Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«14» червня 2022р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
бакалавра
(назва освітнього ступеня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Метод визначення захищеності персональних даних від довіри в соціальних мережах»

Виконавець: студент IV курсу, групи КБ-42

_____ **Максим ТЕРЕМОК**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Олександр ЛАПТЄВ	

Нормоконтроль	Олександр ТОРОШАНКО	

Київ 2022

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентові **КБ-42** **Теремку Максиму Вячеславовичу**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи «Метод визначення захищеності персональних даних від довіри в соціальних мережах»

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Соціальні мережі, персональні дані, вплив на людину та розвиток, існуючі загрози, довіра, параметри інформаційної захищеності системи

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Поняття соціальної мережі, характеристики та вплив мереж, тенденції розвитку, персональні дані, традиційні загрози, фальшиві профілі, деанонімізація, метадані, профайлінг, поняття довіри, залежність захищеності даних від довіри, рекомендації, сфери використання.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Опис методу визначення захищеності персональних даних від довіри в соціальних мережах та формування рекомендацій вдосконалення

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Олександр ЛАПТЄВ (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Максим ТЕРЕМОК (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021 – 27.01.2022	*виконано*
2	Аналіз літератури	28.01.2021 – 11.02.2022	*виконано*
3	Обґрунтування вибору рішення	12.02.2021 – 24.02.2022	*виконано*
4	Збір даних	25.02.2021 – 24.03.2022	*виконано*
5	Написання першого розділу роботи	25.03.2021 – 07.04.2022	*виконано*
6	Написання другого розділу роботи	08.04.2021 – 20.04.2022	*виконано*
7	Написання третього розділу роботи	21.04.2021 – 05.05.2022	*виконано*
8	Підготовка ілюстративного матеріалу	06.05.2021 – 20.05.2022	*виконано*
9	Отримання рецензій	21.05.2021 – 01.06.2022	*виконано*
10	Оформлення пояснювальної записки	02.06.2021 – 06.06.2022	*виконано*
11	Підготовка до захисту	07.06.2021 – 13.06.2022	*виконано*

Завдання видав _____ (підпис) Олександр ЛАПТЄВ (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Максим ТЕРЕМОК (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, має 53 сторінки основного тексту, 10 рисунків, 1 таблицю та 10 формул. Список використаних джерел містить 40 найменувань і займає 4 сторінки.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;

Об'єктом дослідження є вплив параметрів довіри на стан захищеності інформації в соціальних мережах.

Предметом дослідження є метод визначення захищеності персональних даних під час взаємодії між користувачами в соціальних мережах.

Практичною цінністю отриманих результатів є опис методу визначення захищеності персональних даних від довіри в соціальних мережах та формування рекомендацій щодо удосконалення.

Ключові слова: соціальна мережа, захист персональних даних, вразливості, довіра, загрози інформацій безпеці.

ЗМІСТ

ВСТУП

Актуальність. В сучасному світі важко знайти людину, яка б не знала або не користувалась тією чи іншою соціальною мережею. Завдяки швидкому розвитку технологій популярність онлайн соціальних мереж за останнє десятиліття різко зросла. Інформація в соціальних мережах за допомогою Інтернету розповсюджується майже миттєво, що в свою чергу приваблює тих, хто захоче скористатися цією інформацією в своїх цілях.

Важливість захисту персональних даних значно зростає зі збільшенням популярності та розповсюдженням соціальних мереж. Зараз зловмисники користуються різноманітними атаками на систему та на людину, для того щоб досягти мети у порушенні конфіденційності, цілісності, доступності інформації. Для того, щоб побудувати досконалу систему захисту інформації важливо правильно оцінити загрозу, проаналізувати методи протидії або недопущення загрози, та створити механізм мінімізації наслідків вдалої атаки за сторони зловмисника. Практична потреба визначення захищеності персональних даних від довіри в соціальних мережах полягає в тому, щоб визначити стан захищеності інформаційної системи та персональних даних в ній, для швидкого реагування на потенційні загрози.

Тому **метою роботи** є розробка методу оцінки залежності захисту персональних даних від довіри в соціальних мережах.

