ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

СОЦІОЛОГІЧНИЙ ФАКУЛЬТЕТ

Кафедра прикладної соціології та соціальних комунікацій

Пояснювальна записка
до кваліфікаційної роботи
на тему

«Проблема конфіденційності особистої інформації у світлі розвитку новітніх каналів комунікації»

Виконала: студентка 4 курсу групи СМК-42
першого (бакалаврського) рівня вищої освіти
спеціальності 061 Журналістика
Єрмоленко К.І.
Керівник: канд.соц.н., доцентка Зінюк А.В.

Харків – 2024

ЗМІСТ

Вступ

Сучасний світ характеризується стрімким розвитком інформаційних технологій та новітніх каналів комунікації, які значно спростили процес обміну інформацією та зруйнували географічні бар'єри між людьми. Соціальні мережі, такі як Facebook, Instagram, Twitter та інші, стали невід'ємною частиною повсякденного життя мільйонів користувачів по всьому світу. Вони дозволяють людям спілкуватися, ділитися фотографіями, відео, думками та подіями свого життя, створюючи ілюзію безпеки та приватності. Однак, з розвитком цих технологій зростає й ризик витоку конфіденційної інформації, що може призвести до серйозних наслідків як для окремих осіб, так і для суспільства в цілому.

Проблема конфіденційності особистої інформації у світлі розвитку новітніх каналів комунікації набуває все більшої актуальності. Користувачі часто не усвідомлюють, що їх дані можуть бути використані зловмисниками для шахрайства, викрадення особистості, а також інших форм кібератак. Нерозуміння сутності конфіденційних даних та необережне поводження з ними під час використання соціальних мереж призводить до численних витоків інформації, що створює серйозні загрози для приватного життя та безпеки користувачів.

У наш час значна кількість досліджень присвячена питанням інформаційної безпеки та захисту особистих даних. У своїй роботі Макух Н., Чоп Т. описують описують теоретичні засади проблеми конфіденційності, її визначення, а також зачіпають юридичний аспект питання. Також дана тема вивчалася Глянько О. та Недашківським Г. Їхні роботи розкривають проблему з юридичного аспекту, розкривають ставлення держави до захисту персональних даних, а також піднімалося питання неможливості зберігати свої дані повністю конфіденційними при умові постійного користування соціальними мережами. Проте, проблема

конфіденційності у соціальних мережах потребує більш детального вивчення, оскільки ці платформи постійно еволюціонують і змінюють свої політики конфіденційності та умови користування. Це дослідження спрямоване на те, щоб заповнити цю прогалину, надаючи нові дані та аналітику, що допоможуть краще зрозуміти поточну ситуацію та розробити ефективні стратегії захисту конфіденційної інформації.

Мета кваліфікаційної роботи - аналіз проблем конфіденційності особистої інформації у світлі розвитку новітніх каналів комунікації.

Для виконання цієї роботи ми поставили перед собою наступні завданні:

1. Дослідити теоретичний базис питання конфіденційності в соціальних мережах;
2. Проаналізувати суміжну за темою літературу, роботи інших науковців;
3. Провести дослідження та проаналізувати отримані результати, щоб підтвердити або спростувати гіпотезу;

Об'єктом дослідження виступає витік конфіденційних даних, що відбувається через нерозуміння та необережність користувачів під час використання соціальних мереж.

Предметом дослідження є проблема конфіденційності особистої інформації у новітніх медіа, а саме поведінка і ставлення користувачів до власних конфіденційних даних та способів їх захисту.

Для досягнення поставлених цілей було проведено анкетування та онлайн-опитування, які дозволили зібрати дані про ставлення користувачів до їх конфіденційних даних та соціальних мереж. Цей метод збору даних був обраний через його зручність, доступність та можливість охоплення широкої аудиторії. Анкети містили питання, спрямовані на виявлення рівня обізнаності користувачів про загрози, пов'язані з витоком конфіденційної інформації, а також їхніх звичок та практик у сфері інформаційної безпеки.

Дане дослідження націлене на те, щоб не лише виявити існуючі проблеми, але й запропонувати можливі рішення для їх подолання. Результати цього дослідження можуть бути корисними як для користувачів соціальних мереж, так і для розробників платформ та законодавців, які займаються питаннями захисту особистих даних.

Робота пройшла апробацію та була заслухана на XXII Міжнародній науковій конференції студентів, аспірантів, докторантів і молодих вчених “Соціологія у (пост)сучасності” 15 березня 2024 року.

Робота складається з двох розділів, висновків, списку використаних джерел та додатків.

Розділ 1 Теоретичні засади проблеми конфіденційності особистої інформації

1.1 Особливості соціальних мереж як різновид новітніх медіа

Інтернет продовжує традицію розвитку глобальних електронних ЗМІ, і можливості мережі є позитивними в порівнянні з телебаченням.Інтернет не вимагає громіздких і дорогих систем передачі сигналів. Інтернет, як і телебачення, активно використовується адміністративними органами – частка політичного та адміністративного контенту має тенденцію неухильно зростати. У той же час існує різниця в обробці онлайн-контенту з інших носіїв. Щоб отримати інформацію з Інтернету, споживачі повинні спочатку проявити очевидну активність, а іноді потрібні серйозні інтелектуальні зусилля. По-друге, ця діяльність заснована на реалізації права споживачів на вибір. І це право є індивідуальним, на відміну від телевізійних знань, які прагнуть до максимальної маси та стандартизації для досягнення ефективності. Спілкування в Інтернеті характеризується ефективністю, а повідомлення з інформаційних сайтів можуть миттєво відтворюватися онлайн-трансляціями. Як згадувалося раніше, традиційні засоби масової інформації перейшли до Інтернету, і сьогодні в інтернеті представлені всі основні новинні організації, радіо - та телевізійні станції, газети та журнали. Є також авторитетні онлайн-публікації.

Структура Інтернету різноманітна-від окремої людини до колективу, від колективу до людини. Традиційна схема поширення інформації не працює в мережі, від активного суб'єкта інформатора до пасивного об'єкта аудиторії. Інтернет-аудиторія складається з активної спільноти, яка одночасно є відправником та одержувачем інформації. Ці знання невеликі, вони диференційовані і спеціалізовані. Було проведено багато досліджень щодо впливу Інтернету та соціальних мереж на цінності, Політичні чи

соціальні процеси. Дослідження поширення різних ідей у контексті національної безпеки особливо важливі.

Таким чином, Інтернет стає ефективним інструментом, що дає користувачам можливість правильно спілкуватися з частинами реальності, найбільш підходящими для їхніх персонажів. В лютому 2019 року, Київським Міжнародним Інститутом Соціології було проведене всеукраїнське соціологічне опитування, щодо використання українцями інформаційних джерел [19]. З огляду на думки і думки дорослих жителів України (старше 18 років) про використання засобів масової інформації, медіаграмотності населення і російської пропаганди в ході опитування, аналогічне дослідження було проведено в 2018/2 році, результати цього дослідження можна побачити в динаміці.

Центральноукраїнські телеканали залишаються найбільш важливим джерелом інформації для абсолютної більшості населення, але за минулі роки на 12% менше респондентів найчастіше отримували інформацію про ситуацію в Україні порівняно з національними телеканалами світу (з 86% до 74%).Українські телеканали-найкращий ресурс для українських телеканалів. Також родичі, друзі і т.д. частка тих, хто говорить про тебе. Він знизився з 18% до 11%. Існує тенденція до скорочення використання друкованих ЗМІ. У той же час, що стосується інтернет-ресурсів, практично ніяких змін не відбулося: якщо в 2018/2 році 27% згадували інтернет-сайти в Україні, то зараз 27,5%; що стосується соціальних мереж, як в минулому році, так і зараз, 23,5% отримали інформацію з цього джерела. Якщо говорити про довіру до джерел інформації, то відносно найбільше респондентів довіряють також центральним українським телеканалам – 40%. Українським Інтернет-ЗМІ довіряють 14%, соціальним мережам – 12%, а решту джерел назвали не більше 6% респондентів [19]. Також є тенденція до зниження частки тих, хто довіряє інформації з українських Інтернет-сайтів і соціальних мереж.

Що стосується розвитку соціальних мереж, то ці засоби масової комунікації швидко набули популярності. Першою соціальною мережею, в якій використовувалися комп’ютерні технології, була технологія електронної пошти в 1971 році.

Пізніше, у 1988 році студент з Фінляндії Яркко Ойкарінен [20] винайшов технологію листування, що робить можливим спілкування в реальному часі.

Згодом, після винаходу Інтернету, Ренді Конрад заснував у 1995 році Classmates.com [24] – першу соціальну Інтернет-мережу в сучасному розумінні. Виявилося, що поняття масової комунікації користується великою популярністю, що дало поштовх стрімкому розвитку соціальних мереж в Інтернеті.

В 2004 році починається епоха Facebook, який всього за кілька років стає найпопулярнішою в світі соціальною мережею. Станом на грудень 2018 року, аудиторія активних користувачів фейсбук в Україні становить 13 млн. осіб [22].

Кількість соцмереж активно росла, деякі з них отримали певну спеціалізацію чи галузеву направленість. Наприклад LinkedIn переважно використовується для пошуку роботи, особливо популярна серед працівників IT сфери.

Різні типи соціальних мереж стали не тільки центром людського спілкування, але й платформою для різноманітних проектів з різним змістом і різними цілями.

З соціологічної точки зору соціальна мережа розуміється як соціальна структура, що складається з вузлів, об'єднаних одним або кількома типами взаємозалежності. Це дружба, економічні відносини, конфлікти, торгівля, погляди, ідеї, думки та спільні цінності. Моделі соціальних мереж можуть охоплювати різні рівні зв’язку, від сімейного до національного та глобального. Ця мережа уможливила безперервний та

інтенсивний обмін ідеями, на основі якого були створені різні віртуальні спільноти. В Інтернеті соціальні мережі – це програмні сервіси та платформи для взаємодії між людьми в групах. Об’єднайте різних користувачів та інформаційні ресурси відповідно до ваших інтересів.

Соціальні мережі також мають великий потенціал у сфері PR-діяльності та пропонують нові можливості для інтерактивної взаємодії.

Згідно з результатами дослідження Інтернет-середовища в Україні, більше половини всіх користувачів Інтернету вже охоплені соціальними мережами. За даними агентства PlusOne, Facebook користуються 2,1 мільйона українців у віці від 18 до 24 років, що становить 68,28% усіх жителів України цієї вікової групи.

Також агенство вважає, що кількість користувачів Facebook у віковій групі 25-35 років становить 4,6 мільйона, що становить 62,43% усіх жителів України цієї групи [20].

