Етика та професіоналізм. Компетентність управління освітнім закладом вимагає дотримання етичних стандартів, високого професіоналізму та відповідальності перед стейкхолдерами.

Використання соціальних мереж. Спільноти та форуми в мережі можуть стати важливим інструментом для обміну досвідом, підтримки співробітників, а також побудови партнерських відносин з іншими освітніми закладами.

Інформаційні портали та ресурси. Використання спеціалізованих освітніх порталів і ресурсів дозволяє майбутнім керівникам отримувати доступ до актуальної інформації про інноваційні підходи у керівництві освітнім закладом.

Управлінська компетентність є важливою складовою професійної підготовки майбутніх керівників освітніх закладів, оскільки вона дозволяє забезпечити ефективне управління, інноваційний розвиток та досягнення стратегічних цілей в освітній галузі. Розвиток цих компетентностей є важливим завданням у навчальних програмах для підготовки майбутніх керівників освітніх закладів до викликів і можливостей, які стоять перед сучасною освітою [2].

Використання засобів ІКТ сприяє формуванню управлінської компетентності майбутніх керівників освітніх закладів, допомагаючи їм розвивати навички управління, лідерства та стратегічного планування у сучасному освітньому середовищі. Ретельне ознайомлення з цими засобами в процесі підготовки дозволить керівникам ефективно впроваджувати інновації та забезпечувати високу якість освіти у своєму закладі.

Список використаних джерел

1. Світлорусова А. В. Роль ІКТ у професійній підготовці майбутніх керівників навчальних закладів. URL: http://www. nbuv. gov. Ua/ejournals/ITZN/content/ogsavieo. Htm (дата доступу 12..03.2024)

2. Щоголєва Л., Вознюк, В. Стратегічне управління освітнім закладом як соціальною системою. *Нова педагогічна думка*, 2014, 2: 237-240.

КІБЕРЗЛОЧИННІСТЬ У DARK WEB

Іваницький Роман Іванович
кандидат технічних наук, асистент кафедри інформатики та методики її навчання,
Тернопільського національного педагогічного університету імені Володимира Гнатюка,
romik_iv@ukr.net

Ковальчук Ольга Ярославівна
кандидат фізико-математичних наук, доцент кафедри теорії права та конституціоналізму,
Західноукраїнського національного університету,
olhakov@gmail.com,

Інформаційно-комунікаційні технології стали основою розвитку людства та є важливим ресурсом у всіх сферах. Однак, окрім користі, вони становлять загрозу для окремих осіб, бізнесу та держав світу загалом. Темпи інновацій у таких сферах, як штучний інтелект (AI), інтернет речей (IoT) та біотехнології створюють нові загрози, які будуть посилюватися у світі, де зростає геополітична напруга, нерівність та соціальна нестабільність. Протягом останнього десятиліття кібератаки зростали за частотою та вартістю. У рейтингу найбільших глобальних ризиків у 10-річній перспективі масштабне шахрайство та крадіжка даних (Data fraud or theft) займають четверте місце, кібератаками – п’яте [1]. Кіберзлочинність і надалі залишатиметься проблемою безпеки 21 століття.

Сучасне високотехнологічне суспільство поступово переходить у віртуальний світ. Більшість важливих розмов, подій та процесів відбуваються у цифровій формі. Пандемія 2020 лише прискорила цей тренд. Сьогодні соціальними мережами користуються 3 млрд. людей. Це майже половина населення планети [2]. Вони щоденно публікують замітки, обмінюються фото, реагують на дописи друзів, а ще слідкують за життям чужих людей. Дуже важко зберегти анонімність у такому світі. Це складає суттєву загрозу особистій безпеці кожного з користувачів Internet.

The Dark Web – це зашифрована мережа веб-сайтів, доступ до яких можливий лише за допомогою спеціального захищеного браузера (Tor – система проксі-серверів, яка дає можливість встановлювати анонімне мережеве з'єднання, захищене від прослуховування). Вона не регулюється жодним урядом і не може бути піддане цензурі. У Dark Web існує безліч різних веб-сайтів, таких як блоги, що ведуться особами, які не дотримуються конфіденційності, сторінки для преси, форуми для борців за свободу та протестуючих і ринки продажів, що продають (легальну та нелегальну) продукцію. The Dark Web не є незаконною, але її використання може бути дуже небезпечним для незахищених користувачів.