Для досягнення зазначеної мети необхідно вирішити такі *завдання*:

- провести аналіз тенденцій розвитку соціальних мереж;
- провести аналіз існуючих загроз персональним даним в соціальних мережах;
- дослідити залежність захисту персональних даних від довіри в соціальних мережах.

Об'єктом дослідження в даній роботі є вплив параметрів довіри на стан захищеності інформації в соціальних мережах.

Предметом дослідження в даній роботі є метод визначення захищеності персональних даних під час взаємодії між користувачами в соціальних мережах.

Методи дослідження дипломної роботи:

- аналіз літератури;
- аналіз документів;
- порівняння;
- вивчення та узагальнення вітчизняної і зарубіжної практики.

РОЗДІЛ 1
АНАЛІЗ ТЕНДЕНЦІЙ РОЗВИТКУ СОЦІАЛЬНИХ МЕРЕЖ

1.1 Походження поняття «соціальна мережа»

Інформаційно-комунікаційні мережі, завдяки своїм можливостям ефективного прийому, обробки, збереження, відтворення та передачі інформації, відіграють величезне значення в структурі сучасного суспільства. Загальне визначення «соціальна мережа» в наш час встановилось та широко використовується як інтернет-термін. Однак поняття соціальних мереж є більш широким і стосується не тільки сфери інформаційних технологій.

Першими прикладами мережевих комунікацій вважається родове суспільство з племінною системою збереження та передачі інформації. В таких умовах взаємодія могла відбуватися через вербальні (міміка, жести, сигнали) і невербальні, тобто мовні форми комунікації. Наступний етап розвитку мережевих систем комунікацій став можливий завдяки створенню нових та вдосконаленню існуючих технологій та промисловості. З розвитком друкарства засобом передачі інформації стали книги, потім з’явилось радіо, телебачення, телефонія і врешті інтернет. Зі збільшенням попиту та доступності новітніх засобів передачі даних з’явилась можливість поширення мережевих комунікацій, дозволивши людям залишатися «на зв’язку» між собою.

Психолог і соціолог Якоб Морено в 30-тих роках 20 століття проводив дослідження, які заклали основи в аналізі міжособових відносин в групі. Він використовував «соціаграму візуалізації соціальної мережі», де точками в двухмірному просторі позначались окремі люди, а ребра які їх з’єднують – відносини між ними [1]. Перше наукове пояснення терміну «соціальна мережа» з’явилось в 1954 році, і належить соціологу та соціальному антропологу Джеймсу Барнсу [2]. Він описував його як соціальну структуру, яка може складатись із груп об’єктів соціальної комунікації (людей та організацій) та зв’язків між ними. За результатами соціалогічних досліджень, Барнс розділив соціальні взаємовідносини

на такі як: «відносно стабільні формальні організації», «нестабільні спільноти» та «міжособові зв'язки» які формують соціальну мережу. Таким чином, термін визначав моделі зв'язків як близьких між собою груп, так і груп, об'єднуючих людей по різним диференційованим категоріям (національність, стать, хобі і тд.)

З появою і подальшим розвитком глобальної мережі Інтернет, почала набувати все більшої відомості і наукова концепція Джеймса Бернса. Це стало одним з факторів розвитку соціальних мереж всередині глобальної павутини.

Завдяки інтернет-технологіям, найбільш відомим і розповсюдженим значенням поняття «соціальна мережа» стали соціально-мережеві технології або веб-сайти, створені в мережі Інтернет для побудови спільнот людей зі схожими інтересами, соціальної взаємодії. Традиційні інститути, на відміну від Інтернет-мереж, не можуть конкурувати в створенні таких різноманітних та широких спільнот.

Наразі, термін «соціальна мережа» в контексті Інтернет-ресурсу є доволі широким і може трактуватись різними способами. Так, наприклад Д. В. Богданов вважає, що соціальні Інтернет-мережі – це технологічні віртуальні мережі, які є засобом взаємодії між окремими категоріями користувачів завдяки електронним ресурсам з ціллю встановлення та підтримки контактів [3]. Схема стандартної організованої соціальної мережі, де суб'єкти комунікації зображено кружечками, а лініями їх взаємовідносини, представлено на рисунку 1.1:

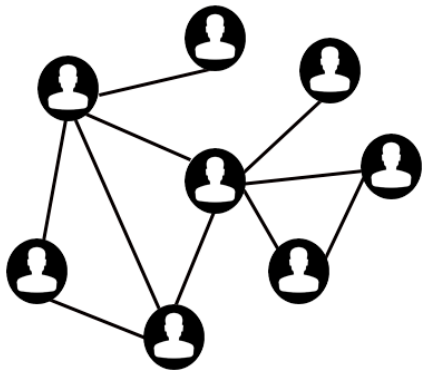


Рисунок 1.1 - Схема стандартної організованої соціальної мережі

А.С. Дужникова вказує, що соціальними мережами в Інтернеті називають інтерактивний багатокористувацький веб-сайт, контент якого наповнюють самі користувачі цього сайту. Сайт є автоматизованою соціальною платформою, яка дозволяє спілкуватись групі користувачів, об'єднаних загальними інтересами [4].

Інтернет соціальна мережа – це веб-сервіс, який дозволяє користувачам створювати публічний або напівпублічний профіль, формувати список інших користувачів, з якими вони підтримують зв'язок, а також переглядати та поширювати цей список іншим користувачам системи [5].

Підводячи підсумок з вищесказаного, соціальна мережа являє собою інтерактивний багатокористувацький веб-ресурс, який реалізує соціально-комунікаційну структуру, яка складається з суб'єктів (люди, спільноти, групи) та зв'язки між ними.

1.2 Загальні характеристики та вплив сучасних соціальних мереж

Інформація, яка циркулює в соціальних мережах, концентрується в облікових записах користувачів (аккаунтах), за допомогою яких суб'єкти взаємодіють між собою.

Характерними особливостями більшості соціальних мереж є:

- можливість створювати персональний профіль, в якому вказані персональні дані (ПІБ, дата народження, стать, хобі та інтереси);
- можливість створювати список контактів, з якими відбувається взаємодія (дружні, робочі, кровні зв'язки);
- надання користувачам можливості обміну повним спектром інформації (розміщення, зберігання, надсилання даних текстового, відео або аудіо форматів).

Сучасні технології копіюють і транспонують мережі соціальної комунікації, які вже існують в реальному житті, у віртуальний простір. Це дозволяє підвищити інтенсивність та щільність соціальних зв'язків.

Н. Христакис та Дж. Фаулер описують правила життя в соціальних мережах наступним чином [6]:

1. мережі на основі спілкування зі схожими на себе людьми формуються самими людьми;

2. мережі формують коло спілкування людей шляхом включення в нього нових учасників (друзі друзів);

3. люди знаходяться під впливом їх друзів через механізми копіювання їх поведінки;

4. на користувачів соціальної мережі впливають друзі друзів (до четвертого ступеню віддалення).

Зараз немає єдиної думки за якими критеріями варто проводити класифікацію соціальних мереж. Як правило, класифікація проводиться беручи за основу технологічний, цільовий, географічний принцип розділення. Загалом, соціальні мережі в Інтернеті можна розділити на декілька великих груп:

- індивідуально-персональні (блоги, веб-сторінки, спрямовані на міжособову взаємодію з конкретною людиною);
- масові (універсальні мережі, спрямовані на відкрите спілкування, пошук друзів, родичів, колег);
- тематичні (форуми, блоги з вузькою тематикою, спрямовані на обговорення конкретних тем);
- відео- та фотохостинги (розміщення користувачами контенту у фото, відео форматі з можливостю коментування та оцінки).

Вченими пропонуються й інші варіанти класифікації соціальних мереж. Наприклад, Е. Д. Патаракін виділяє дві категорії мереж (мережі, основою яких є профілі або сторінки учасників, та мережі, в яких найбільше значення мають цифрові об’єкти – статті, відео, музика, програми) [7]. В. Тоіскін та В. Красильников визначають класифікацію соціальних мереж за ступенем активності людини в мережі і характером комунікації між її учасниками [8].