Сьогодні Інтернет стає загальновизнаним інформаційним каналом, що дозволяє проводити опитування громадської думки в режимі реального часу, запускати виборчі кампанії, надавати вичерпну інформацію про діяльність органів державної влади та отримувати зворотний зв'язок Дивлячись на ставлення населення до мережевих інформаційних ресурсів, можна помітити наступні тенденції.

Хоча сьогодні Інтернет є загальновизнаним інформаційним каналом, абсолютної довіри до суспільної свідомості як до джерела інформації немає. З огляду на те, що найбільше залученою в мережеву комунікацію є молодь віком від 18 до 35 років, більший вплив на неї має мережевий інформаційний простір.

Інтернет визнано альтернативним джерелом різноманітної нецензурної інформації, місцем спілкування, місцем віртуальної взаємодії людей, націй і приватних структур. Інтернет започаткував нову еру

спілкування та значно посилив вплив соціальних мереж на життя та повсякденне життя молоді.

Хоча багато людей не повністю усвідомлюють масштаби цього явища, соціальні мережі вже є найпопулярнішою діяльністю в Інтернеті. Сьогодні присутність соціальних мереж (Facebook, Twitter, блоги тощо) чітко помітна в повсякденному житті, і жодна частина суспільства не може відокремитися від неї.

Соціальні медіа змінили спосіб нашого спілкування та взаємодії один з одним. Все, що ми сьогодні пишемо, записуємо, зберігаємо, є свідченням того, що було описано вище.

Ми щодня створюємо величезні обсяги даних, ці величезні обсяги інформації, і швидкість, з якою ми ділимося своїми думками один з одним, вражає. Одна публікація, публікація в блозі чи твіт може охопити мільйони людей у всьому світі за лічені секунди. Це революційна особливість сучасних ЗМІ. Організації та великі підприємства використовують це середовище як ефективний інструмент для залучення нових клієнтів.

Соціальні медіа стали платформою для обговорення та переговорів, а фактичні учасники дискусії, тобто покупці та продавці, не взаємодіють безпосередньо та навіть не знають один одного. Кілька десятиліть тому вважалося, що це неможливо або можна побачити лише у фільмах і книгах, але сьогодні це реальність, у якій ми живемо, і ми є її частиною.

Багато компаній використовують соціальні мережі як для спілкування зі споживачами, так і для ведення бізнесу. Більш того, намічається ціла революція з використанням можливостей мережевого спілкування. Соціальні мережі стали центром і джерелом спілкування та інформації у Всесвітній павутині. Соціальні мережі та Інтернет подарували нам паралельний світ, який сильно відрізняється від реального.

Цей віртуальний світ є місцем, де двоє незнайомців можуть вільно взаємодіяти, встановлювати або розривати стосунки, налагоджувати зв'язки та ділитися майже будь-якими емоціями, приватно чи публічно.

Ця технологія дає людству можливість розширити свій кругозір, дозволяючи нам контактувати, спілкуватися та бачити в реальному часі людей, які фізично знаходяться далеко, у той час як деякі люди стають глибоко залежними від них. Користувачі навіть не усвідомлюють, що ігнорують свій реальний світ.

Це середовище також надає унікальну платформу та можливість для розвитку творчих, академічних і практичних навичок. Це дуже потужний інструмент, який ми можемо використовувати як забажаємо: спілкуватися з друзями та родиною, поширювати обізнаність, поширювати любов і свободу, поширювати повідомлення про рівність, боротися з дискримінацією, ненавистю та використовувати для поширення упереджень.

Ілюстративність тощ, що Зі 100 найбільш відвідуваних сайтів у світі сьогодні, 20 є соціальними мережами, а решта 60 пропонують широкий спектр можливостей спілкування.

Соціальні мережі наразі є величезними базами даних, що містять інформацію про сотні мільйонів людей у всьому світі, але вони також часто погано структуровані та погано захищені.

Користувачі добровільно надають інформацію про своє життя, інтереси, мрії та здібності. Ми жертвуємо конфіденційністю та безпекою нашого життя заради зручності та потужності соціальних мереж.

Замість гривневої плати кожен користувач платить за інформацією про своє життя та надає необмежений доступ до інформації про своє життя. В останні роки інформаційна безпека та захист даних у соціальних мережах стала актуальною темою.

У 2018 році Cambridge Analytica звинуватили у втручанні у вибори по всьому світу через крадіжку особистих даних потенційних виборців у соціальних мережах та використання інформаційних технологій для маніпулювання думкою. Велика частина даних була отримана з Facebook компанією Cambridge Analytica.

Згодом з'ясувалося, що співробітники компанії мали доступ до паролів більшості користувачів соціальної мережі Facebook, які не були захищені від третіх осіб. Втрата персональних даних користувачів різноманітних інтернет-ресурсів стала поширеним явищем.

Тим не менш, ми добровільно пропонуємо рекламодавцям можливість відображати цільову (таргетовану) рекламу та/або вибирати потенційно цікавий контент. Було б логічно припустити, що більшість людей все ще вірять і цінують святість свого особистого життя.

Тим не менш, дослідження показують, що кількість користувачів мережі ЗМК продовжує зростати як в Україні, так і в усьому світі.

1.2 Конфіденційність і безпека, ризики в соціальних мережах

Соціальні мережі без ризиків для безпеки не існують. Більшість соціальних мереж займаються питанням конфіденційності. В «The impact of polices on government social media usage: Issues, challenges, and recommendations» [27] пишеться, що існує багато проблем з управління інформацією в службах соціальних медіа, в основному в сфері конфіденційності та особистої інформації, а також того, як правильно зберігати та захищати її. Це часто робить інформацію доступною державним установам. Пояснюється це тим, що, як стверджує «A privacy paradox: Social networking in the United States» [20]: «Соціальні мережі створюють центральне сховище особистої інформації, яке продовжує зростати, оскільки користувачі постійно додають туди нову інформацію». Що ще гірше, підлітки, які менше турбуються про конфіденційність і безпеку, продовжують дуже охоче ділитися інформацією про себе. Іноді це робиться в ім'я популярності. Іноді це просто чиста недбалість. Це велика частина проблеми, і можливе рішення для боротьби з цією проблемою буде запропоновано пізніше. У статті йдеться про те, що «приватні та публічні межі просторів соціальних медіа розмиваються». Далі в статті наголошується, що батьки часто не знають і не піклуються про те, що їхні діти вивчають онлайн.

Інший основний ризик конфіденційності та безпеки інформації в соціальних мережах полягає в централізованій архітектурі цих платформ. Як зазначалося раніше, сервери соціальних медіа є справжньою золотою шахтою особистої інформації, яку безпосередньо та добровільно надають підлітки та дорослі користувачі. У статті «Privacy and Security: Online Social Networking» стверджується, що це створює серйозні конфлікти та може призводити до таких негативних явищ, як крадіжка особистих даних та продаж даних користувачів третім особам. Користувачі змушені довіряти своїм соціальним мережам щодо захисту своєї інформації, хоча

насправді вона часто продається третім сторонам або стає здобиччю хакерів. У статті також зазначено, що хоча Facebook додав налаштування конфіденційності, які користувач може змінювати, їхні налаштування за замовчуванням є загальнодоступними під час першого створення облікового запису. Отже, новий користувач, який не змінює ці налаштування на більш обмежувальні, фактично публікує інформацію, яку може бачити будь-хто. Це означає, що будь-яка особа з доступом до мережі може легко знайти та використовувати особисту інформацію користувача для власних цілей. У статті «Privacy and Security: Online Social Networking» також йдеться про те, що кількість інформації, яку користувачі викладають у своїх профілях на популярних сайтах соціальних мереж, може бути об'єднана для створення детального портрета користувача. Зловмисники можуть використати цю інформацію для створення фальшивого профілю цієї особи, додати всіх друзів жертви, а потім обманом отримати більше особистої інформації від друзів користувача. Це дозволяє зловмисникам збирати ще більше даних про користувача, що може призвести до ще більших ризиків для безпеки та конфіденційності. У підсумку, користувачі соціальних мереж повинні бути обережними з тим, яку інформацію вони викладають, і активно керувати своїми налаштуваннями конфіденційності, щоб мінімізувати ризики.

«Social Networking Sites and Their Security Issues» [21] називає цю практику "клонуванням профілю". Стаття стверджує, що деякі злодії викрадають інформацію про користувачів з одного сайту, щоб створити підроблений профіль на іншому. Вона заявляє, що інформація також може бути викрадена у користувачів через використання фішингових атак, де інформація збирається про користувачів шляхом створення фальшивих веб-сайтів, які запитують особисту інформацію або навіть паролі та номери соціального забезпечення. Згідно з цією статтею, різні інші атаки спрямовані або на використання особистої інформації користувачів, або на

зараження їхніх систем вірусами. До них належать натискання клавіш, під час яких зловмисник публікує відео для користувача і, коли користувач його відтворює, впроваджує шкідливий код у систему, а також атаки ін’єкцій, під час яких використовується зламаний форум, і кожен, хто відвідує цей форум, заражає свою систему троянським вірусом. Інші ризики включають онлайн-шахрайство та залякування. Ризик, який бере на себе користувач, залежить від того, скільки особистої інформації він публікує та як налаштовує свої налаштування безпеки та конфіденційності.

Таким чином, користувачі повинні бути дуже обережними щодо того, які дані вони надають в інтернеті, і уважно стежити за своїми налаштуваннями конфіденційності, щоб мінімізувати ризики. Без належних заходів безпеки користувачі можуть стати жертвами численних кібератак, які не тільки загрожують їх особистій інформації, але й можуть спричинити значні фінансові та емоційні збитки. Зловмисники також можуть використовувати викрадену інформацію для шантажу або вимагання, що додає ще один рівень загрози. Крім того, втрачена або викрадена інформація може призвести до довготривалих наслідків, таких як крадіжка особистих даних, що може тривати роками. Постраждалі від таких атак часто стикаються з труднощами у відновленні своєї репутації та фінансової стабільності. Користувачі повинні бути обізнаними про ці ризики і вживати відповідних заходів для захисту своїх даних в онлайн-середовищі. Найбільша проблема полягає в тому, що багато користувачів не знають про налаштування конфіденційності та способи їх використання. Вони також «не знають про ризики, пов’язані із завантаженням конфіденційної інформації».

Дослідження показали, що сайти соціальних мереж створені для обслуговування великої кількості користувачів в одному місці, багато з яких не знають, як використовувати налаштування конфіденційності. Ці сайти цінують «відкритість, зв’язок і обмін інформацією з іншими – на

жаль, саме ті аспекти, які дозволяють кіберзлочинцям використовувати ці сайти як зброю для різних злочинів». Співробітники часто публікують інформацію про компанію в соціальних мережах, піддаючи організації ризику, ким вони працюють для.

