УДК 004.056

Д. С. Тіщенко
Л.М. Куперштейн

ДЕЯКІ АСПЕКТИ ІНФОРМАЦІЙНИХ АТАК В УМОВАХ ВІЙСЬКОВОЇ АГРЕСІЇ

Вінницький національний технічний університет

Анотація

Розглянуто поняття інформаційної війни, інформаційної атаки та інформаційної зброї. Досліджено деякі методи інформаційної агресії в умовах військового вторгнення.

Ключові слова: *військова агресія, інформаційна атака, фейкова інформація, інформаційна війна, пропаганда.*

Abstract

The concepts of information warfare, information attack and information weapons are considered. Some methods of information aggression in the conditions of military invasion are investigated.

Keywords: *military aggression, information attack, fake information, information warfare, propaganda.*

Вступ

Сьогодні, в умовах військової агресії, інформаційна безпека як ніколи важлива. Відомо, що засоби масової інформації є четвертою гілкою влади і , таким чином, можуть суттєво впливати на думку та світосприйняття громадян і, як наслідок, на політичну та соціальну ситуацію в країні в цілому. Цьому підтвердження є російсько-українські відносини, що склалися за останнє десятиліття. Десятки мільйонів людей стали жертвами інформаційної зброї. Тому зараз дуже актуальними є навички відрізняти правдиву інформацію від фейкових новин та інформаційних атак.

Інструменти ведення війни на сьогодні дуже змінилися. Під час військової агресії окрім традиційної зброї на новий важливий рівень виходить і інформаційна. Інформаційна та кібернетична війна стали невід'ємними частинами воєнних операцій. Нажаль, ми стали свідками військового вторгнення російської федерації в Україну, підтримку цієї активності більшістю населення агресора, що стало наслідком багаторазового використання потужної інформаційної зброї.

Результати дослідження

Інформаційна війна має на меті формувати у суспільстві потрібну точку зору, громадську думку, погляди щодо окремих питань на користь

організатора інформаційної атаки. Метою є усвідомлення людьми окремих фактів чи подій у вигідному для маніпуляторів світлі. Щоденно ми можемо спостерігати у новинах, соціальних мережах, месенджерах, десятки повідомлень, серед яких трапляється не правдива інформація, інформація, яка не має офіційного підтвердження, але швидко розповсюджується, та сприймається за правдиву, діп-фейки та інші види інформаційних атак.

Проблема інформаційних атак є надзвичайно важливою. Людина, яка знаходиться під впливом інформаційної атаки та не вміє відрізняти правдиву інформацію від фейкової та здатна здійснювати дії, які можуть причинити шкоду не лише їй, а й оточуючим.

Термін «Інформаційна атака» використовується для опису цілеспрямованих дій з використанням технічних і програмних засобів з метою порушення інформаційної безпеки системи, що дають змогу впливати на її вміст. Інформаційна війна – це дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації, процесам, що базуються на інформації та інформаційних системах супротивника при одночасному захисті власної інформації, процесів, що базуються на інформації та інформаційних системах [1]. Основні методи інформаційної війни – блокування або спотворення інформаційних потоків та процесів прийняття рішень супротивника. Метою інформаційної атаки є порушення доступності, цілісності, конфіденційності інформації, послаблення моральних і матеріальних сили супротивника або конкурента та зміцнення власних, вона передбачає використання заходів пропагандистського впливу на свідомість людини в ідеологічній та емоційній сферах. Об’єктом можуть бути державні установи, телеканали, соціальні мережі, конкретні особи тощо [2].

З 2014 року Україна зазнає прямої агресії з боку російської федерації. Спочатку було анексовано Автономну Республіку Крим, згодом через пряме втручанню росії та підтримку сепаратистських рухів було анексовано ще дві територіальні одиниці України – Донецької та Луганської областей, а в 2022 році військової агресії зазнала майже вся територія України. Інформаційні атаки використовуються як елемент ведення війни, вони є наступальною інформаційною операцією. Можна виокремити такі основні методи інформаційної агресії проти України:

1) дезінформування та маніпулювання;
2) пропаганда;
3) диверсифікація громадської думки;
4) психологічний та психотропний тиск;
5) поширення чуток.