В наш час популяризація соціальних мереж продовжує невпинно зростати. Згідно ресурсу Statista за 2021 рік число активних користувачів по всьому світу налічує більш ніж 3.8 мільярдів чоловік. До трійки найбільш відвідуваних соціальних мереж традиційно входять такі платформи як Facebook, YouTube та

WhatsApp. Кількість активних користувачів соціальних мереж станом на 2021 рік зображено на рисунку 1.2:

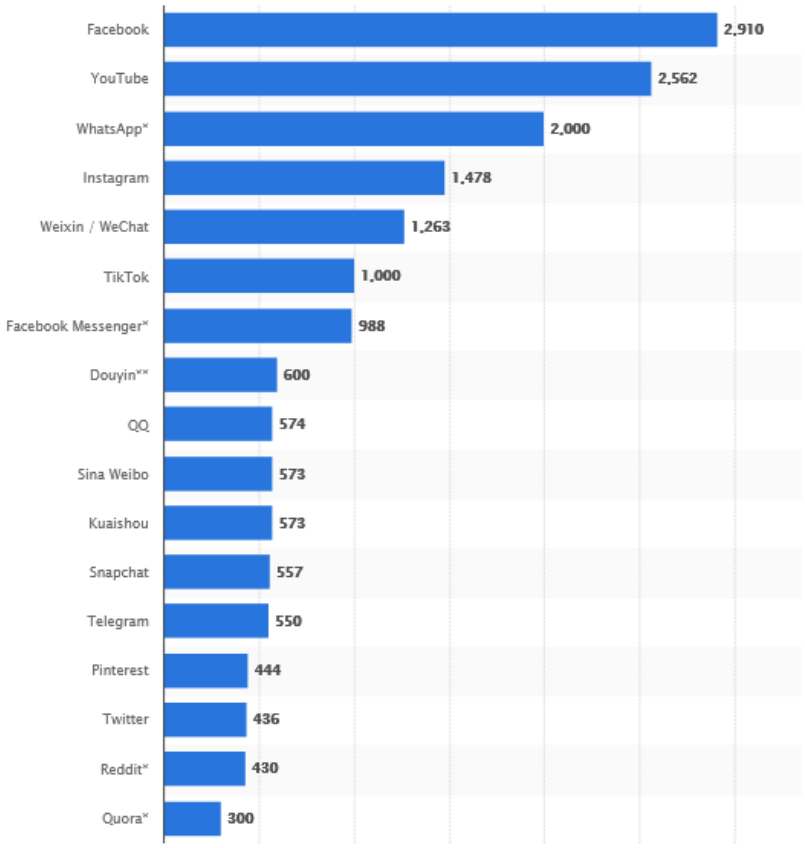


Рисунок 1.2 - Кількість активних користувачів соціальних мереж на 2021 р., млн [9]

Водночас зі стрімким збільшенням швидкості обміну інформаційними повідомленнями зростає і їх кількість, що в свою чергу впливає на характер комунікації між людьми. У кожного користувача соціальної мережі є можливість зберігати анонімність, створювати та поширювати контент під псевдонімами. Така практика зменшує відповідальність окремого індивіда за розповсюджені їм повідомлення. В результаті чого, люди перевантажуються контентом, і не встигаючи оцінити повідомлення не завжди можуть сформувати свою потребу на інформацію отриману з Інтернету. І, оскільки з кожного джерела зростає кількість трактувань деякого повідомлення, як позитивних так і негативних, то в цілому зменшується вірогідність критичного сприйняття та об’єктивної оцінки інформації [10].

Враховуючи це, вчені намагаються оцінити наслідки, які соціальні мережі можуть нести людині.

Дослідження Д. Хоффмана виявили зв'язок між ступенем залучення в онлайн-комунікації із задоволенням потреб людини [11]. Потреба в спілкуванні задовольняється як за рахунок взаємодії з іншими людьми, так і за рахунок контенту соціальної мережі. Також при використанні соціальних мереж, окрім спілкування та споживання контенту, люди часто створюють і свій контент. Таким чином, людина отримує відчуття досягнення цілі. Було виявлено, що при користуванні соціальними мережами приводить до задоволення таких соціальних потреб як приналежність до деякої групи, самовираження та самопрезентація. Крім того, ідентифікація себе приналежним до деякої онлайн-спільноти приводить до посилення соціальної та колективної ідентичності людини, що в свою чергу підвищує самооцінку.

Дж. Бергер вважає, що користування соціальними мережами має терапевтичний ефект [12]. Він виявив, що публікуючи чутливий для себе або особистий контент (думки, емоції, почуття), знаходячись в результаті емоційної нестабільності. Публікація таких речей допомагає виражати негативні емоціональні переживання, отримати соціальну підтримку від інших користувачів.