Таким чином, відповідно до «Privacy and Security: Online Social Networking» [25], зрозуміло, що навіть якщо технології та політика можуть використовуватися на сайтах соціальних мереж так само, як і будь-яка інша організація, централізована структура та величезний репозиторій приватної інформації створюють великі прогалини в галузі безпеки. Це означає, що користувачі часто опиняються у вразливому становищі, коли їхні особисті дані можуть бути використані для зловмисних цілей. Зокрема, злочинці можуть отримувати доступ до великих обсягів інформації, використовуючи різні методи атак, такі як фішинг або злом акаунтів.

Для подолання цих проблем необхідно впроваджувати більш суворі політики безпеки, які регулюють збирання, зберігання та обробку даних користувачів. Окрім цього, користувачам слід проявляти обережність та використовувати здоровий глузд під час публікації своїх даних в інтернеті. Соціальні мережі також повинні розглянути можливість змін у своїй архітектурі, щоб мінімізувати ризики витоку даних. Наприклад, можна використовувати децентралізовані підходи до зберігання даних, що ускладнить доступ до них для хакерів [3].

Загалом, проблема конфіденційності в соціальних мережах є складною та багатоаспектною. Вона вимагає комплексного підходу, який включає технологічні, політичні та освітні заходи. Лише за таких умов можна досягти більш високого рівня безпеки та захисту персональних даних користувачів. Водночас, важливо продовжувати дослідження та моніторинг нових загроз і викликів, які виникають у цій галузі, щоб своєчасно адаптувати стратегії захисту.

1.3 Проблема конфіденційності інформації у сучасних месенджерах

Одночасно з розвитком комунікації йшла еволюція кіберзлочинності. Вірус Мікеланджело з'явився в 1992 р. [26] році і вважається першим деструктивним вірусом. У 1995 році з'явився макровірус, який спочатку поширювався через документи Word. У 1999 році з'явився нешкідливий черв'як happy99, перший вірус, який поширювався через електронну пошту. Першим вірусом, якому вдалося отримати вигоду від зараженого носія, був Fizzer, який з'явився в 2003 році.

Не існує ідеального засобу для захисту будь-якої системи. Це завжди компроміс, нескінченний, а не одноразовий. Те, що сьогодні безпечно, може стати небезпечним завтра.

Конфіденційні дані часто можуть мати різні форми та формати. Користувачі часто помилково вважають, що конфіденційна інформація, яку вони поширюють, може бути відправлена тільки в текстовому форматі (ім'я користувача, пароль, номер паспорта і т.д.). Однак ви можете розголошувати конфіденційну інформацію Користувача третім особам, навіть якщо ви передаєте матеріали будь-якого характеру. Метадані, тобто дані про дані, важко приховати. Це інформація, в якій перераховані такі характеристики, як IP-адреса відправника, що стосуються інформації (файлів, фотографій і т.д.). Однак вона не описує зміст повідомлення. Правові системи часто захищають вміст більш суворо, ніж метадані. Наприклад, у Сполучених Штатах правоохоронцям не потрібен ордер на прослуховування особи, але їм потрібно мати право на список людей, яким ця особа телефонувала. За даними NowSecure Mobile Security Report [21], чверть мобільних додатків включає один або декілька недоліків безпеки високого ризику. 35% повідомлень, що надсилаються з мобільних пристроїв, виявляються не зашифрованими. 43% користувачів не встановили PIN-коду, графічний або цифровий пароль на свої пристрої. 50% пристроїв підключаються до незахищеної бездротової мережі

принаймні раз на місяць у США. Половина популярних додатків надсилає рекламним компаніям інформацію, таку як номери телефонів, ідентифікатори пристроїв, інформація про дзвінки та географічні координати Користувача.

Прихильник концепції інтернет-безпеки і засновник програми обміну миттєвими повідомленнями E2E (End-to-End Encryption) під назвою Telegram, компанія стверджує, що інтернет-компанії, такі як Google і Facebook, спритно вкрали конфіденційні дані, і що найважливіше в забезпеченні конфіденційності - це захист повідомлень, фотографій публічних користувачів. та інші дані Користувача. Це переконує громадськість, що вони приховують дані.Facebook стверджує, що такі інтернет-компанії вміло крадуть конфіденційні дані. Додавши правильні налаштування, компанії можуть привернути увагу громадськості до надання персональних даних маркетологам і третім особам. Джуліан Ассанж, головний редактор Wikileaks, також підтримує концепцію безпеки в Інтернеті. У своїй книзі "Google Met WikiLeaks [28]" він поділяє подібну точку зору, зазначивши, що Google – американська компанія і тісно співпрацює з політичними та військовими структурами, часто дає доступ до конфеденційних даних користувачів.

Необхідність миттєвого обміну повідомленнями полягає у запобіганні несанкціонованому доступу до комунікацій між користувачами. 1. Ще однією сферою відповідальності Користувача за безпеку його особистих даних є процес збору, обробки, зберігання та розповсюдження конфіденційних даних користувачів від постачальників послуг, які використовуються для створення реклами, залякування та поширення політичних поглядів, що в кінцевому підсумку підриває єдність соціальних верств, відомих в даний час як в СИЛУ своєї природи.

Secure IM спеціалізується на шифруванні вмісту повідомлень і надає ключ для розшифровки інформації тільки тому користувачеві, у якого є

доступ. Ідея користувальницького захищеного месенджера полягає в забезпеченні безпеки для тих, хто нічого не розуміє в безпеці. Отже, додаток повинен бути не тільки безпечним, але і швидким, потужним і зручним у використанні.

При використанні на робочому місці додаток для обміну миттєвими повідомленнями має безліч функцій, але він також несе ризики для безпеки та інші небезпеки. Існує безпека та ризик отримання згоди, неправильного використання та втрати інтелектуальної власності.

Під час сеансу спілкування в загальнодоступній мережі кожен користувач Інтернету має доступ до конфіденційних даних користувача. У цьому контексті підвищення рівня захисту передачі та прийому інформації від Постачальника послуг має вищу цінність, ніж зміст інформації, що передається від користувача. Інформація, що надсилається за допомогою миттєвих повідомлень, не повинна відстежуватися або записуватися з метою підвищення безпеки компанії. Це також стосується пристроїв, які використовуються для передачі інформації. Смартфони збирають багато конфіденційних даних, включаючи країни, місцезнаходження та переглянутий вміст. Однак користувачі не можуть повністю покласти відповідальність за конфіденційні дані на постачальників послуг або пристрої. Найбільша частка відповідальності за поширення, використання і зберігання даних лежить на користувача. Ця відповідальність береться до уваги при правильному розумінні переданих даних, наприклад, при наданні дозволу на використання даних, такого як дозвіл на збір файлів cookie при відвідуванні сайту або дозвіл на обробку даних при реєстрації на сайті. Для тих організацій, що збирають дані заради отримання наживи існує три головні цілі: дані, справжність та доступність. Дані означають будь-яку конфіденційну інформацію про особу чи компаніію. Вони інтерпретуються як логін автентифікації та паролю, приватну інформацію або журнали активності, зібрані або вкрадені програмним забезпеченням.

Справжність або достовірність розуміється як відповідність отриманих даних до реальних об’єктів чи осіб в реальному часі. Від цього параметру залежить успішність операції з їх використання. Доступність в такому разі мається на увазі як ступінь того, наскільки важко ці дані зібрати і опрацювати. Цей параметр відповідає за цінність цих даних.

Тому провайдери послуг впроваджують заходи для підвищеного захисту від збору конфіденційної інформації та попередження користувачів про потенційну небезпеку.

Наприклад, з початку липня 2018 року Google Chrome позначає всі сайти, які не мають SSL-сертифікату для безпечного з'єднання, як незахищені, тобто вони не можуть встановити зашифроване з'єднання HTTPS. Таким чином користувач дізнається про потенційну небезпеку одразу як переходить за посилання сайту і далі сам вирішує чи користуватися даним ресурсом чи ні.

Одним з найбільш популярних засобів захисту особистої переписки, який реалізований у месенджерах – це E2E-шифрування, спосіб передачі даних, коли доступ до повідомлень мають виключно користувачі, які задіяні в спілкуванні.

За рахунок використання криптографічних ключів технологія E2E передбачає, що контроль над листуванням здійснюється безпосередньо користувачами, а розшифрувати повідомлення не можуть ні перехоплювачі, ні сервери, які передають дані.

Для того, щоб зрозуміти, що з себе представляє метод E2E, по-перше, необхідно з'ясувати, що не є наскрізним шифруванням. Відомо про шифрування, яке використовується веб-сайтами з метою захисту онлайн активності. Наприклад сервіс https://www.gmail.com, протокол HTTPS на початку адресного рядка свідчить про те, що для шифрування передачі даних між комп'ютером і серверами Google використовуються криптографічні протоколи SSL або TLS. Даний протокол є більш

безпечним, ніж HTTP і широко застосовується веб-ресурсами для захисту від перехоплення даних. Головним недоліком технології HTTPS є той факт, що при спілкуванні двох користувачів передані дані проходять через централізовані сервера (наприклад, GMail), які мають ключі для розшифровки інформації. Щоб виключити сервера з ланцюжка, підвищивши таким чином приватність даних, можна використовувати наскрізне шифрування.

За допомогою наскрізного шифрування кінцевими точками передачі є безпосередньо пристрої відправника та одержувача. Повідомлення шифрується локально на пристрої відправника, і його можна розшифрувати лише на пристрої одержувача. Наскрізне шифрування часто називають «шифруванням на стороні клієнта» або «нульовим доступом», оскільки шифрування відбувається на пристроях кінцевих користувачів, а не на хмарних серверах. Завдяки цій функції наскрізне шифрування запобігає можливому зчитуванню серверами даних користувача. При реалізації наскрізного шифрування розрізняють два типи криптографічних алгоритмів: симетричні та асиметричні.

1.4 Огляд проблематики в сучасній зарубіжній та вітчизняній науковій спільноті

В сучасному цифровому віці, коли інформаційні технології стрімко розвиваються та впливають на всі сфери життя, питання конфіденційності особистої інформації стає все більш актуальним та нагальним. Суспільство стикається з безпрецедентними можливостями комунікації та обміну даними завдяки новітнім каналам комунікації, але одночасно із цим зростають загрози для приватності та безпеки індивідів. Ця дипломна робота присвячена дослідженню проблеми конфіденційності особистої інформації у контексті постійного розвитку та поширення нових засобів комунікації як у світі, так і в Україні. В даному розділі ми розглянемо огляд сучасних досліджень та підходів до вирішення цієї проблеми як у міжнародній, так і вітчизняній науковій спільноті.

