Вишневська Марія Юріївна
курсант 201 навчальної групи ННІ № 3 НАВС, рядовий поліції

Науковий керівник:
Яровий Кирило Васильович
кандидат юридичних наук, старший викладач кафедри інформаційних технологій та кібербезпеки ННІ № 1 НАВС, капітан поліції

СУЧАСНИЙ СТАН КІБЕРЗАХИСТУ УКРАЇНИ В УМОВАХ ПОВНОМАСШТАБНОЇ ВІЙНИ

Україна, з самого початку повномасштабної війни з російською федерацією, зіткнулася не лише з постійним обстрілом ракетами, але і з різноманітними видами кібератак у цифровому інформаційному просторі. Кібератаки, на які звертається увага, різняться за формою та метою: від спроб дестабілізації суспільно-політичної обстановки до атак на критичну інфраструктуру та незаконного доступу до конфіденційної інформації громадян.

Агресія російська у кіберпросторі принесла значні виклики для української кібербезпеки. Зокрема, надійний захист від кібератак став пріоритетним завданням для уряду та правоохоронних органів України.

Незважаючи на те, що проблеми кіберзахисту в Україні були предметом наукових дискусій у роботах Алпеєва А.С., Архіпова О.Є., Бакалинського О.О. Богданова О.М., Грибуніна В.Г., Горбатько О.В., Мохора В.В., Чепуренко Я.О. в даний час питання кіберзахисту в кіберпросторі є найбільш розповсюдженим і актуальним для суспільства, оскільки це стосується всіх, хто має справу з інформаційними технологіями.

У цьому контексті, аналіз сучасного стану кіберзагроз та заходів захисту в Україні є надзвичайно важливим для розуміння проблеми та розробки ефективних стратегій протидії. Дослідження цих питань має на меті не лише виявлення потенційних ризиків та вразливостей, але й розробку практичних рекомендацій та інноваційних підходів до підвищення кібербезпеки в Україні.

На рівні адміністративно-правового регулювання процесів кібербезпеки відсутні систематичні заходи державного регулювання у сфері захисту кіберпростору і їх перелік не є чітко визначеним [1].

Крім цього, сьогодні, коли наша держава знаходиться в умовах воєнного стану важливим є не лише для ІТ-фахівців, але й для будь-якого громадянина навчання застосування цифрової грамотності, дотримання цифрового етикету та правил кібергігієни.

З початком війни ІТ-фахівці з усієї країни долучилися до кіберполіції та зуміли дати відсіч агресору. В результаті злагоджених дій були виведені з ладу критично важливі інформаційні системи окупанта.

Найбільшу активність від атак російських хакерів відчувають на собі державні та місцеві органи влади, інформаційні ресурси сектору безпеки та оборони, енергетичний, фінансовий і комерційний сектори, а також ІТ-інфраструктура та транспортна галузь. Наразі хакери все більш активно атакують енергетичний сектор, щоб позбавити українців умов для нормального життя навіть поза окупованими територіями, де вони фізично знищують інфраструктуру населених пунктів.

Щодо мети кібератак, то в 306 випадках здійснювався несанкціонований збір інформації, у 267 – були спроби розмістити шкідливий програмний код, у 149 – спроби втручання у функціонування роботи ресурсів, інші різновиди атак – 401 [2].

Слід зазначити, що війна відбувається не лише на фізичному фронті, а й у інформаційному полі. Загарбники здійснюють кібератаки не лише на урядові структури – жертвами зламів і викрадення даних стають і пересічні громадяни. Вони намагаються отримати доступ до персональних даних та державних реєстрів через приватні комп'ютери та мобільні телефони. Українці масово отримують листи із шкідливою програмою, яка викрадає паролі й файли.

Проте українцям необхідно дотримуватися вимог кібергігієни, оскільки інформаційний простір це джерело поширення фейків, діпфейків, підробки сайтів, фішингових атак, заволодіння акаунтами громадян [3, с. 46].

Розглянемо детальніше основні правила кіберзахисту в Україні, які виникають в умовах воєнного стану. Передусім, важливо дотримуватись основного принципу кібергігієни щодо фейків: слід читати лише із офіційних та перевірених джерел. Однак у воєнний час слід мати на увазі, що навіть надійні медіа та офіційні особи можуть допускати помилки. У таких обставинах українці постійно оновлюють стрічку новин, щоб дізнатися про ситуацію на фронті та в дипломатичному полі. Тим часом ворог активно розповсюджує фейки про виглядання міст, капітуляцію України чи евакуацію місцевих мешканців.

Крім цього, якщо мова йде про сторінки в соціальних мережах, важливо звернути увагу на те, чи має аккаунт верифікацію (синя галочка поруч із назвою). Ще однією ознакою є невелика кількість підписників та дописів. Щодо веб-сайтів, варто звернути увагу на наявність символу замочка в адресному рядку браузера, що свідчить про успішну перевірку та отримання сертифіката безпеки. Додатково можна скористатися сервісом Whois для перевірки дати реєстрації/створення сайту, власності компанії та інших юридичних даних. Ще один вдосконалений метод фішингу – підробка посилань на підпис електронних петицій.

DeepFakes (контамінація Deep Learning та Fake, англ. – фальшивка) є продуктом двох алгоритмів ШІ, які взаємодіють у так званій Generative Adversarial Network (укр. генеративній змагальній мережі) [3, с. 17].

Іншими словами, діпфейк – це підроблене відео, на якому можна побачити публічну особу з виступом, а також чути її голос. Наприклад, у Центрі інформаційної безпеки повідомляли, що в мережі може з'явитися відеозвернення Президента Володимира Зеленського, в якому він, мабуть, оголосить про капітуляцію. Проте це використання технології машинного навчання, яка може бути застосована для збентеження та підірвання бойового духу.

Україна має бути здатною забезпечити свій соціально-економічний розвиток у цифровому світі, що вимагає набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі, досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі.

Отже, встановлено, що нова ера кібербезпеки вимагає цілком нових підходів до управління ресурсами, зокрема інформаційними. Успіх таких змін значною мірою залежить від того, як гнучко організовані процеси на рівні держави, а також як імплементуються нові моделі та методи роботи у боротьбі з можливими загрозами.

Наша точка зору полягає в тому, що для вирішення проблем інформаційного забезпечення в Україні важливо дотримуватись основних правил кібергігієни у боротьбі з фейками, діпфейками, підробкою сайтів, фішинговими атаками, заволодінням акаунтами громадян: надавати перевагу лише офіційним та перевіреним джерелам інформації, уникаючи підозрілих постів у соціальних мережах. Одночасно слід мати на увазі, що навіть довірені медіа та офіційні особи можуть допускати помилки, особливо у період воєнного стану.

Список використаних джерел:

1. Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серп. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Як забезпечити захист кіберпростору України на тлі збройної агресії рф. Інформаційний Інтернет-ресурс URL: https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf.

3. Кудінов В. А., Яровий К. В. Комплексний підхід щодо створення стійких паролів інформаційних систем спеціального призначення МВС та Національної поліції України (частина 1). Сучасна спеціальна техніка. 2023. № 3 (74). С. 42-49.

4. Вальорска М. Аґнєшка. Діпфейк та дезінформація: практ. посіб. / Аґнєшка М. Вальорска ; пер. з нім. В. Олійника. Київ : Академія української преси; Центр Вільної Преси, 2020. 36 с.