Седляківська К.Г.
асистентка кафедри права та правоохоронної діяльності
Омелюх В.Л.
студентка групи НБ-6,
Державний університет «Житомирська політехніка», м. Житомир

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ПРОТИДІЯ ГІБРИДНИМ ЗАГРОЗАМ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

На сам перед інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [3]. Сфера інформаційної безпеки є дуже розширена і до неї входить багато різних чинників. Такими чинниками можуть бути: різноманітні структури, які забезпечують достовірність і актуальність інформації(ЗМІ), також входить така сфера – як кібербезпека або ж по іншому її називають кібернетична безпека. На теперішній час постають різні виклики перед інформаційною безпекою.

Під час повномасштабного вторгнення росії на територію України, та й навіть задовго до цього, ворожі спецслужби застосовували пропаганду, дезінформацію, перебільшення. Саме ці їхні заходи спричинювали серед громадян нашої держави великі сумніви, страх і зневіру до влади. Пропаганду часто використовують під час гібридних війн, і саме ми переконалися в цьому. Спецслужби роблять усе можливе щоб застерегти людей, їх попереджають, що не варто довіряти інформації яка надійшла з не перевірених джерел, або ж сумнівних. Варто довіряти інформації з надійних сайтів, груп у меседжері, в яких інформація перед тим як потрапити на простори інтернету детально перевіряється.

З вдосконаленням інформаційних технологій, штучного інтелекту, розвитку діпфейків – боротися з такими загрозами стало в рази важче. На рахунок діпфейків, можна зазначити, що з часом розпізнавати їх стало важче. Діпфейк — це

найвідоміша форма того, що називають «синтетичними носіями»: зображення, звук та відео, які, здається, були створені традиційними засобами, створюються за допомогою складного програмного забезпечення [4]. Їхнє використання може впливати на політику, а саме: вибори, політичні рішення, довіру суспільства до влади. Зловмисники часто використовують діпфейки, відносно нещодавно такі технології були використані до екс-міністра закордонних справ України Дмитра Кулеби під час розмови з головою Комітету із закордонних справ США, Бенджаміном Кардіном [5]. На даному етапі їх можна розпізнати, тому що технологія ще не є ідеальною. Явним показником діпфейку є несправжні (занадто ідеальні) риси обличчя, розмиті контури тіла, не чіткі деталі, малорухливість, або ж навпаки не природні рухи як для людини. Є безліч програмних забезпечень, які можуть розпізнати і відео- фото- діпфейки, а також аудіо.

Що ж таке «гібридна загроза»? Гібридні загрози передбачають, що противник може застосовувати як традиційні, так і неконвенційні засоби для досягнення своїх цілей [1]. Ми чітко розуміємо що гібридна загроза під час гібридної війни була цілком очікувана. Ворог атакує не лише стандартною зброєю, а й використовує різноманітні сфери впливу. До прикладу це може бути не стандартна тактика, кібертероризм, звичайний тероризм, пропаганда не лише на території нашої держави, а й за її межами, а також порушення прав людини, недотримання законів. Гібридні загрози різноманітні і постійно змінюються, а засоби варіюються від фейкових профілів у соціальних мережах чи ретельно розроблених кібератак, аж до відкритого застосування військової сили, включно з усім, що знаходиться між ними [2].

Звертаючи увагу на те, що гібридні загрози часто змінюються, вдосконалюються чи навіть утворюються нові, потрібно завчасно визначити в якому секторі може виникнути наступна небезпека і попередити її, а в кращому випадку – знищити її ще до того, як вона повністю утвориться. Протистояти таким видам небезпеки набагато важче, ніж класичним загрозам. Але усі ми розуміємо те, що світ вдосконалюється, а разом і з ним технології, які використовують у подвійному призначенні. Таким прикладом можуть бути дрони, яких до війни використовували під час фотосесій, чи зйомки вашого

свята. На даний час їх використовують для оборони нашої країни, або знищення прямого ворога. Крім того, до предметів подвійного призначення для наших громадян стали підвали та споруди, які знаходяться нижче рівня землі. Їх використовують для укриття під час повітряної загрози. Ці споруди, які на перший погляд були як кімнати для зберігання продуктів на зиму, чи для зберігання речей, які не актуальні на певні пори року – стали спасінням і прямим сховищем для людського життя. За короткий період часу українці зрозуміли наскільки важливо спускатися в підвал під час оголошення повітряної тривоги, саме ці дії спасали життя не однієї людини.

Підсумовуючи можна зазначити, що інформаційна безпека під час російсько-української війни відіграє важливу роль. Вчасне розпізнавання синтетичного контенту може врятувати не лише чиєсь життя, а й цілу державу. Гібридна війна, яку веде росія проти України, чітко показує, як за допомогою різних технологій можна досягти цілі. Щоб запобігти утворення нових загроз, чи то в інформаційній сфері чи в будь-якій іншій, потрібно вдосконалювати кібербезпеку усіх інфраструктур. Якщо атака вже відбулась, на неї потрібно швидко відреагувати і убезпечити людей від її поганих наслідків. Громадяни повинні об’єднатися і спільно з усіма зусиллями встати на захист нашої рідної землі у всіх сферах. Допомагати гуманітарною допомогою, донатами, а також підтримувати наших захисників усім чим ми можемо. Головне не забувати, те що якщо в нас декілька днів немає повітряної тривоги – це не означає, що на фронті усе добре, ми повинні пам’ятати, що війна досі триває!

Список використаних джерел

1. “Гібридні загрози: зрозуміти, адаптуватись, реагувати“. Radware Captcha Page. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-prezentation-2019/9.2019/pfpc-esc-hybrid-agenda-final.pdf (дата звернення: 01.12.2024).

2. Hagelstam A. НАТО Ревю - Співпраця заради протидії гібридним загрозам. NATO Review. URL:

https://www.nato.int/docu/review/uk/articles/2018/11/23/spvpratsya-zaradi-protid-gbridnim-zagrozam/index.html (дата звернення: 01.12.2024).

3. ІПС ЛІГА:ЗАКОН - система пошуку, аналізу та моніторингу нормативно-правової бази. LIGA:ZAKON. URL: https://ips.ligazakon.net/document/JG3TH00A?an=9 (дата звернення: 01.12.2024).

4. Діпфейки: як розпізнати та захиститися?. Інтернет Свобода. URL: https://netfreedom.org.ua/article/dipfejki-yak-rozpiznati-ta-zahistitisya (дата звернення: 03.12.2024).

5. Штучний інтелект і діпфейки: як країни реагують на загрози - Центр демократії та верховенства права. Центр демократії та верховенства права -. URL: https://cedem.org.ua/analytics/shtuchnyi-intelekt-i-dipfeiky/ (дата звернення: 03.12.2024).