Для огляду запропонованих була обрана структура подачі інформації від найменш розкритої з точки зору огляду теми до найбільш грутовної роботи.

У своїй роботі Н.Б. Макух, Т.О. Чоп. розкривають загальні питання принципу роботи соціальних мереж, принцип поширення та витоку конфіденційної інформації, як рукотворне явище самим користувачем [29, с. 1]. Також автор роботи пропонує розглянути практичні рекомендації як запобігти витоку особистої інформації. Робота базується на теоретичному огляд джерел та не описує власні дослідження цієї теми на практичному рівні [29, с. 2].

Друга робота, що представлена в огляді, висвітлює проблему конфіденційності персональної інформації у соціальних мережах з боку юридичної призми вивчення. Включення цієї роботи до списку опрацьованих допомагає нам отримати мультиканальний доступ до питання для подальшого глибшого вивчення питання.

У роботі Глянько О. С. розглядає дану тему з юридичної призми та в якості джерел для аналізу використовує законодавчу базу України. Найбільше в роботі розкрита позиції держави відносно захисту персональних даних громадян, резидентів та нерезидентів України [30]. За допомогою цього аналізу ми отримуємо розуміння про важливість даної теми для більш глибокого вивчення з боку громадян.

В роботі Недашківський Г. В. розглядає проблему конфіденційності з розрізі неможливості зберігати свої дані конфіденційними при умовах користування соціальними мережами. Автор роботи розглядає занепокоєння користувачів за збереження конфіденційності свої даних з боку великих компаній, корпорацій. В роботі описуються дослідження інших авторів про ставлення користувачів до цього питання, також автор розкриває тему способів використання цих даних ат цілей, які можуть стояти за їх незаконним збором, викраденням тощо. [31]

Четверте дослідження “Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator” за авторством Subai Chen , Chenyu Gu, Juan Wei, Mingjie Lvcorresponding, що пула опублікована на сайті National Library of Medicene в січні 2023 року.

Дослідження описує збільшення частки випадків порушень онлайн-приватності через витік особистої інформації користувачів соціальних мереж. Незважаючи на це, спостерігається тенденція до втоми від захисту конфіденційності, що сприяє ще більшому порушенню приватності та утворює замкнуте коло. Дослідженням вивчено вплив досвіду порушення конфіденційності на наміри користувачів захищати свою приватність. Теорія мотивації захисту широко використовується в цих дослідженнях, проте вказано на потребу у врахуванні індивідуальних емоційних факторів. З метою заповнення цих прогалин використовується модель заснована на теорії мотивації захисту та теорії регулювання фокусу,

де введено концепцію втоми від приватності. Результати дослідження показали, що досвід порушення приватності сприяє збільшенню намірів захисту приватності, при цьому цей процес медіюється відгуковими витратами та втомою від приватності. Втома від приватності знижує бажання особи захищати свою приватність, що є ключовим фактором "лежати плоско" у захисті приватності. Особи з акцентом на просування менш схильні до втоми від приватності, ніж ті, що мають акцент на запобігання. Таким чином, втома від приватності може бути впливовим фактором у розвитку стратегій захисту приватності, що вказує на потребу у подальших дослідженнях [32].

З огляду на короткий опис розглянутої літератури можна зробити висновок, що в Україні дане питання не є повністю і вичерпно вивченим. Українській спільноті не вистачає досліджень на дану тему з предметними результатами, що б описували ситуації щодо розуміння захисту власної конфіденційної інформації з боку громадян-користувачів. Такі дані було б вкрай важливо отримати також у розрізі російсько-української війни, в ході якої активно використовуються особистій дані користувачів з україни заради фішингових атак та побудови ІПСО.

Висновки до розділу 1

У розділі 1 було розглянуто теоретичні засади для вивчення проблематики конфіденційності, що дозволило створити базис для подальшого дослідження питання. Цей розділ охоплює різні аспекти, пов'язані з конфіденційністю та безпекою даних у соціальних мережах та інших онлайн платформах.

У підрозділі 1.1 було презентовано погляд на соціальні мережі як на новітні канали комунікації. Було розглянуто, як соціальні мережі трансформували спосіб, у який люди взаємодіють, діляться інформацією та створюють спільноти. Також було проведено аналіз досліджень інших вчених та організацій, що стосуються використання соціальних мереж та їх впливу на суспільство.

У підрозділі 1.2 розкривається питання конфіденційності та безпеки даних користувачів. Описані ризики, що можуть виникнути при використанні соціальних мереж, такі як несанкціонований доступ до особистої інформації, зловживання даними та кіберзагрози. Також згадано погляд на конфіденційність даних з боку розробників додатків та сервісів, які створюють політики конфіденційності для захисту користувачів. Були детально розглянуті різні підходи до забезпечення конфіденційності та приклади ефективних політик.

Підрозділ 1.3 описує проблему конфіденційності у специфічному середовищі - у месенджерах. Було досліджено еволюцію ризиків для користувачів, починаючи з появи першого макровірусу, і до сучасних заходів, що вживаються компаніями, такими як Google, для забезпечення безпечного з’єднання та зберігання даних. У цьому підрозділі також розглянуто питання шифрування повідомлень, двофакторної автентифікації та інших технологій, спрямованих на підвищення безпеки користувачів у месенджерах.

Підрозділ 1.4 дозволяє детальніше оглянути роботи інших дослідників у векторі конфіденційності даних в мережі та соціальних мережах. Було зібрано та проаналізовано різноманітні дослідження, що висвітлюють різні підходи до забезпечення конфіденційності, виклики та новітні рішення в цій галузі. Огляд включає як теоретичні, так і практичні аспекти досліджень, що дозволяє скласти комплексне уявлення про стан питання на сьогоднішній день.

Таким чином, розділ 1 створює ґрунтовну основу для подальшого вивчення проблематики конфіденційності та безпеки даних у цифрову епоху, акцентуючи увагу на ключових питаннях та сучасних викликах, з якими стикаються користувачі та розробники.

Розділ 2 Основні результати дослідження щодо ставлення користувачів до безпеки їхніх конфіденційних даних

Після детального вивчення теоретичної бази та аналізу різноманітної наукової літератури на цю тему, а також проведення огляду досліджень з інтердисциплінарним підходом до вивчення інформаційних питань, доречним було зробити висновок про необхідність розробки гіпотези стосовно ставлення користувачів до власних особистих даних та способів їх захисту.

Проаналізувавши розділ “1.4 Огляд проблематики в сучасній зарубіжній та вітчизняній науковій спільноті”, ми прийшли до висновку, що питання конфіденційності та захисту даних не отримало належного розгляду в літературі та дослідженнях, і це потребує подальшого уваги в науковому дискурсі. Додатково, в аналізі роботи “Неможливість збереження конфіденційності у соціальних мережах” [31] зазначено, що багато користувачів перекладають відповідальність за захист своїх даних на провайдерів послуг та інші компанії. Отже, наша гіпотеза полягає в тому, що соціальні мережі можуть впливати на ставлення користувачів до захисту їхніх особистих даних через підвищення ризику розголошення цих даних та збільшення відповідальності за захист даних на інших учасників інтернет-середовища.

У світлі цієї інформації та з урахуванням теоретичного фундаменту та практичних даних, було вирішено здійснити дослідження з метою кращого розуміння підходів користувачів до захисту їхніх даних та їхніх особистих уподобань у цьому контексті. Основна мета цього дослідження полягатиме в тому, щоб вивчити, як користувачі реагують на ризики та як вони реалізують заходи безпеки в онлайн-середовищі.

Також під час дослідження ми маємо отримати відповіді на наступні питання:

1. Чи мають юзери коректне розуміння, які саме дані є конфіденційними та вартими захисту?
2. На якому рівні знаходиться розуміння реципієнтів, що є конфіденційними даними?
3. Чи вважають реципієнти соціальні мережі полем власної відповідальності за поширення їхніх чутливих даних?

2.1 Методологія, вибірка та презентація питань для проведення дослідження

Вибір якісного методу дослідження для аналізу проблеми конфіденційності особистої інформації у світлі розвитку новітніх каналів комунікації був зумовлений кількома ключовими факторами.

По-перше, якісний метод дозволяє отримати детальні та глибокі відповіді від респондентів. Це особливо важливо в контексті проблеми конфіденційності, оскільки він зазвичай пов'язаний з особистими переживаннями, страхами та цінностями. Анкетування та співбесіди дозволяють розкрити більше інформації про думки та почуття респондентів, їхні уявлення про приватність та погляди на захист особистої інформації.

По-друге, якісний підхід дозволяє глибше зрозуміти контекст та обставини, в яких виникають певні погляди та поведінка. Це дозволяє нам звернути увагу на фактори, що впливають на рішення користувачів щодо конфіденційності, такі як культурні чи соціальні впливи, особистісні переживання та інші фактори.

Крім того, якісні методи дозволяють отримати детальніше розуміння індивідуальних досвідів та відмінностей між різними групами користувачів. Це особливо важливо для розуміння того, як різні люди реагують на питання приватності та як це впливає на їхню поведінку в онлайн-середовищі.

Отже, використання якісного методу дослідження було обрано з метою отримання глибшого та більш повного розуміння проблеми конфіденційності особистої інформації, а також для виявлення складних взаємозв'язків та факторів, що впливають на ставлення користувачів до цієї проблеми.

Обираючи методологію дослідження через анкетування та онлайн-опитування, ми виходили з декількох факторів, які вважаємо важливими для ефективного та об'єктивного збору даних щодо захисту особистих даних у соціальних мережах.

По-перше, цей підхід вважається найбільш доступним та ефективним у сучасному цифровому світі. Він дозволяє залучити широке коло респондентів з різних регіонів та вікових груп, що сприяє отриманню репрезентативних даних. Також це знижує витрати на дослідження та робить його більш масштабним.

По-друге, використання Google-форми для проведення дослідження має ряд переваг. Це включає високу гнучкість у формулюванні питань, можливість швидкого збору та аналізу даних, а також зручність для респондентів у заповненні опитувальника. Такий підхід дозволяє легко структурувати дані для подальшого аналізу.

По-третє, через розповсюдження опитування через мережу, я отримала можливість залучити широке коло користувачів соціальних мереж, що забезпечило більшу увагу до дослідження та покращило його репрезентативність. Також це дозволило залучити респондентів з різними соціальними та демографічними характеристиками, що робить результати дослідження більш комплексними та репрезентативними.

Таким чином, вибір методології дослідження через анкетування та онлайн-опитування був обґрунтований цілком практичними та методологічними міркуваннями, спрямованими на максимально об'єктивне та дієве проведення дослідження.

