3. Про проект. MAVKA the forest song | Повнометражний анімаційний фільм Мавка. URL: https://mavka.ua/uk/about (дата звернення: 10.01.2024).

4. «Мавка» і Lviv Croissants: як українське мистецтво та бізнес досягають спільної мети. MAVKA the forest song | Повнометражний анімаційний фільм Мавка. URL: https://mavka.ua/uk/news/text/34-939e46 (дата звернення: 3.01.2024).

5. До Дня вишиванки «Укрпошта» випустила дві нові марки. Кіровоградщина отримала майже 2,5 тисячі блоків| Суспільне Кропивницький. URL: https://suspilne.media/kropyvnytskiy/74707-do-dna-visivanki-ukrposta-vipustila-dvi-novi-marki-kirovogradsina-otrimala-majze-25-tisaci-blokiv/ (дата звернення: 5.01.2024).

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ГІБРИДНА ВІЙНА В КОНТЕКСТІ ГЛОБАЛЬНИХ ТА НАЦІОНАЛЬНИХ ІНТЕРЕСІВ

БРОВЧЕНКО К.,
здобувач вищої освіти, факультет торгівлі та маркетингу,
Державний торговельно-економічний університет, Україна
ОНОФРІЙЧУК І.,
доцент кафедри журналістики і реклами,
Державний торговельно-економічний університет, Україна

Інформаційна безпека є важливою складовою сучасної національної та глобальної безпеки. У епоху глобалізації інформаційні війни та гібридні конфлікти набувають нового значення. Особливо актуальним це питання стало у світлі російсько-українського конфлікту, де інформаційні атаки є важливим інструментом ведення гібридної війни. Це дослідження розглядає виклики інформаційної безпеки в контексті глобальних та національних інтересів.

Інформаційна безпека – це захист інформаційних ресурсів держави та її громадян від загроз, спрямованих на порушення їх конфіденційності, цілісності та доступності. На глобальному рівні це стосується захисту інформаційних систем від кібератак, дезінформації

та інших видів інформаційного впливу, які можуть поставити під загрозу національну безпеку.

Національні інтереси в інформаційній сфері – визначальні потреби людини (громадянина), суспільства і держави в інформаційній сфері, реалізація яких гарантує інформаційний суверенітет, а також прав та свобод людини в інформаційній сфері.

Гібридна війна - нове поняття в політичному житті планети. Вперше з'явилося в військових документах США і Великобританії на початку XXI століття. Дане поняття означає підпорядкування певній території за допомогою інформаційних, електронних, кібернетичних операцій, в поєднанні з діями збройних сил, спеціальних служб і інтенсивним економічним тиском.

Приклад: Російсько-українська війна

Під час російсько-української війни інформаційні атаки були використані для дискредитації української влади та впливу на міжнародну громадську думку. Наприклад, в 2014 році, під час анексії Криму, Росія активно поширювала дезінформацію через медіа та соціальні мережі для виправдання своїх дій на міжнародній арені. Відома операція з використанням «тролів» та фейкових акаунтів у соціальних мережах мала на меті вплинути на міжнародне сприйняття конфлікту.

Іншим прикладом є кібератака на енергетичну інфраструктуру України в грудні 205 року, коли хакери, пов'язані з Росією, здійснили атаку на українські електромережі, залишивши без електропостачання частину Західної України. Це перший задокументований випадок, коли кібератака спричинила відключення електроенергії [1,3].

Глобальні виклики та національні стратегії

Країни стикаються з новими викликами в контексті інформаційної безпеки. Наприклад, вибори в США у 2016 році стали об'єктом інформаційних атак, спрямованих на дезінформацію та втручання у внутрішні справи держави через соціальні мережі. Російські хакери отримали доступ до електронних листів політичних кандидатів та використали цю інформацію для впливу на результати виборів.

На національному рівні важливою стратегією є розробка політик кібербезпеки та інвестування в розвиток технологій для захисту від інформаційних атак. Уряди країн повинні створювати системи моніторингу та реагування на кібератаки, а також забезпечувати навчання населення, щоб зменшити вразливість до дезінформації [2].

Таблиця

Результати використання методів маніпуляцій

Приклад	Результат
Кібератака на енергосистему України (205)	Відключення електроенергії в частині Західної України, порушення функціонування критичної інфраструктури [5]
Вибори в США (2016)	Втручання у вибори через соціальні мережі, дискредитація кандидатів і вплив на громадську думку [4]
Атака NotPetya (2017)	Порушення роботи державних установ і компаній по всьому світу, включаючи Україну, завдано збитків у мільярди доларів [6]

Висновки. Інформаційна безпека є ключовим елементом національної та міжнародної безпеки в умовах гібридних воєн. З огляду на зростання кібератак, дезінформації та маніпуляцій інформаційними потоками, держави повинні розробляти стратегії захисту своїх інформаційних ресурсів та підвищувати обізнаність населення про загрози інформаційної безпеки. Забезпечення інформаційної безпеки на глобальному рівні вимагає співпраці між державами та міжнародними організаціями.

Список використаних джерел

1. Міністерство цифрової трансформації України. (2023). Кіберзахист критичної інфраструктури: Виклики та рішення. URL: https://thedigital.gov.ua/news/kiberbezpeka-ukrainy.

2. Національний координаційний центр кібербезпеки. (2022). Кібератаки в Україні: аналіз загроз та стратегій захисту. URL: https://nccc.gov.ua/news/cyberattacks-analysis.

3. Голос Америки українською. (2022). Як кібератаки впливають на національну безпеку України. URL: https://ukrainian.voanews.com/a/cybersecurity-in-ukraine/

4. Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

5. BBC News. (2015). Ukraine cyber attack: Hackers caused power cut, US confirms. URL: https://www.bbc.com/news/technology-38573074.

6. U.S. Department of Justice. (2020). Report on the Investigation into Russian Interference in the 2016 Presidential Election. URL: https://www.justice.gov/storage/report.pdf.