ОСНОВНІ ПРИНЦИПИ КІБЕРВІЙНИ

Максим Кушнір
здобувач першого (бакалаврського) рівня вищої освіти,
спеціальність 061 Журналістика,
Національний авіаційний університет
Науковий керівник –
кандидат наук із соціальних комунікацій,
доцент кафедри журналістики
Національного авіаційного університету
Олена Мельникова-Курганова

Нами було сформовано основні принципи кібервійни та їх вплив на сучасне глобальне середовище, описуються технічні методи атак, такі як використання вразливостей, шкідливих програм та DDoS-атак, а також методи соціальної інженерії, дезінформації та маніпулювання громадською думкою. Визначили якими є наслідки кібератак для економіки, безпеки та суспільства. Також у роботі підкреслюється важливість міжнародної співпраці та спільних стратегій для захисту від кіберзагроз, та є цінним ресурсом для будь-кого, хто хоче краще зрозуміти кібервійну та її вплив на наш світ.

Кібервійна стала невід'ємною частиною сучасного геополітичного ландшафту, де інформаційні та комунікаційні технології (ІКТ) використовуються для завдання шкоди або виведення з ладу комп'ютерних систем, мереж та даних противника. Розуміння основних принципів кібервійни є критичним для журналістів, які висвітлюють цю складну тему.

Ключові принципи кібервійни:

Конфіденційність: Захист інформації від несанкціонованого доступу, розкриття або зміни. Це стосується як даних, так і методів ведення кібервійни. Журналісти повинні бути особливо обережні з чутливою інформацією, отриманою під час розслідування кіберзлочинів або кібератак [1].

Цілісність: Гарантування точності та автентичності інформації, щоб уникнути маніпуляцій та дезінформації з боку противника. Це означає, що журналісти повинні ретельно перевіряти інформацію з різних джерел, перш ніж публікувати її, та критично ставитися до тверджень, які здаються занадто хорошими, щоб бути правдою.

Доступність: Забезпечення безперебійного доступу до ІКТ для авторизованих користувачів, щоб мінімізувати вплив кібератак на критичні операції. Журналісти повинні усвідомлювати потенційні наслідки кібератак для роботи ЗМІ та вживати заходів для захисту своїх даних та систем.

Відмова в обслуговуванні: Запобігання противнику в використанні ІКТ, що може включати блокування доступу до вебсайтів або перешкоджання роботі мереж. Журналісти повинні бути обережні з посиланнями, на які вони клікають, та файлами, які вони завантажують, щоб уникнути зараження своїх комп'ютерів шкідливим програмним забезпеченням.

Брехня: Введення противника в оману з метою отримання переваги, наприклад, шляхом імітації легітимних веб-сайтів або розповсюдження фейкових новин. Журналісти повинні бути обізнані про методи соціальної інженерії та інші тактики обману, які використовуються в кібервійні.

Експлуатація: Використання вразливостей у системах та мережах противника для запуску кібератак. Журналісти повинні розуміти, як кіберзлочинці шукають та експлуатують вразливості, щоб краще захищати себе та свої джерела.

Україна, на жаль, з 2014 року зазнала низки масштабних кібератак, організованих з метою дестабілізації країни та підриву довіри до її уряду. Цей аналіз дослідить кібератаки, спрямовані проти України в 2014 та 2022 роках, деталізуючи їхні цілі, методи та наслідки.

Почнемо з 2014 року, а саме з кібератак на тлі Євромайдану та Кримської кризи:

Вторгнення в комп'ютерні системи урядових установ: Під час Євромайдану та Кримської кризи 2014 року українські урядові установи, включаючи Міністерство оборони та Центральну виборчу комісію, зазнали кібератак. Вважається, що ці атаки були здійснені проросійськими хакерами з метою дестабілізувати Україну та підірвати довіру до її уряду. Наслідками атак стали відключення веб-сайтів, витік даних та порушення роботи комп'ютерних систем [3].

Кібератаки на енергосистему: У грудні 2015 року Україна зазнала масштабної кібератаки на свою енергосистему. Внаслідок

атаки близько 250 000 людей залишилися без світла. Ця атака, ймовірно, також була здійснена проросійськими хакерами, ставши першим відомим випадком, коли кібератака призвела до широкомасштабного відключення електроенергії.