З урахуванням специфіки теми і питань, я вирішив провести дослідження в анонімному форматі, щоб забезпечити об'єктивність результатів і уникнути страху реципієнтів викрити свої відповіді. Це дозволило отримати чистий і достовірний результат дослідження, оскільки

респонденти мали відчуття безпеки і конфіденційності у наданні відповідей.

Щодо збору відповідей та залучення реципієнтів, ми активно використовували поширення посилання на опитування у різних тематичних групах, колективах та спільнотах для спілкування. Цей підхід дозволив залучити реципієнтів з різних соціальних та демографічних груп, що забезпечило різноманітність у вікових категоріях, рівні освіти та досвіді життя, що стало ключовим для отримання репрезентативних даних і об'єктивної оцінки ставлення користувачів до захисту їхніх особистих даних у соціальних мережах.

Для проведення дослідження та збору відповідей, було обрано широку репрезентативну вибірку реципієнтів з різних вікових груп. Були залучені такі вікові категорії: 18-25 років, 25-35 років, 35-45 років та 45+. Цей вибір вікових груп був обгрунтований метою дослідження, яка полягає у зборі широкого та різноманітного поперечного перерізу розуміння користувачів щодо конфіденційності власних даних та способів їх захисту.

Важливо зазначити, що такий вибір вікових груп також допоможе виявити можливу кореляцію між ставленням до своїх чутливих даних та віком або ступенем освіти. Це дозволить зробити більш об'єктивні висновки щодо того, як різні групи користувачів реагують на питання захисту особистих даних у соціальних мережах.

Збір даних від різних вікових груп є ключовим елементом дослідження, оскільки дозволяє отримати більш повне та різноманітне уявлення про перспективи захисту особистої інформації серед різних категорій користувачів. Такий підхід створює можливість для глибшого аналізу та розуміння тенденцій у ставленні до приватності в цифровому середовищі.

Для вирішення поставлених завдань та з'ясування важливих аспектів нашого дослідження, ми розробили комплексне питання, що охоплює широкий спектр аспектів проблеми. Наш набір питань орієнтується на збирання різноманітних відповідей та думок, спрямованих на виявлення ставлення користувачів до конфіденційності та їхнього уявлення про захист особистої інформації. Кожне питання має свою вагу в контексті дослідження та дозволяє нам систематизувати і аналізувати отриману інформацію для досягнення наших цілей та висновків. Пропонуємо детальніше оглянути питання та їх формулювання для більш глибокого розуміння представлених у наступному розділі результатів.

Для отримання повної та аналітичної відповіді на питання про кореляцію рівня освіти та віку до ставлення до своїх чутливих даних, ми включили в наш дослідницький набір питань запити щодо рівня освіти та віку респондентів. Питання про вікові групи були ретельно структуровані відповідно до категорій, які відображають основні покоління, а саме: 18-25 років, 26-35 років, 36-45 років та 45 років і старше. Цей підхід має обґрунтування в уявленнях про різницю у сприйнятті інформації, її засвоєння та значимості для різних поколінь. Враховуючи широкий спектр соціокультурних та технологічних змін, важливо розглядати ці питання в контексті вікових та генераційних розбіжностей, які можуть впливати на сприйняття та реакцію на проблеми конфіденційності даних. Такий підхід дозволяє не лише виявити залежності між освітою, віком та ставленням до особистих даних, а й зрозуміти, як саме ці фактори взаємодіють у сучасному цифровому середовищі.

Додатково, для забезпечення широкого спектру покриття дослідження ми врахували різні рівні освіти. Питання про рівень освіти були розподілені за більш класичною схемою градації, що відповідає національним стандартам. Такий підхід дозволить отримати не лише кількісні дані, але й якісну інформацію, оскільки він дозволяє зіставити

рівні освіти зі ставленням до конфіденційності даних та розглядати цю динаміку в контексті змін у суспільстві та технологіях.

Отже, обрані питання та методологія дослідження дозволять нам не лише отримати повну картину ставлення користувачів до своїх особистих даних, але й зрозуміти глибину та широту проблеми конфіденційності у сучасному цифровому середовищі.

Питання “Перерахуйте всі наведені типи даних, які ви вважаєте конфіденційними ” направлене на визначення рівня розуміння сутності чутливих даних серед реципієнтів. Для зручного отримання та опрацювання результатів питання було поставлено у формі вибору усіх відповідей, що реципієнт вважає правильними. Серед 10 категорій даних реципієнти мали обрати лише ті відповіді, що відповідають їх уявленню про персональні дані. Для більш широкої картини до списку з 6 (ПІБ; Домашня адреса; геолокація в реальному часі; метадані надісланих файлів; номер паспорту; дата народження) категорій, що дійсно відносяться до чутливих конфіденційних даних було додано ще 4 (дівчое прізвище матері; номер школи; в якій навчалися перші 4 роки, музичні вподобання; група крові), які мімікрують під персональні дані. Таким чином відповіді учасників опитування всебічно репрезентують розуміння того, що є чутливими даними. Для дослідження чутливими даними виступають ті категорії, що відповідають визначенню, а саме дані чи сукупність даних, що можуть ідентифікувати персону.

Питання “Чи читаєте ви документи на сторонці при реєстрації про збір та обробку ваших персональних даних?” є одним із ключових у анкеті та має форму закритого типу з трьома варіантами відповіді: “так”, “ні” та “важко відповісти”. Це питання спрямоване на оцінку рівня усвідомленості реципієнтами процесу збору, обробки, зберігання та передачі їх особистих даних, які вони надають сервісам та платформам, які вони використовують. Відповіді на це питання дозволяють оцінити ступінь уважності та

зацікавленості користувачів у питаннях приватності та захисту особистих даних. Такий аналіз є важливим для розуміння практик користувачів у сфері конфіденційності та розробки ефективних стратегій захисту інформації.

Наступні три запитання в анкеті стосуються безпеки даних користувачів: “Чи використовуєте ви різні паролі для кожного аканту?”, “При зміні паролю базується ваш новий пароль на основі старого?” та “Чи використовуєте ви пов'язані паролі для своїх акаунтів в соціальних мережах? Наприклад, qwerty5678 та 5678qwerty”. Ці питання спрямовані на виявлення практики користувачів у створенні і використанні паролів для захисту своїх акаунтів. Вони передбачають три можливі відповіді: “так”, “ні” та “важко відповісти”. Аналіз відповідей на ці питання дозволить оцінити ступінь усвідомленості користувачів щодо важливості безпеки в інтернеті та їхню готовність вживати заходи для захисту своїх особистих даних.

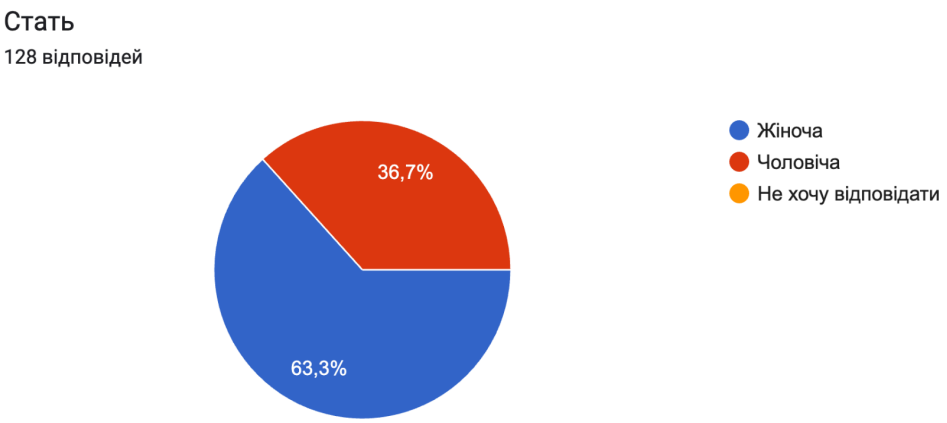
Запитання “Чи публікуєте ви фотографії з відпустки з геолокацією в реальному часі?” та “Чи публікуєте ви в соціальних мережах своє місцезнаходження в реальному часі? Наприклад, Stories з відміткою закладу, де ви наразі знаходитеся”, “Чи публікуєте ви в соціальні мережі матеріальні підтвердження своїх досягнень?

Наприклад, дипломів, лотерей, квитків і т.д.”, “Чи вказуєте ви свої реальні дані (ім'я, прізвище, місто проживання) в профілі або при реєстрації? ” мають на меті дослідити, наскільки свідомі користувачі щодо можливих ризиків, пов'язаних з публікацією особистої інформації в соціальних мережах. Ці запитання допомагають уявити реальні ситуації, коли викладена інформація може бути використана зловмисниками. Це особливо актуально в контексті функцій, які дозволяють додавати географічні мітки до фотографій та Stories, що розміщуються у соціальних мережах. Підставою для включення цих питань було переконання, що

багато користувачів можуть мають ілюзію безпеки у віртуальному просторі соціальних мереж, тому що вони сприймають цей сервіс як зону розваг та відпочинку, не усвідомлюючи потенційні небезпеки, пов'язані з недбалістю до розголошення особистих даних.

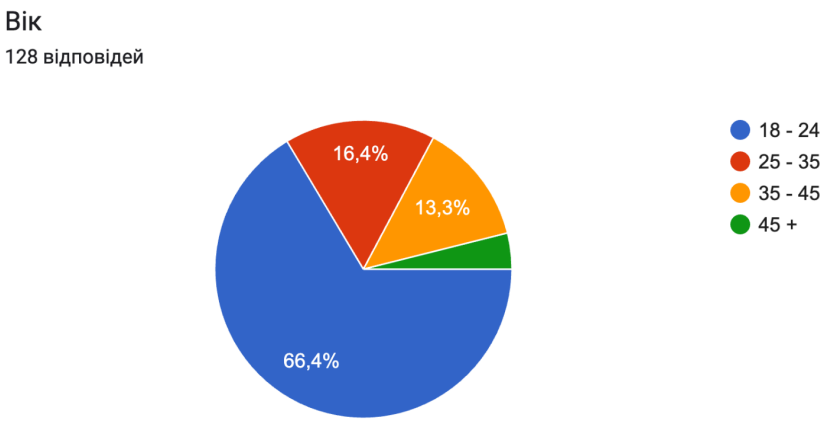
2.2 Представлення та інтерпретація результатів проведеного дослідження

Під час проведення дослідження ми звернулися до 128 реципієнтів, щоб опитати їх та опрацювати отримані результати. Це дозволило нам отримати об'єктивну картину щодо ставлення користувачів до розглянутої проблеми. Аналіз результатів надав цінну інформацію для подальших висновків та рекомендацій у дослідженні. Такий обсяг дослідження забезпечив достатню статистичну репрезентативність даних. В цілому, процес опитування та обробки результатів був важливим етапом у розвитку нашої роботи. Згідно з результатами дослідження на Діаграмі 2.1, серед 128 реципієнтів 36,7% становлять чоловіки, тоді як 63,3% - жінки. Варто зауважити, що жоден з реципієнтів не обрав опцію "Не хочу відповідати" під час опитування. Такі відсотки статевого розподілу учасників дослідження дозволяють отримати репрезентативну картину стосовно гендерного складу обраної групи. Розподіл за статевою ознакою є важливим аспектом у збалансованому аналізі результатів дослідження та формуванні відповідних висновків.



