Кіберзагрози є одним із ключових елементів сучасної військової доктрини багатьох країн, оскільки вони дозволяють впливати на супротивника без застосування фізичної сили [1, с. 15]. Використання кіберпростору як арени бойових дій дає змогу завдавати шкоди стратегічно важливим об’єктам, підривати економічну стабільність, маніпулювати громадською думкою та дезорганізовувати військові операції [1, с. 37]. Кібератаки можуть здійснюватися різними методами, серед яких найбільш поширеними є атаки на критичну інфраструктуру, кібершпигунство, дезінформаційні кампанії та використання шкідливого програмного забезпечення [1, с. 94]. Атаки на критичну інфраструктуру спрямовані на порушення роботи енергосистем, фінансових установ, транспортних мереж та військових комунікацій [1, с. 120]. Такі дії можуть призвести до масштабних економічних втрат, а також створити хаос у державному управлінні та системах безпеки [2, с. 65].

Кібершпигунство є ще одним небезпечним видом кіберзагроз, що полягає у викраденні важливих державних, військових та корпоративних даних [2, с. 188]. Отримана інформація може бути використана для отримання стратегічної переваги або для подальших атак [2, с. 242]. Дезінформаційні кампанії мають на меті маніпулювання громадською думкою шляхом поширення фейкових новин, викривлення фактів та створення хибних наративів [3, с. 75]. Особливо важливу роль відіграють соціальні мережі, через які швидко поширюється неправдива інформація [3, с. 156]. Це може впливати на політичні процеси, підривати довіру до уряду та дестабілізувати суспільство [3, с. 180]. Також широко використовуються віруси, трояни та програми-вимагачі, які можуть знищувати або викрадати інформацію, паралізуючи роботу державних органів або важливих установ [4, с. 99]. Головна особливість кіберзагроз полягає в їхній невидимості, анонімності та можливості здійснення атак на значні відстані без фізичного втручання, що значно ускладнює їхнє виявлення та протидію [4, с. 210].

Сучасні кібератаки стають дедалі складнішими та технологічно досконалішими, що вимагає від держав і компаній постійного вдосконалення механізмів захисту [5, с. 85]. Основними методами здійснення кіберзагроз є DDoS-атаки, які спрямовані на перевантаження серверів, що призводить до порушення їхньої роботи та зниження доступності важливих інформаційних ресурсів [5, с.134]. Такі атаки використовуються для дестабілізації державних та фінансових установ, а також для блокування критично важливих онлайн-сервісів [6, с.17]. Фішингові атаки є методом соціальної інженерії, що передбачає обманне отримання конфіденційної інформації, зокрема паролів, банківських даних або доступу до закритих систем. Зазвичай фішинг здійснюється через електронні листи або підроблені вебсайти. Zero-day атаки використовують невідомі або неперекриті вразливості програмного забезпечення до моменту їх офіційного виправлення. Це один із найнебезпечніших методів кіберзагроз, оскільки захист від таких атак фактично відсутній до моменту їх виявлення. Використання ботнетів передбачає масове зараження пристроїв вірусами, що дозволяє хакерам централізовано здійснювати атаки, наприклад, на урядові установи або великі компанії. Розповсюдження шкідливого програмного забезпечення, такого як віруси, трояни та програми-вимагачі, може уражати стратегічно важливі комп'ютерні системи, викрадати дані або їх шифрувати з метою вимагання викупу.

Висновки

У сучасних умовах кіберзагрози стали не лише допоміжним інструментом у військових конфліктах, а й повноцінним засобом ведення війни. Вони охоплюють широкий спектр дій – від атак на критичну інфраструктуру та кібершпигунства до інформаційних операцій, спрямованих на дестабілізацію суспільства та маніпулювання громадською думкою. Головна небезпека кібератак полягає в їхній невидимості, анонімності та глобальному охопленні, що дозволяє здійснювати атаки на значній відстані без необхідності фізичного втручання. Проаналізовані методи кіберзагроз, такі як DDoS-атаки, фішинг, використання ботнетів, програми-вимагачі та експлуатація вразливостей програмного забезпечення, демонструють їхню високу ефективність у підриві економічної та військової стабільності. Кібератаки можуть призводити до значних фінансових збитків, порушення роботи державних установ, витоку конфіденційної інформації та навіть впливати на політичні процеси, включаючи вибори. Саме тому кібербезпека стає одним із головних пріоритетів національної безпеки у XXI столітті. В умовах цифровізації всі аспекти життєдіяльності держави та суспільства залежать від захисту інформаційних систем. Відтак адаптація до нових викликів, розробка ефективних механізмів протидії кіберзагрозам та посилення міжнародної взаємодії є критично важливими для забезпечення стабільності, суверенітету та безпеки держав у сучасному світі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Clarke R. A., & Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. HarperCollins, 2010. 304 с.
2. Rid T. Cyber War Will Not Take Place. Oxford University Press, 2013. 256 с.
3. Singer P. W., & Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2014. 320 с.
4. Nye J. The Future of Power. PublicAffairs, 2011. – 320 с.

5. Libicki M. C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press, 2007. 320 с.
6. Волцман Р. The Weaponization of Information: The Need for Cognitive Security. RAND Corporation, 2017. 142 с.

Безруков Владислав Олександрович – студент групи 2КІ-23б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bezrukovvladyslav8578212@gmail.com

Bezrukov Vladyslav O. – student, 2CE-23B, Faculity of information Technologies and Computer Engeneering, Vinnytsa National Technical University, email: bezrukovvladyslav8578212@gmail.com

Науковий керівник – Герасимов Тимофій Юрійович – доктор історичних наук, доцент кафедри суспільно-політичних наук, Вінницький національний технічний університет, м. Вінниця, Україна, e-mail: timger84@gmail.com

Supervisor – Gerasymov Tymophiy – doctor of historical sciences, assistant of professor of Social and Political Sciences, Vinnytsia National Technical University, Vinnytsia. e-mail: timger84@gmail.com