Головко Олександр Віталійович
курсант 208 навчальної групи ННІ № 1 НАВС, рядовий поліції

Ботнаренко Ірина Анатоліївна
кандидат юридичних наук, старший науковий співробітник наукової лабораторії з проблем протидії злочинності ННІ № 1 НАВС

АСПЕКТИ ТА ПИТАННЯ КІБЕРБЕЗПЕКИ ДЛЯ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

У сучасному світі інформаційних технологій та становлення інформаційного суспільства виникають нові виклики та загрози у сфері кібербезпеки. Обсяг персональних даних, які збираються підприємствами, організаціями, державними установами та урядами, швидко зростає. Ці особисті дані використовуються для створення профілів людей, прогнозування та контролю їхньої поведінки.

З одного боку, це може забезпечити персоналізований досвід та ефективніше використання ресурсів, проте з іншого боку, це створює ризики дезінформації та зловживання зібраними даними.

Проблема конфіденційності даних. Основною проблемою конфіденційності, з якою стикаються розробники та користувачі інформаційних систем, є захист конфіденційності персональних даних. Багато організацій досі зберігають приватну інформацію та навіть паролі в незашифрованому вигляді. Незважаючи на прогрес у протоколах безпеки, кількість порушень конфіденційності продовжує зростати. Згідно зі звітом Risk Based Security, загальна кількість скомпрометованих записів у 2022 році перевищила 37 млрд [1].

Порушення даних відбувається через несанкціонований доступ до баз даних організацій, що дозволяє хакерам викрасти конфіденційну персональну інформацію, включно з паролями, номерами кредитних карток, номерами соціального страхування та банківськими даними. Ці добре задокументовані інциденти мали негативні наслідки, такі як шахрайство з кредитними картками та крадіжка особистих даних [2].

Ситуація в Україні. В Україні в умовах війни з росією інтенсивність кібератак з боку російських хакерів не зменшується. Найбільше атакам піддаються уряд, місцеві органи влади, оборонний, фінансовий та енергетичний сектори, транспортна інфраструктура та телекомунікаційна галузь. Спостерігається неухильне зростання кіберзлочинності, метою якої є крадіжка або знищення інформації, дестабілізація ситуації в країні, виведення з ладу державних установ та обладнання.

Для протидії зростанню кіберзлочинності був прийнятий Закон «Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам» № 2137-IX [3], який спрощує процедуру розслідування кіберзлочинів, та Закон «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» № 2149-IX [4], які вносять зміни до Кримінального кодексу з метою посилення відповідальності за кіберзлочини. Проте для підвищення рівня кібербезпеки необхідно забезпечити належний захист державних установ та об’єктів критичної інфраструктури, а також підвищувати обізнаність громадян про кіберзагрози [5].

Наразі у нас в країні надзвичайно слабке становище в питанні, що стосується інформаційної війни з росією. Країна-агресорка є державою, яка веде інформаційну війну одна з найкращих у світі. Про це свідчить масова пропаганда, яка створюється не лише для росіян, що спрямована на їх «зомбування», а також і безпосередньо на громадян України. Вся ця робота росії спрямована на погіршення морального духу українців, адже велика кількість ІПСО демотивує українців на боротьбу з росією і це на користь країні-агресору.

В якості прикладу можна зазначити інтернет-ботів, які представляють із себе звичайних людей, проте насправді це просто фейк. Одна з їхніх робіт полягає в сіяні розладу між українцями. Так вони намагаються зробити внутрішні міжусобиці, які негативно впливають на український дух серед громадян. Це лише один приклад дії інформаційної війни росії. До того ж дезінформація зі сторони росії спрямована не тільки на прямі сторони конфлікту, а ще й союзників нашої держави. Надзвичайно велика пропаганда спрямована на європейців та на американців, які є прямими нашими союзниками та від їхньої допомоги залежить наше становище в цій довготривалій війні. У 2024 році вийшло інтерв’ю Такера Карлсона з володимиром путіним. Воно було спрямоване на виправдання російської агресії проти України та мало на меті перетягнути якнайбільше іноземців на бік підтримки росії. Є достатня кількість іноземців, які стали жертвами цієї дезінформації, тому Україні треба якнайкраще боротися в інформаційній війні та впроваджувати свої нові методи боротьби з ними або запозичувати їх у країн Європи, які можуть допомогти з цим.

Законодавче регулювання. У відповідь на зростання кіберзлочинності та занепокоєння користувачів з приводу конфіденційності їхніх даних пропонується та впроваджується законодавство щодо захисту персональних даних. Проте наразі існують недоліки у законодавчому регулюванні кібербезпеки в Україні. Зокрема, відсутній уніфікований понятійно-термінологічний апарат, є невідповідність визначень чинним актам та міжнародним документам, окремі норми застаріли, повільно впроваджується європейське законодавство. Нормативно-правові акти розрізнені, бракує кодифікованого акту.