Діаграма 2.1 Стать респондантів

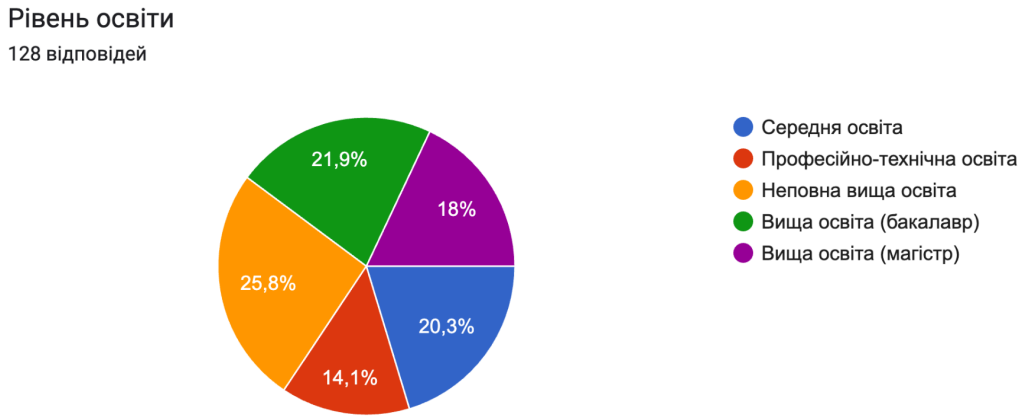
Згідно з дослідженням, стосовно вікового розподілу реципієнтів, ситуація представляється наступним чином: найбільшою часткою опитаних є особи віком 18-24, що складають 64,4% від загальної кількості; наступною за чисельністю групою є вікова категорія 25-35 років, яка становить 16,4% усіх реципієнтів; третє місце за чисельністю належить віковій групі 35-45 років, яка становить 13,3% від загальної кількості опитаних; найменшою з усіх категорій є вікова група 45+, яка складає всього 3,9% від загальної кількості реципієнтів. Ця інформація надає можливість зрозуміти динаміку розподілу реципієнтів за віком та виділити основні групи, які складають основу дослідження. Візуальне представлення цих даних можна знайти на Діаграмі 2.2, яка дозволяє зробити аналіз розподілу за віком більш зрозумілим та інформативним.



Діаграма 2.2 Вік респондентів

Запитання про рівень освіти у дослідженні містить п'ять опцій для відповіді, які відповідають національному стандарту градації рівнів освіти: середня освіта, професійно-технічна освіта, неповна вища освіта, вища освіта (бакалавр), вища освіта (магістр). Виходячи з відповідей реципієнтів, найбільшу частку складають особи з неповною вищою освітою (25,8%). Друге місце за часткою належить вища освіта (бакалавр) з результатом 21,9%. Третє місце у відсотковому співвідношенні займають

особи з середньою освітою (20,3%), а четверте - ті, що мають вищу освіту (магістр), яких становить 18% від загальної кількості опитаних. Найменшою часткою серед реципієнтів є група з професійно-технічною освітою (14,1%). Графічне представлення цих даних знаходиться на Діаграмі 2.3, що дозволяє візуально оцінити розподіл реципієнтів за рівнем освіти у дослідженні.



Діаграма 2.3 Рівень освіти респондентів

Питання “Перерахуйте всі наведені типи даних, які ви вважаєте конфіденційними ” має на меті визначити рівень розуміння одержувачем природи конфіденційних даних.

Для зручності отримання та обробки результатів питання задавалися у форматі, де отримувачі вибирали всі відповіді, які вони вважали правильними.

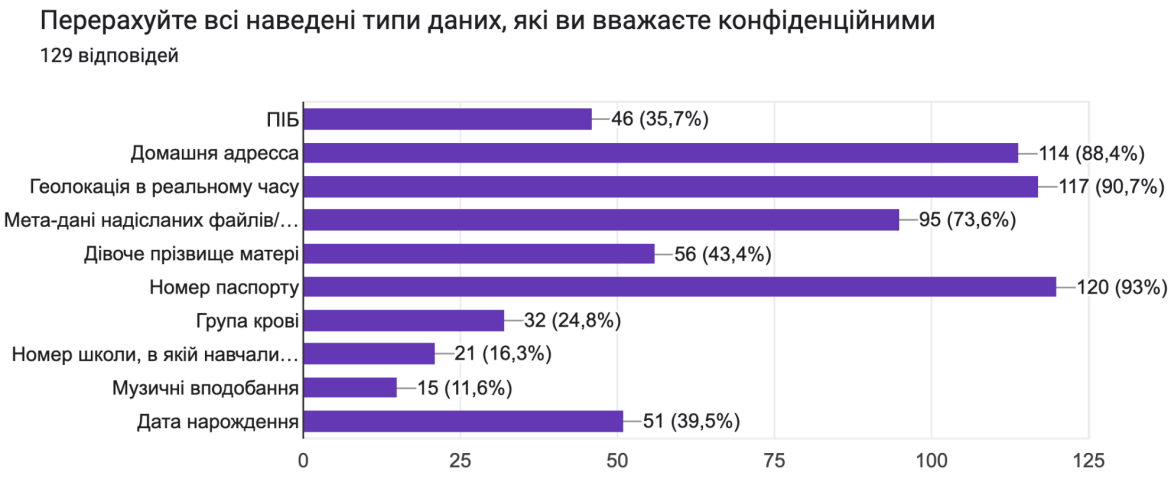
Серед 10 категорій даних одержувачі мали вибрати лише ті відповіді, які відповідають їхнім переконанням щодо персональних даних.

Щоб отримати більш повну картину, ми розглянули ще чотири імітації особистої інформації: дівоче прізвище матері, номер школи, де вона навчалася перші чотири роки, музичні уподобання та групу крові.

Тому відповіді учасників опитування всебічно відображають їхнє розуміння того, що таке конфіденційні дані.

У випадку дослідження конфіденційні дані — це категорія, яка відповідає визначенню: особисті дані або набори даних.

Як можна побачити з Діаграми 2.4 більшість користувачів обрали варіанти відповіді “Домашня адреса”(84,4%), “Геолокація в реальному часі”(90,7%), “Метадані надісланих файлів/фото” (73,6%), “Номер паспорту” (93%) як важливі конфіденційні дані. Варто звернути увагу, що тільки 39,5% користувачів обрали “Дату народження” як конфіденційні дані.



Діаграма 2.4 Типи даних, які користувачі вважають конфіденційними

Також для вибору були доступні і інші варіанти відповідей, що не є категоріями конфіденційних даних. Категорію “Дівоче прізвище матері” визначили як конфіденційні дані 43,4%; Варіант відповіді “Група крові” обрали 24,8%; Опцію “Номер школи, в якій навчалися перші 4 роки” було обрано 16,3%; На варіант вибору припало “Музичні вподобання” 11,6% користувачів. З цих даних ми розуміємо, що опитані реципієнти мають розуміння власних конфіденційних даних на рівні вище середнього.

На питання “Чи читаєте ви документи на сторонці при реєстрації про збір та обробку ваших персональних даних?” реципієнти дали відповіді у таких співвідношеннях: відповідь “так” отримала всього 39,5%; варіант “ні” обрали 44,2% реципієнтів; опцію “важко відповісти” обрали ще 16,3%. Ці результати свідчать про те, що значна частина користувачів соціальних мереж не приділяє належної уваги документам, які регламентують політику конфіденційності та збирання даних. Це може призвести до необізнаності щодо того, як їхні дані використовуються та обробляються.

Графічне відображення відповідей зображено на Діаграмі 2.5. З діаграми видно, що майже половина опитаних не читає документи про збір та обробку персональних даних, що є потенційно небезпечною практикою. Важливим є те, що 16,3% реципієнтів вагаються з відповіддю, що може свідчити про їхню непевність або недостатнє розуміння важливості цих документів.

Також, звернення уваги на ці питання під час реєстрації може допомогти користувачам краще розуміти свої права та обов'язки, а також бути обачнішими в розкритті своїх особистих даних. Однак, результати опитування показують, що більшість користувачів або не читають, або не впевнені у своїх відповідях щодо політики конфіденційності, що підкреслює необхідність підвищення обізнаності та освіти з питань кібербезпеки та конфіденційності.

Діаграма 2.5 Досвід користувачів в ознайомленні з документами про збір даних сервісами

На питання “Чи читаєте ви документи на сторінці при реєстрації про збір та обробку ваших персональних даних?” реципієнти дали відповіді у таких співвідношеннях: відповідь “так” отримала всього 39,5%; варіант “ні” обрали 44,2% реципієнтів; опцію “важко відповісти” обрали ще 16,3%. Графічне відображення відповідей зображено на Діаграмі 2.5. Ці результати свідчать про те, що значна частина користувачів соціальних мереж не приділяє належної уваги документам, які регламентують політику конфіденційності та збирання даних. Це може призвести до необізнаності щодо того, як їхні дані використовуються та обробляються.

Тож з огляду на отримані відповіді, можемо зробити висновок, що більшість реципієнтів не звертають уваги на документи, що надають сервіси, про обробку, збереження та передачу їхніх даних третім особам, третім країнам і т.д. Тобто користувачі перед або під час реєстрації не цікавляться, які дії може вчиняти сервіс з їхнім даними. Це свідчить про те, що користувачі довіряють сервісам без достатнього розуміння потенційних ризиків, пов'язаних з обробкою їхніх особистих даних. Така поведінка може мати серйозні наслідки, оскільки відсутність усвідомлення про те, як

їхні дані можуть використовуватися або передаватися, може призвести до небажаного розкриття особистої інформації або навіть до її зловживання.

Питання “Чи використовуєте ви різні паролі для кожного аканту?” та “Чи використовуєте ви пов'язані паролі для своїх акаунтів в соціальних мережах?

Наприклад, qwerty5678 та 5678qwerty” мають різне формулювання, але носять один характер та описують для нас один і той самий вектор вивчення цього питання. Такий вибір розбивання питання націлений на отримання більш правдивої відповіді від реципієнтів, щоб краще проаналізувати їх.