В дослідженні негативних наслідків користування соціальних мереж в яких приймав участь К. Уілкокс було виявлено, що це приводить до погіршення фінансового і психологічного стану [13]. Регулярне користування соціальними мережами може призвести до зниження контролю над фінансовими затратами і зниження самоконтролю. Ці негативні наслідки пояснюються активацією нарцисичного стану із завищеною самооцінкою. Підвищена самооцінка в деяких випадках може призвести не до позитивного соціального ефекту, а до нарцисизму, якому характерний надмірна самопрезентація та захисне самоствердження. Цікавим також виявилось те, що був визначений взаємозв'язок між «нарцисом» і користуванням соціальними мережами, оскільки користування мережами людьми з такими рисами лише сприяє розвитку нарцисизму.

Одним з досліджень негативних наслідків користування соціальними мережами є дослідження Університету Бата щодо фізичної залежності від

соціальних мереж та вплив на психоемоційний стан. Дослідження було направлене на те, щоб зрозуміти вплив 1-тижневої перерви від соціальних мереж (Facebook, Instagram, Twitter, TikTok) на самопочуття, депресію та тривогу. Випадковим чином було взято 154 людини і розділено на дві групи. Першій групі було запропоновано не користуватися соціальними мережами впродовж тижня, а іншій користуватися мережами без обмежень. Результати експерименту показали, що у піддослідних які відмовились від соціальних мереж на тиждень значно зменшилась депресія, самопочуття та тривожність. Майбутні дослідження мають оцінити розповсюдження цього та вивчити ефекти в довгостроковій перспективі [14].

1.3 Тенденції розвитку соціальних мереж

1.3.1 Інтеграція в сторонні сайти та програми

Інтеграція із зовнішніми сайтами та програмами є одним з важливих напрямків розвитку соціальних мереж. Оскільки соціальними мережами користуються мільйони людей по всьому світу, власники мереж отримують можливість прямого та непрямого впливу над величезними людськими масами. В більшості випадків, цей вплив направлений на збільшення трафіку соціальної мережі, що в свою чергу в поєднанні з комерційними інтересами мережі, принесе більший дохід.

Наразі велика кількість веб-сайтів вже інтегровані із соціальними мережами тим чи іншим чином, а також все більше сайтів закладають інтегрування ще на етапі проектування та створення веб-сайту.

Найрозповсюдженим прикладом такої інтеграції є кнопка «мені подобається» та «поширити», які можна зустріти на більшості сучасних веб-сайтів. Дана функція дозволяє користувачеві користуватись функціями соціальними мережі поза її меж. Ще одним прикладом є використання власниками сайтів плеєру відеохостинга Youtube на своїх ресурсах. Це можна спостерігати на веб-сайтах пов’язаних з поширенням відео- та аудіо контенту (сайти новин, блоги, форуми).

Практика інтегрування соціальних мереж в цілому є позитивною для користувачів, оскільки підвищує зручність користування веб-сайтом. Прикладом є інструмент входу на сайт використовуючи профіль соціальної мережі. За результатами досліджень ресурсу LoginRadius виявилось, що 73% користувачів надають перевагу входу через соціальну мережу [15], стандартна форма для входу зображена на рисунку 1.3:

Рисунок 1.3 - Стандарта форма входу через соціальні мережі

Даний інструмент входу є вигідним і для власника веб-сайту. Увійти через одну із соціальних мереж для користувача є легшим ніж створити новий аккаунт, вводити свою електронну пошту та вигадувати новий пароль. Це може відлякувати частину нових користувачів, що призведе по покидання сайту.

Веб-сайти активно додають нові можливості інтеграції з соціальними мережами, оскільки це приваблює та утримує відвідувачів Інтернету, що допомагає отримати додаткові прибутки. Таким чином, соціальні мережі «підсаджують» сайти на інтеграцію.