Пропонується формування Інформаційного кодексу України як зводу інформаційно-правових норм, зокрема з питань кібербезпеки. Необхідно узгодити понятійно-термінологічний апарат відповідно до національних та міжнародних актів, посилити відповідальність за кіберправопорушення та імплементувати положення європейського законодавства.

Євроінтеграція у сфері кібербезпеки. Для ефективної євроінтеграції України потрібна реалізація державної політики у сфері кібербезпеки відповідно до європейських норм і стандартів. Органи виконавчої влади мають стати провідними суб'єктами впровадження євроінтеграційного курсу в цій сфері. Необхідна співпраця з ЄС та НАТО, залучення кращих світових практик і експертизи. Слід підвищувати кіберстійкість України відповідно до стандартів ЄС, реформувати органи кібербезпеки згідно з євроінтеграційними вимогами.

Кібербезпека займає особливе місце в сучасних наукових дослідженнях і активно розвивається з кожним роком. Сама концепція кібербезпеки вимагає переосмислення через швидкі зміни у сфері інформації та зростаючу "інформаційну" складову розвитку світової спільноти [6].

Підсумовуючи, можна зазначити, що забезпечення кібербезпеки є одним з найважливіших завдань у сучасному інформаційному світі.

Необхідно вдосконалювати законодавчу базу, впроваджувати передові практики та технології захисту інформації, а також підвищувати обізнаність громадян про кіберзагрози. Лише комплексний підхід, що поєднує правове регулювання, технічні рішення та освіту громадськості, дозволить ефективно протидіяти зростаючим кіберзагрозам та захистити конфіденційність персональних даних. Для України, що прагне євроінтеграції, питання кібербезпеки набуває особливого значення в умовах війни з росією та необхідності посилення обороноздатності держави.

Список використаних джерел:

1. RiskBased Security. 2022 Year End Report: Data Breach Quickview. URL: https://flashpoint.io/resources/report/state-of-data-breach-intelligence-2022-midyear.

2. Балацька Валерія Сергіївна, Опірський Іван Романович. Забезпечення конфіденційності персональних даних і підтримки кібербезпеки за допомогою блокчейну. URL: https://journals.indexcopernicus.com/search/article?articleId=3786215.

3. Про внесення змін до Кримінального процесуального кодексу України та Закону України "Про електронні комунікації" щодо підвищення ефективності досудового розслідування "за гарячими слідами" та протидії кібератакам : Закон України від 15.03.2022. URL: https://zakon.rada.gov.ua/laws/show/2137-20#Text

4. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.2022. URL: https://zakon.rada.gov.ua/laws/show/2149-20#Text.

5. Смілянець Єгор Ігорович, Білаш Олексій Олександрович, Плахотний Артем Павлович. Щодо кібербезпеки в умовах воєнного стану. URL: https://archive.mcnd.org.ua/index.php/conference-proceeding/article/view/936.

6. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. URL: http://www.sulj.oduvs.od.ua/archive/2022/4/part_1/35.pdf.

Гордієнко Данило Сергійович
курсант 2 курсу факультету № 4 Харківського національного університету внутрішніх справ, рядовий поліції

Науковий керівник:
Світличний Віталій Анатолійович *кандидат технічних наук, доцент, доцент кафедри протидії кіберзлочинності факультету № 4 Харківського національного університету внутрішніх справ*

ОСНОВНІ ТЕХНІКИ ЗБОРУ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ OSINT-ІНСТРУМЕНТІВ В УМОВАХ ВОЄННОГО СТАНУ

Вступ. Використання розвідувальних даних з відкритих джерел (OSINT) може стати ключовим інструментом у різних сферах у майбутньому.

Виклад основного матеріалу. У сфері безпеки і боротьби з тероризмом OSINT може допомагати відстежувати діяльність терористичних груп та розкривати їхні плани, аналізуючи загальнодоступну інформацію. У кризовому управлінні ці дані також можуть бути використані для оперативної реакції на загрози та кризи. В політичному аналізі OSINT може надати важливу підтримку, збираючи та аналізуючи дані з різних відкритих джерел і розуміючи громадську думку та настрої. У сфері економічного аналізу OSINT може відстежувати ринкові тенденції та допомагати у розумінні потоків капіталу та прийнятті обґрунтованих економічних рішень. Автоматизований аналіз великих обсягів медіа-контенту за допомогою OSINT може покращити аналітичні можливості в аналізі ЗМІ. У наукових дослідженнях OSINT може стати ключовим інструментом для збору та аналізу даних, що дозволить отримувати більш точні результати. У сфері кібербезпеки OSINT може допомагати виявляти потенційні загрози та вразливості в мережах.