Тож на запитання “Чи використовуєте ви різні паролі для кожного аканту?” ми отримавли такі відповіді: “так” – 65,1%; “ні” – 27,1%; “частково” – 7,8%;

На запитання Чи використовуєте ви пов'язані паролі для своїх акаунтів в соціальних мережах?

Наприклад, qwerty5678 та 5678qwerty” реципієнти дали такі відповіді: “так” – 18%; “ні” – 37,5%; “частково” – 42,2%; “важко відповісти” –2,3%.

Графічне співвідношення відповідей до кількості реципієнтів відображені на Діаграмі 2.6 та Діаграмі 2.7.

Діаграма 2.6 Досвід користувачів щодо різноманітностей паролів для різних сервісів

Діаграма 2.7 Досвід користувачів у створені або зміні паролів

З огляду на відповіді реципієнтів, ми можемо зробити висновок, що більшість користувачів відповідально ставляться до своїх даних, цілісності та захищеності персонального листування та особистого життя. Це свідчить про те, що користувачі соціальних мереж усвідомлюють важливість захисту своїх особистих даних і прагнуть забезпечити безпеку своєї інформації в онлайн-середовищі. Вони розуміють, що їхні дані можуть бути вразливими до атак та зловживань, і вживають заходів для мінімізації цих ризиків.

Користувачі, які усвідомлюють необхідність захисту своєї особистої інформації, частіше читають документи про політику конфіденційності та налаштовують свої акаунти відповідно до рекомендацій щодо безпеки. Вони також можуть використовувати складніші паролі та уникати поширення особистих даних у публічному доступі. Це свідчить про зростаючу цифрову грамотність та відповідальність серед користувачів соціальних мереж.

Однак, існує також значна частка користувачів, які не приділяють належної уваги захисту своїх даних. Вони можуть не читати політику

конфіденційності, використовувати прості або однакові паролі для різних акаунтів, а також публікувати особисту інформацію без належного обдумування. Це може призвести до підвищеного ризику витоку даних та їх зловживання з боку третіх осіб.

Зрозуміло, що необхідно продовжувати освітню роботу серед користувачів щодо важливості захисту особистих даних і ризиків, пов'язаних із їх недбалим поводженням. Такий підхід допоможе підвищити рівень обізнаності та відповідальності серед користувачів, що в свою чергу сприятиме загальному підвищенню безпеки в онлайн-середовищі.

Наступний блок з 4 питань формує розуміння як юзери ставляться до поширення власних конфіденційних даних, а саме чи готові юзери самі розкривати чутливі дані, як часто вони це роблять та побачити чи наявне розуміння способів поширення власних чутливих даних.

Питання “Чи публікуєте ви фотографії з відпустки з геолокацією в реальному часі?” отримало таке співвідношення відповідей: “так” – 24,2%; “ні” – 58,6%; “Публікую без геолокації” – 17,2% (Діаграма 2.8).

Діаграма 2.8 Ставлення користувачів до публікації фото з геолокацією під час відпустки

Питання “Чи публікуєте ви в соціальних мережах своє місцезнаходження в реальному часі? Наприклад, Stories з відміткою

закладу, де ви наразі знаходитеся" реципієнти дали такі відповіді: "так" – 14,7%; "ні" – 55,8%; "час від часу" – 27,1%; "важко відповісти" – 2,3%.(Діаграма 2.9)

Діаграм 2.9 Ставлення користувачів до публікації контенту з відмітками геолокації у повсякденному житті

Запитання "Чи публікуєте ви в соціальні мережі матеріальні підтвердження своїх досягнень? Наприклад, дипломів, лотерей, квитків і т.д." реципієнти дали такі відповіді: "так" – 10,9%; "ні" – 68,2%; "важко відповісти" – 20,9% (Діаграма 2.10).

Діаграма 2.11 Ставлення користувачів до поширення своїх даних через публікацію своїх досягнень

На питання “Чи вказуєте ви свої реальні дані (ім'я, прізвище, місто проживання) в профілі або при реєстрації?” реципієнти дали наступні відпвіді: “так” – 10,9%; “ні” – 68,2%; “час від часу” – 20,9%(Діаграма 2.12).

Діаграма 2.12 Ставлення користувачів до поширення свого ім’я у соціальних мережах

На основі отриманих відповідей можемо зробити наступні висновки. Перш за все, більшість користувачів проявляють обережність при публікації інформації, що може розкрити їх місцезнаходження в реальному часі. Зокрема, 58,6% реципієнтів зазначили, що не публікують фотографії з геолокацією під час відпустки, і 55,8% уникають публікації свого місцезнаходження у реальному часі в соціальних мережах. Це свідчить про те, що користувачі усвідомлюють ризики, пов’язані з розкриттям свого місцезнаходження, та намагаються захистити свою приватність.

Далі, лише 10,9% респондентів готові публікувати матеріальні підтвердження своїх досягнень, таких як дипломи або квитки, у соціальних мережах, тоді як 68,2% цього не роблять. Це може свідчити про побоювання щодо потенційного зловживання їхніми особистими даними. Крім того, значна частина користувачів (68,2%) уникає вказувати свої

реальні дані (ім'я, прізвище, місто проживання) у профілях або при реєстрації, що знову ж таки підкреслює їх прагнення до конфіденційності.

З іншого боку, інші питання показують дещо інші тенденції. Наприклад, більшість реципієнтів (66,7%) все ж вказують свої реальні дані при реєстрації, що може свідчити про відсутність у них побоювань щодо розголошення такої інформації або ж про вимоги сервісів, які вони використовують.

Отже, загальний висновок полягає в тому, що хоча багато користувачів соціальних мереж усвідомлюють ризики і прагнуть захистити свою приватність, існує значна частина, яка не приділяє достатньої уваги безпеці своїх особистих даних. Це може бути пов’язано як з недостатнім рівнем обізнаності, так і з певними обмеженнями та вимогами самих соціальних мереж. Важливо продовжувати роботу з підвищення рівня цифрової грамотності серед користувачів, щоб забезпечити більш ефективний захист їхньої приватності та безпеки в онлайн-середовищі.

Висновки до розділу 2

У розділі 2 було детально описано процес дослідження, методи його проведення та презентацію інтерпретованих даних, отриманих у ході дослідження. Цей розділ є ключовим, оскільки дозволяє зрозуміти, як саме було організовано дослідження, які підходи використовувалися та які результати були отримані.

У підрозділі 2.1 ми детально описали методологію нашого дослідження. Було розглянуто вибірку, на якій базувалося дослідження, а також обґрунтовано вибір методів збирання даних. Важливим аспектом цього підрозділу є опис інструментів, що використовувалися для збору інформації, таких як анкети, опитувальники та інтерв'ю. Також було ретельно обґрунтовано питання, які були включені до опитування, пояснено їх значущість та очікувані результати.

Підрозділ 2.2 присвячено презентації результатів дослідження. Тут ми розкрили інтерпретацію отриманих даних та представили їх у зручній для розуміння формі. Було використано графічні відображення, такі як діаграми, графіки та таблиці, що дозволяють наочно продемонструвати основні висновки та тенденції, виявлені в ході дослідження. Ці візуальні матеріали допомагають краще зрозуміти структуру та взаємозв'язки між різними аспектами досліджуваної теми.

Наприклад, було створено кілька діаграм, які ілюструють розподіл відповідей респондентів на ключові питання анкети. Це дозволило виявити основні тенденції та патерни у відповідях, що, у свою чергу, допомогло глибше зрозуміти поведінку та ставлення користувачів до питань конфіденційності та безпеки даних у соціальних мережах та месенджерах. Також було проведено порівняння між різними групами респондентів, що дозволило виявити відмінності у ставленні до конфіденційності залежно від віку, статі, рівня освіти та інших соціально-демографічних характеристик.

Цей розділ завершується загальним аналізом отриманих даних та висновками, що роблять можливим подальше обговорення та формування рекомендацій. Підсумовуючи результати дослідження, ми змогли визначити ключові проблеми та виклики, пов'язані з конфіденційністю та безпекою даних, а також запропонувати можливі шляхи їх вирішення. Ці висновки створюють основу для наступних розділів, де розглядатимуться практичні аспекти впровадження політик конфіденційності та рекомендації для користувачів і розробників додатків.

Таким чином, розділ 2 забезпечує всебічне розуміння проведеного дослідження та його результатів, створюючи міцну базу для подальшого аналізу та обговорення.

Висновки

Проведене дослідження дозволило отримати цінну інформацію про ставлення користувачів до конфіденційних даних та їх поведінку у соціальних мережах. На основі отриманих результатів можна зробити висновок, що більшість реципієнтів демонструють певний рівень обізнаності про важливість конфіденційних даних.

Наприклад, значна частина користувачів уникає публікації свого місцезнаходження в реальному часі та не публікує матеріальні підтвердження своїх досягнень, що свідчить про їхню обережність. Однак, водночас, значна частина респондентів все ж таки вказує свої реальні дані при реєстрації в соціальних мережах, що може свідчити про недостатню обізнаність щодо ризиків, пов’язаних з розголошенням цієї інформації.

Результати показують, що рівень розуміння реципієнтів щодо конфіденційних даних є неоднорідним. Хоча користувачі усвідомлюють ризики, пов’язані з публікацією особистої інформації у соціальних мережах, багато з них все ще не приділяють достатньої уваги налаштуванням приватності своїх акаунтів. Наприклад, лише 39,5% респондентів читають документи про збір та обробку персональних даних перед реєстрацією.

Дослідження показало, що реципієнти не завжди вважають себе відповідальними за поширення своїх чутливих даних у соціальних мережах. Це можна побачити з того, що значна частина користувачів вказує свої реальні дані при реєстрації, не приділяючи достатньої уваги налаштуванням приватності.

З іншого боку, багато користувачів намагаються обмежити доступ до своїх геолокаційних даних, що свідчить про певну усвідомленість ризиків. Чи мають юзери коректне розуміння, які саме дані є конфіденційними та

вартими захисту? Частково. Хоча користувачі виявляють певну обізнаність щодо конфіденційності даних, багато з них все ще не усвідомлюють повною мірою, які саме дані потребують захисту та які ризики можуть виникнути через їх розголошення. Це видно з того, що значна частина респондентів не читає документи про обробку персональних даних та вказує свої реальні дані при реєстрації.