Кіберзлочинна підпільна економіка змінюється щохвилини. Постійно розвивається інструменти та методи кіберзлочинців, які можуть за частку секунди поставити когось під загрозу. Злочини on Dark Web мають широкий спектр – від легальних товарів та простої електронної крадіжки, маніпуляції свідомістю спільноти соцмереж з метою прихованого впливу на покупців чи електорат до продажу контрабанди, як наркотики та вогнепальна зброя, та шокуючих реальних злочинів, як дитяча порнографія, спонукання до суїциду та замовних вбивств. І все це відбувається у Dark Web. Сьогодні як ніколи нам потрібний безпечний цифровий світ.

Dark Web не лише для злочинців. Середня щодобова кількість клієнтів Tor у грудні 2023 складала більше 2,5 млн., і більше 50 % domains on the dark web є легальними [1]. Для осіб, які живуть під гнітючими режимами, що блокують значну частину інтернету або карають за політичну незгоду, dark web – це остання можливість отримати доступ до інформації та захист від переслідування. У більш вільних суспільствах це може бути критично важливим інструментом інформування та комунікації, який захищає людей від відплати чи осуду на робочому місці чи в громаді. Крім того, він може просто забезпечити конфіденційність та анонімність для тих, хто насторожено ставиться до того, як корпорації та уряди відстежують, використовують та потенційно монетизують свої дані. Оскільки Dark Web не підпадає під цензуру та є анонімною, вона приваблює людей, які хочуть купувати та продавати нелегальні товари, але мають законні причини використовувати її [3].

Значна частина користувачів Dark Web – це прості люди, що хочуть залишитись анонімними, обійти цензуру та захистити свою приватність. Це безпечний спосіб для викривачів, активістів та журналістів ділитися інформацією, не ризикуючи піддатись політичному переслідування чи відплаті з боку їх уряду. Поліція та спецслужби використовують його для спостереження за терористичними групами та відстеження кіберзлочинців. Фахівці з кібербезпеки використовують Dark Web для пошуку викрадених даних та ознак викрадення

особистих даних, щоб мати змогу попередити та захистити їх власників. Він розміщує сайти, що належать медіа-організаціям, які займаються журналістськими розслідуваннями. Навіть WikiLeaks – веб-сайт, що публікує секретні офіційні матеріали – також має свій веб-сайт у Dark Web. Навіть Facebook підтримує свою присутність там, щоб стати доступним у країнах, де цю соцмережу цензурує уряд.

Dark Web використовують для обміну інформацією та ресурсами в країнах з інтернет-цензурою. Dark Web – це безпечне місце для обміну інформацією без відстеження та переслідування урядом. У Dark Web можна купувати заборонені товари. Хоча правоохоронні органи та уряди не потурають купівлі незаконних товарів, вони все ж визнають окремі певні випадки, коли такі покупки можуть бути виправданими. Наприклад, деякі знеболюючі засоби та засоби для сну, поширені в Європі, є незаконними в багатьох країнах Близького Сходу та Азії. Крім того, багато людей не мають доступу до необхідних їм ліків, що відпускаються за рецептом, серед них 15,5 % американців, які не мають медичного страхування [4]. Тим не менш, відсутність нагляду за Dark Web робить її надзвичайно ризикованою.

Покупки в магазинах Dark Web можуть бути більш безпечними, ніж інші через інтернет-магазини (наприклад, Amazon), оскільки можна розрахуватись криптовалютами. Це означає, що користувач робить покупки, не вказуючи інформацію про свій банк або кредитну картку, а звичайні магазини зберігають платіжні реквізити клієнтів. Dark Web дає можливість легко купувати легальні товари анонімно. Однак, ніколи не можна давати веб-сайтам Dark Web свою домашню адресу, це найкращий спосіб захистити себе.

Використання Dark Web через Tor – анонімний та більш безпечний спосіб користування інтернетом. Активність та місцезнаходження користувача неможливо простежити, і він отримує доступ до тієї частини інтернету, яку уряди та провайдери не можуть цензурувати чи забороняти. Однак щоб залишатися абсолютно анонімними в Dark Web, потрібно використовувати анонімний зашифрований обліковий запис електронної пошти, псевдоніми та паролі, які ніколи раніше не використовувались і які неможливо простежити, анонімний біткойн-гаманець для здійснення покупок.