Дезінформування та маніпулювання інформацією – метод, який передбачає обман чи введення об'єкта спрямувань в оману щодо справжності намірів для спонукання його до запрограмованих суб'єктом дій.

Одним з прикладів явного дезінформування є створення діп-фейку з заявою про капітуляцію Президента України Володимира Зленського в

березні 2022 року. Відео намагались вірусно розповсюдити мережею та запевнити народ що Україна здалась, але така провокація не мала успіху.

Ще одним прикладом є хакерська атака у ніч проти 14 січня 2022 року, хакери масово атакували українські урядові сайти. Йдеться про сайт уряду, окремих міністерств і навіть сайт застосунку "Дія". У СБУ кажуть, що витоку персональних даних не було. Шкідливе програмне забезпечення слідчі компанії виявили у десятках постраждалих систем.

На сайті МЗС України та деяких інших можна було побачити таке повідомлення: "Українець! Всі ваші особисті дані були завантажені в загальну мережу. Всі дані на комп'ютері знищуються, відновити їх неможливо. Вся інформація про вас стала публічною, бійтеся і чекайте гіршого. Це вам за ваше минуле, сьогодення і майбутнє. За Волинь, за ОУН УПА, за Галичину, за Полісся і за історичні землі". Його опублікували українською, російською та польською мовами [3].

Для захисту простих користувачів, підприємств, державних установ необхідно навчати користувачів правилам інформаційної безпеки, а саме: як відрізнити правдиву інформацію від фейкової, як не стати жертвою шкідливого програмного забезпечення, як перевірити інформацію на достовірність, як забезпечити захист клієнтських або персональних даних та іншої конфіденційної інформації.

Висновок

Отже, в наш час, система виявлення інформаційних атак в умовах інформаційної війни є необхідною. Вирішення даної проблеми є актуальним та дуже важливим, адже інформаційні атаки це частина сучасної війни. Не дотримання правил інформаційної безпеки може призвести до втрати цінної інформації, загальної паніки та втрат серед населення.

Наразі інформаційна безпека є над важливою для кожного громадянина України, а особливо працівникам установ, які займаються обробкою конфеденійних даних. Керівники фірм, державних підприємств, установ критичної інфраструктури мають проводити роботу з персоналом, навчати співробітників безпечно користуватися додатками, сайтами та вміти відрізнити правдиві повідомлення від фекових.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Сливка В. Інформаційна війна проти України: міф чи реальність? [Електронний ресурс] / В. Сливка. – Режим доступу : http://intkonf.org/slivka-vv - informatsiyna-viyna-proti-ukrayini-mif-chi-realnist/

2. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції [Електронний ресурс] / В. Ліпкан, Ю. Максименко, В. Желіховський. – Режим доступу : http://mobile.pidruchniki.com/15800119/politologiya/ ponyattya_ zmist_zagroz_informatsiyniy_bezpetsi

3. Кібератака на Україну: Microsoft розповіла подробиці розслідування : веб-сайт. URL: https://www.bbc.com/ukrainian/news-59936067

Тіщенко Дарина Сергіївна – студентка групи 2БС-18б, факультет інформаційних технологій на комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: daria.tsc@gmail.com

Куперштейн Леонід Михайлович – к.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail: kupershtein@vntu.edu.ua

Tishchenko Daryna S. – student of group 2BS-18b, Faculty of Information Technology in Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: daria.tsc@gmail.com

Kupershtein Leonid M. – PhD, Associate Professor, Vinnytsia National Technical University, Vinnytsia, e-mail: kupershtein@vntu.edu.ua