Інтеграція даних із різних мереж, переміщення інформації на різних сайтах і ідентифікація всього контенту є складною задачею, яка потребує стандартів і технологій які підтримують постачальники соціальних мереж. В багатьох сайтах

використовуються інтерфейси прикладних програм, а деякі соціальні мережі створили спеціальні функції, які дозволяють імпортувати і експортувати інформацію. Постійно збільшується кількість відкритих протоколів, які використовують постачальники [16]:

- Аутентифікація: OpenID, i-card, Facebook Connect;
- Авторизація: Open Authentication (Oauth), i-card, OpenSocial;
- Семантична розмітка та опис: Resource Description Framework (RDF), MicroFormats;
- Опис мережі: FOAF, XHTML Friends Network (XFN), OpenSocial;
- Візуалізація мережі: TouchGraph, Web Positioning System (WPS);
- Віддалене керування даними: Representational State Transfer (REST), SOAP (Simple Object Access Protocol, XML-RPC, DiSo;
- Транспортування повідомлень: EST, SOAP, Extensible Messaging and Presence Protocol (XMPP), and Simple Mail Transfer Protocol (SMTP);
- Індексація та пошук: Google Social Graph.

Окрім веб-сайтів активно соціалізуються і інтегруються з соціальними мережами і настільні застосунки. В першу чергу йдеться про програми пов’язані з обміном даних, але поступово прогнозується інтеграція елементів соціальних мереж і в інші програми. Програми, які відмовляться від «соціалізації» поступово будуть витискатися конкурентами і займати більш вузьку нішу.

1.3.2 Торгівля в соціальних мережах

Торгівля в соціальних мережах є одним з головних і швидкозростаючих трендів. Всі найбільші онлайн соціальні мережі розвивають свою бізнес стратегію, переміщуючи торгівлю на перший план. Основна ідея полягає в тому, що соціальна мережа має переконати користувача знайти потрібний йому товар, оцінити товар по фото або відео і швидко купити його.

Дана тенденція стрімко почала зростати приблизно з 2019 року. Цей період співпав з глобальною світовою пандемією. В багатьох країнах світу почали впроваджувати карантин, в наслідок чого людям довелось переходити на

дистанційну форму роботи та сидіти вдома. В результаті цього, значно зросла кількість на тривалість відвідування соціальних мереж. Багато малих підприємців, справи або магазини яких зачинились через пандемію були змушені перейти до соціальних мереж і пропонувати свої послуги там.

Зараз більшість брендів, від глобальних корпорацій до сімейних підприємств використовують соціальні мережі для просування або прямого продажу своїх товарів та послуг. Загалом виділяють такі типи торговців в соціальних мережах: бренди (продають напряму кінцевому покупцю через платформу), лідери думок (рекламують або просувають свій товар або товар деякого бренду серед своїх підписників), фізичні особи (ведуть діяльність через свої мережі, знайомства та рекомендації).

Станом на 2021 рік об’єм торгівлі через соціальні мережі сягає близько 500 мільярдів доларів. Компанія Accenture провела дослідження, яке показало, що об’єм покупок в соціальних мережах зросте до 1,2 трильйонів доларів до 2025 року [17]. Більшу частину покупок буде здійснювати молоде та підростаюче покоління, на них буде прилягати більше 62 відсотків світових продажів. Діаграма зростання об’ємів торгівлі в соціальних мережах зображено на рисунку 1.4:

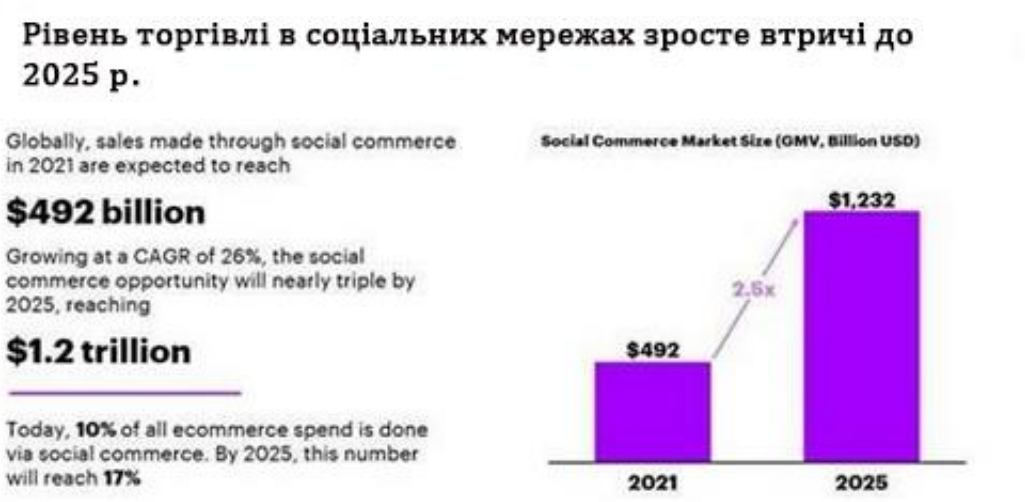


Рисунок 1.4 - Зростання об’ємів торгівлі в соціальних мережах [17]

Очікується, що найбільш популярними серед покупців в соціальних мережах буде одяг, електроніка, декор для будинку, їжа. Також очікується значне зростання об’ємів продажів засобів для гігієни та краси.

Враховуючи те, що соціальні мережі налічують більше 4 мільярдів активних користувачів, використання мереж в маркетингу є доволі ефективним і недорогим способом охопити величезну потенційну «клієнтську базу».

Перевагами такого підходу є те, що розміщуючи свої товари в мережі є можливість підвищити впізнаваність свого бренду. Функціонал соціальних мереж дозволяє підтримувати соціальні контакти з клієнтами, що в свою чергу підвищить довіру та сприйняття.

Сучасні соціальні мережі створюють зручний функціонал для торгівлі, що дозволяє підвищити ефективність та об’єми продажів. Прикладом є рекламні функції в соціальних мережах. За гроші вони надають можливість рекламувати, а також надають функції таргетування, що є одним з найголовніших факторів для бізнесу. Торговець, знаючи особливості свого товару, може налаштувати його рекламу обираючи вік, стать, країну або місто, в якому користувачі соціальної мережі будуть бачити дану рекламу.

Окрім вбудованих функцій рекламування існують так звані «лідери думок», які часто на своїх профілях в мережах мають велику кількість послідовників і користуються великою довірою. Зараз звичайною практикою є співпраця торговця і блогера, ціллю якої є реклама товару.

Одним з напрямків розвитку торгівлі в соціальних мережах є «вбудовані магазини». Його суть полягає в створенні готового функціоналу інтернет-магазину всередині соціальної мережі з усіма його перевагами (додавання в кошик, сортування, покупка всередині застосунку). Торгівцю або бренду залишається лише завантажити фото та опис товару, приклад магазину в мережі Instagram зображено на рисунку 1.5:

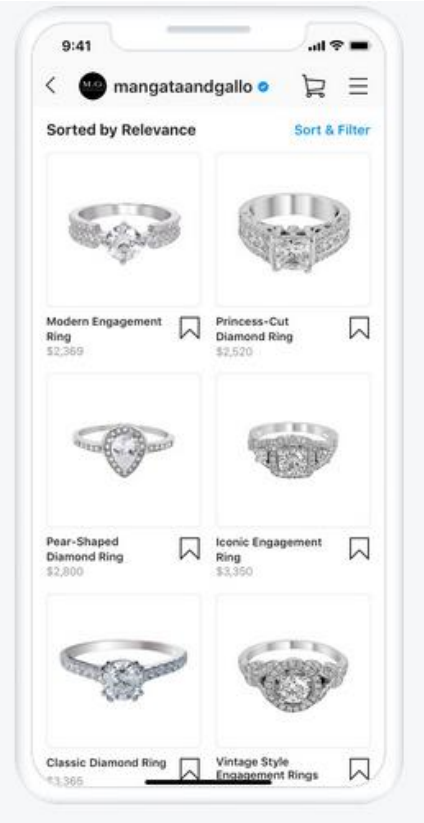


Рисунок 1.5 - Магазин всередині соціальної мережі Instagram [18]

Не менш важливим ніж функціонал продажу є функціонал звітності і аналітики. За допомогою інструментів відслідковування в соціальних мережах торговці можуть побачити і оцінити вплив дій спрямованих на підвищення продажів. Прикладом є Google Analytics, який може відслідковувати трафік соціальної мережі, рентабельність інвестицій та конверсії в соціальних мережах.