Сьогодні існує великий ризик підриву цифрової економіки та традиційних інституцій, на які покладається забезпечення безпеки і довіри в суспільстві. Вирішення проблем кіберзлочинності вимагатиме більш глибокої транснаціональної інтеграції та діалогу між урядами як з точки зору політики, так і з точки зору можливостей.

Dark Web є частиною анонімного інтернету, яка використовується як для незаконної діяльності (торгівля забороненими товарами, крадіжка даних, шахрайство), так і для законних цілей (обхід цензури, захист свободи слова). Боротьба з кіберзлочинністю в Dark Web потребує міжнародної співпраці та розвитку технологій кібербезпеки. Проте слід зберегти можливість використання Dark Web для захисту прав людини в репресивних режимах.

Список використаних джерел

1. World Economic Forum, The Global Risks Report, 2023. URL: https://www.weforum.org.

2. Razis G., Georgilas S., Haralabopoulos G., Anagnostopoulos I. User Analytics in Online Social Networks: Evolving from Social Instances to Social Individuals. *Computers*, 2022. № 11, P. 149.

3. Kovalchuk O., Masonkova M., Banakh S. The Dark Web Worldwide 2020: Anonymous vs Safety. *2021 11th International Conference on Advanced Computer Information Technologies (ACIT)*, Deggendorf, Germany, 2021. P. 526–530.

4. Dark web statistics & trends for 2024. URL: https://preyproject.com.

ОСОБЛИВОСТІ ОСНОВНИХ ПІДХОДІВ АНАЛІЗУ ТОНАЛЬНОСТІ ТЕКСТУ: ТЕОРЕТИЧНИЙ АСПЕКТ

Крошняк Петро Ярославович
магістрант спеціальності 014.09 Середня освіта (Інформатика, математика, STEM-освіта)**,**
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
kroshnyak_py@fizmat.tnpu.edu
Карабін Оксана Йосифівна
кандидат педагогічних наук, доцент кафедри інформатики та методики її навчання,
Тернопільський національний педагогічний університет імені Володимира Гнатюка,
karabin@tnpu.edu.ua

Сьогодні велика увага приділяється обробці природної мови, оскільки дана галузь науки відкриває широкі можливості для аналізу та інтерпретації великих обсягів текстових даних, що щодня генеруються людством. Розвиток технологій у цій сфері сприяє поліпшенню комунікації між людьми та машинами, забезпечуючи більш ефективне взаємодію через комп'ютеризовані системи, такі як чат-боти, системи автоматичного перекладу, голосові асистенти, та інші аплікації, що спрощують наше повсякденне життя й роботу.

Одним з популярних методів обробки природної мови в наукових дослідженнях є аналіз тональності текстів (sentiment analysis), що проявляється в автоматичному виявленні емоційно забарвленої лексики та думок авторів щодо об'єктів, що обговорюються у тексті. Варто зазначити, що у сьогоднішніх реаліях цифрового прогресу аналіз тональність тексту є ключовим компонентом багатьох сучасних технологій обробки природної мови (Natural Language Processing). Аналіз тональність тексту забезпечує можливість автоматично визначати емоційний настрій тексту, що є важливим завданням у багатьох областях, включаючи аналіз відгуків користувачів, виявити публічний настрій щодо подій, опцій, інвентів тощо. Відтак застосування концепції аналізу тональності текстів у свою чергу, упроваджується:

– по-перше, в аналізі природньої мови (лексична тональність тексту, яка визначається сумою лексичних тональностей кожного слова у тексті);

– по-друге, в машинних перекладах;

– по-третє, в аналізі й розумінні думок автора або самого автора (спроба наблизити мислення комп'ютера до людського).

Нині існує декілька основних підходів аналізу тональності тексту, а саме:

– *лексичний аналіз.* Використання словникових і лексичних ресурсів для визначення емоційного забарвлення слова чи фрази. Даний підхід кожному слову призначається певне значення тональності (позитивне, негативне або нейтральне), що ґрунтується на його вживанні та семантиці. Наприклад, слово «радісний» має позитивне забарвлення, «смуток» – негативне. Однак, лексичний аналіз має свої