Розуміння реципієнтів щодо конфіденційних даних знаходиться на середньому рівні. Вони усвідомлюють необхідність захисту певної інформації, наприклад, геолокаційних даних, але не завжди розуміють важливість захисту інших типів даних, таких як ім'я, прізвище, або місто проживання. Не завжди. Хоча користувачі розуміють, що вони самі повинні контролювати поширення своїх даних, багато з них не вважають це своєю основною відповідальністю. Це видно з того, що значна частина респондентів не налаштовує належним чином параметри конфіденційності своїх акаунтів та не читає умови використання сервісів перед реєстрацією.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Іванов В. Основні теорії масової комунікації: навч.посіб. Київ: Центр Вільної Преси, 2010. 260 с.
2. Twitter now acts more like a messaging app with read receipts, typing indicators & web link previews / Інтернет-джерело TechCrunch URL:https://techcrunch.com/2016/09/08/twitter-now-acts-more-like-a-messaging-app-with-read-receipts-typing- indicators-web-link-previews/
3. Most popular global mobile messenger apps as of January 2023, based on number of monthly active users/ Інтернет-джерело Statista URL: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/
4. Messenger Wars: How Facebook lost its lead/ Інтернет-джерело On Device Resaerch URL: https://ondeviceresearch.com/blog/messenger-wars-how-facebook-lost-its-lead
5. Дойч К. Народи, нації та комунікація / Карл Дойч // Націоналізм : антологія / [упорядн. О. Проценко, В. Лісовий]. К. : Смолоскип, 2000. 872 с.
6. Федонюк С. В. та ін/ За ред. С. В. Федонюка, В. Й. Лажніка. Європейська інтеграція : навч. посіб. для студ. вищ. навч. закл. Луцьк : Волин. нац. ун-т ім. Лесі Українки, 2010. 760 с.
7. Макаренко Є.А., Ожеван М.А., Рижков М.М. та ін. Європейські комунікації: монографія. / К.: Центр вільної преси, 2006. 536 с.
8. Шинкарук А.Л., Парфенюк В.М., Кац Е.Я. Європейські публічні комунікації: культура, політика, технології: колективна монографія / Рівне, 2013. 416 с.
9. Королько В.Г. Некрасова О.В. Зв’язки з громадськістю. Наукові основи, методика, практика. Наукові основи, методика, практика: Підручник для студентів вищих навчальних закладів/ 3-е вид. Доп. І

перероблене К.: Вид. дім «Києво-Могилянська академія», 2009. 831 с.

10. Макаренко Є. А., Рижков М. М., Ожеван М. А. та ін. Інноваційна дипломатія XXI століття: колективна монографія / К.: Центр вільної преси, 2012. 408 с.
11. Кавун С. В. Інформаційна безпека: навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. 352 с.
12. 15. Картунов О. Маруховський О. В. Інформаційне суспільство: аналіз політичних аспектів зарубіжних концепцій: монографія К.: Університет економіки та права «КРОК», 2012. 344 с.
13. Макаренко Є. А., Рижков М. М., Кучмій О. П., Фролова О. М. Міжнародна інформація: терміни і коментарі. Навч. посіб. / Вид. 2-ге, К.: Центр вільної преси, 2016. 518 с.
14. Угрин Л., за наук. ред. д-ра політ. н. Н.М. Хоми. Комунікаційна політика. навч. енцикл. словник довідник Львів : «Новий Світ-2000», 2014. С. 311-312.
15. Губерський Л. В. Українська дипломатична енциклопедія : у 2 Т. Київ: Знання України, 2004. Т. 2. 797 с.
16. Яшенкова О.В. Основи теорії мовної комунікації: навч. посіб. для самостійної роботи студента / О.В. Ященкова. Київ : Академія, 2011. 304 с.
17. Barnes, S. B. A privacy paradox: Social networking in the United States. First Monday, 11(9). URL: https://doi.org/10.5210/fm.v11i9.1394
18. Abhishek Kumar, Subham Kumar Gupta, Animesh Kumar Rai, Sapna Sinha . Social Networking Sites and Their Security Issues. URL: https://www.ijsrp.org/research-paper-0413/ijsrp-p1666.pdf
19. Київський міжнародний інститут соціології на замовлення ГО «Детектор Медіа» . Джерела інформації, медіаграмотність і російська пропаганда: результати всеукраїнського опитування громадської

думки. URL: https://detector.media/infospace/article/164308/2019-03-21-dzherela-informatsii-mediagramotnist-i-rosiyska-propaganda-rezultaty-vseukrainskogo-opytuvannya-gromadskoi-dumky/

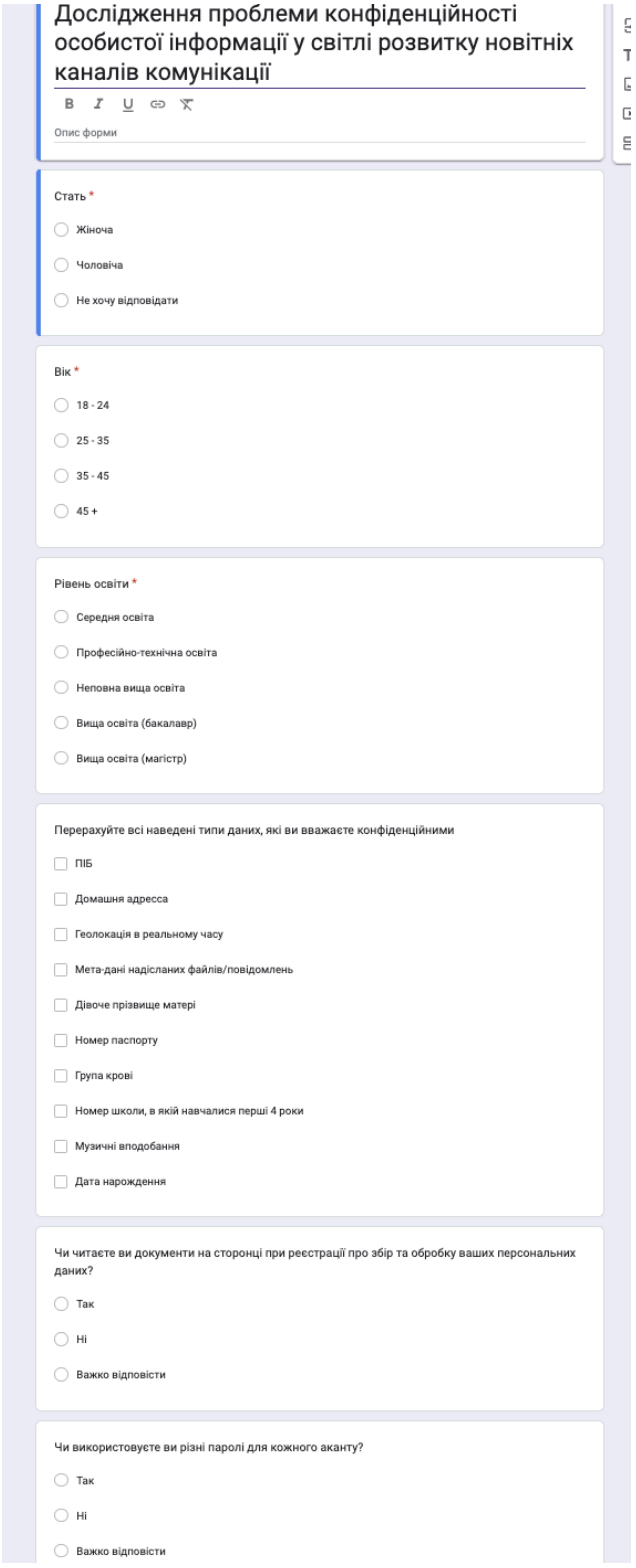
20. Дóренський О.П. Сучасні інформаційні технології та програмне забезпечення комп'ютерних систем. Збірник тез доповідей Всеукраїнської науково-практичної конференції студентів та магістрантів – Кіровоград: «КОД», 2016. 105 с.
21. Інтернет-джерело "Українське право". URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_berkiy_Social_networks_and_there_involves/
22. Інтернет-джерело "УНІАН". URL: https://www.unian.ua/economics/telecom/10445769-ukrajinska-auditoriya-facebook-za-rik-zrosla-na-3-milyoni-osib-infografika.html
23. Інтернет-джерело. PlusOne. Facebook в Україні. URL: https://plusone.com.ua/fb/
24. John Carlo Bertot, Paul T. Jaeger, Derek Hansen . The impact of policies on government social media usage: Issues, challenges, and recommendations URL: https://www.sciencedirect.com/science/article/pii/S0740624X11000992
25. Shaukat Ali, Naveed Islam, Azhar Rauf, Ikram Ud Din, Mohsen Guizani, Joel J. P. C. Rodrigues(2018) Privacy and Security Issues in Online Social Networks URL: https://www.mdpi.com/1999-5903/10/12/114
26. Інтернет-джерело "Tepabit". URL: https://tebapit.com/%D0%B2%D1%96%D1%80%D1%83%D1%81%D0%B8-%D0%B7%D0%B0%D0%B2%D0%B0%D0%BD%D1%82%D0%B0%D0%B6%D1%83%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%B3%D0%BE-%D1%81%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%B0/

27. Інтернет-джерело “Now Secure” URL: https://www.nowsecure.com/resources/nowsecure-ms/cobyj0gpcak-20?x=9z-j5n&pflpid=10536
28. Julian Assange. When Google Met WikiLeaks. Нью Йорк: OR Books, 2014
29. Макух Н.Б., Чоп Т.О. Конфіденційністьу соціальних мережах. Матеріали X Міжнародної науково-практичної конференції молодих учених та студентів «Актуальні задачі сучасних технологій» Тернопіль: Тернопільський національний університет ім. І.Пулюя, 2021
30. Глянько О. С. Соціальні мережі – загроза конфіденційності. Інтернет-джерело “Spilnota.net.ua” URL: http://www.spilnota.net.ua/ru/article/id-3250/
31. Недашківський Г. В. Неможливість збереження конфіденційності у соціальних мережах. Державний університет «Житомирська політехніка»

Додатки

Додаток А

Анкета опитування реципієнтів для проведеного дослідження



Дослідження проблеми конфіденційності особистої інформації у світлі розвитку новітніх каналів комунікації

Опис форми

Стать *
- Жіноча
- Чоловіча
- Не хочу відповідати

Вік *
- 18 - 24
- 25 - 35
- 35 - 45
- 45 +

Рівень освіти *
- Середня освіта
- Професійно-технічна освіта
- Неповна вища освіта
- Вища освіта (бакалавр)
- Вища освіта (магістр)

Перерахуйте всі наведені типи даних, які ви вважаєте конфіденційними
- ПІБ
- Домашня адресса
- Геолокація в реальному часу
- Мета-дані надісланих файлів/повідомлень
- Дівоче прізвище матері
- Номер паспорту
- Група крові
- Номер школи, в якій навчалися перші 4 роки
- Музичні вподобання
- Дата нарождення

Чи читаєте ви документи на сторонці при реєстрації про збір та обробку ваших персональних даних?
- Так
- Ні
- Важко відповісти

Чи використовуєте ви різні паролі для кожного аканту?
- Так
- Ні
- Важко відповісти