Перейдемо до 2022 року, де кібератаки стали інструментом військової агресії, наприклад масштабні кібератаки перед вторгненням. У січні та лютому 2022 року, напередодні повномасштабного вторгнення Росії в Україну, країна зазнала серії масштабних кібератак. Ці атаки були спрямовані на веб-сайти урядових установ, ЗМІ та фінансових систем. Їх метою було зламати комп'ютерні системи, викрасти дані та посіяти хаос перед вторгненням.

Кібератаки під час війни: З початку повномасштабного вторгнення Росія продовжує активно використовувати кібератаки як зброю проти України. Ці атаки спрямовані на критичну інфраструктуру, ЗМІ, а також на кібершпіонаж та дезінформаційні кампанії. Деякі з найвідоміших кібератак під час війни: атака на супутниковий інтернет Starlink у лютому 2022 року; атака вірусом-вимагачем Petya на українські підприємства у червні 2017 року; атаки на українські ЗМІ з метою поширення дезінформації та пропаганди.

Окрім кібератак, російські спецслужби постійно нарощують інтенсивність інформаційно-психологічних операцій. Це робиться, щоб дискредитувати зовнішню і внутрішню політику, зменшити міжнародну підтримку України, розколоти наше суспільство, поширювати панічні настрої. Згенеровані кремлівським режимом фейки масово тиражують підконтрольні йому медіа, політики, блогери [2].

Кібератаки завдали Україні значних економічних збитків, адже вони можуть спричинити порушення роботи підприємств, втрату даних та зниження довіри до інституцій. Кібератаки на енергосистеми, транспортні мережі та системи зв'язку можуть призвести до значних перебоїв у роботі цих систем, що негативно впливає на життя людей та економіку. Кібератаки, спрямовані на урядові установи та ЗМІ, можуть підірвати довіру до них з боку населення, що послаблює їхню легітимність та спроможність керувати ефективно. Кібератаки можуть використовуватися для координації військ, дезінформації противника та інших цілей, що без безпосереднього застосування сили. Це робить кібервійну потужним інструментом, який може використовуватися для досягнення стратегічних цілей без ризику прямого військового зіткнення

Вплив кібервійни на журналістику:

Кібервійна може використовуватися для цензури інформації та маніпулювання громадською думкою. Це може призвести до того, що журналістам буде важко отримувати доступ до надійної інформації та публікувати правдиві репортажі. Журналісти можуть стати мішенями кібератак з метою залякування або мовчання. Це може мати серйозний вплив на свободу слова та право журналістів на ведення репортажів. Кібервійна може ускладнити перевірку інформації та розрізнення правди від брехні. Це може призвести до поширення дезінформації та пропаганди, що може мати негативні наслідки для суспільства [4].

Роль журналістів у кібервійні:

Журналісти повинні бути обізнані про основні принципи кібервійни та її вплив на журналістику. Це допоможе їм краще розуміти контекст подій, які вони висвітлюють, та уникати потенційних ризиків. Журналісти повинні використовувати надійні джерела інформації та критично ставитися до прочитаного. Це допоможе їм забезпечити точність та неупередженість своїх репортажів [5].

Принципи кібервійни визначають нову реальність сучасних конфліктів та війн, де цифрові технології відіграють ключову роль. Розуміння цих принципів та їх впливу на суспільство та міжнародні відносини дозволяє країнам ефективно захищати свої інтереси та забезпечувати кібербезпеку.

Список використаних джерел

1. Гороховський О., Мельникова-Курганова О., Мирошниченко П., Островська Н. Фактчекінг і медіаграмотність: словник термінів. К.: ГО «Центр аналітики і розслідувань», 2020. 77 с.
2. Захист інформаційного та кіберпростору. https://ssu.gov.ua. URL: https://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky.
3. Інформаційна безпека людини як споживача телекомунікаційних послуг: Монографія. НДІ інформатики і права НАПрН України. К. : Право України; Х. : Право, 2013. 184 с.
4. Когут Ю. Кібербезпека та ризики цифрової трансформації компанії. Сідкон, 2021. 372 с.
5. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк. Безпека інформації.* Том 19, №1. 2013. С. 40-45.