1.3.3 Віртуальні валюти

Перші віртуальні валюти з’явились в комп’ютерних іграх, але з розвитком інформаційних технологій потреба в них зростала, а горизонти використання розширювались. Віртуальні валюти вважаються першозасновниками цифрових грошей.

Одне з визначень «віртуальних валют» говорить, що це вид нерегульованих, цифрових грошей, які випускаються і контролюються їх розробниками, а також

приймаються членами деякої онлайн-спільноти. Віртуальні валюти в контексті соціальних мереж частіше за все використовувались в іграх. Оскільки монетизація являється важливою частиною багатьох ігор, соціальні мережі почали розповсюджувати свої віртуальні валюти. Вони використовувались в покупці ігрових речей, а також на покупку додаткового контенту соціальної мережі (розширені функції, преміум-статуси, тощо).

Так, компанія Facebook в 2011 році створила свою платіжну систему на основі віртуальних валют Facebook Credits. Вони зобов'язали всіх розробників ігор проводити платежі через дану систему, і всього було доступно 15 валют. Але вже 2012 році компанія відмовилась від цієї ідеї, а користувачі отримали можливість конвертувати валюту назад.

Іншою спробою створення віртуальної валюти всередині соціальної мережі є китайська компанія Tencent і її QQ Coins. Валюту можна було купити за допомогою кредитної карти, а обмінний курс був прив'язаний до юаня. На початку планувалось використання валюти лише для покупки продукції Tencent, але згодом дозволили і особисті (P2P) платежі. В результаті, валюта QQ Coins почала використовуватись для обміну юанів на чорному ринку, а китайська влада була вимушена її заборонити.

Ще одним прикладом невдалого запуску є мессенджер Telegram і його криптовалюта Ton. Проект був направлений на власної криптовалюти всередині месенджера для зручного замовлення і оплати послуг. Однак через суперечності в законодавстві США дана ідея не була втілена в життя.

В багатьох країнах світу віртуальні валюти, електронні гроші та криптовалюти досі не мають юридичного статусу, що і призводить до складностей розробці і впровадженні платіжних систем. Однак, через популяризацію в світі криптовалют, все більше країн починає серйозно звертати на них увагу. Так, в Тайланді для проводження операцій з Bitcoin необхідно отримати спеціальну ліцензію, в Японії за них стягується податок, в Німеччині прирівняли до звичайних платіжних операцій, а в Україні в 2022 році повністю легалізували як віртуальний актив [19]. Така тенденція на узаконення віртуальних грошей в різних країнах може значити

потенційний розвиток в імплементації операцій з віртуальними грошима в соціальні мережі.

1.3.4 Політичне застосування

Соціальні мережі є потужним інструментом в руках політиків. Згідно досліджень 2018 року, президенти, міністри, депутати багатьох країн мають профілі в соціальних мережах, а також активно використовують їх для комунікації зі своїм електоратом, громадянами та колегами з інших країн.

Таблиця 1.1

Кількість зареєстрованих політиків в соціальних мережах (2018 р.) [20]

Соціальна мережа	**Кількість аккаунтів**	**% країн**	**Розмір аудиторії млн.**
Twitter	856	92	356,9
Facebook	606	88	283,2
Instagram	330	73	53,6
Google+	261	66	11,9
YouTube	343	76	4,2

Політики часто використовують популярні засоби комунікації, якими зараз є соціальні мережі, для того щоб «бути в тренді». Також соціальні мережі є гарною платформою для просування своїх ідей і політичних позицій. Часто активізація по роботі з аудиторією в соціальних мережах йде перед виборами для завоювання якомога більшої кількості послідовників, в тому числі молодого покоління, яке є великою частиною всіх активних користувачів мереж.

Застосування комунікації в соціальних мережах «скорочує дистанцію» між політиком і звичайною людиною. Будь-який користувач має можливість звернутися до політика, «тегнувши» його у Facebook або написавши у приватні повідомлення. Така практика дозволяє ефективно комунікувати на низьких та середніх рівнях управління. Політики найвищих посад також починають активно користуватись

цим. Прикладом є президент України і його відео-звернення, що вже стало відомою «фішкою».

Соціальні мережі можуть бути використані як інструмент мобілізації народу у протестному русі. Прикладом є президентські вибори у Білорусі в 2020 році. Значна кількість громадян не погодилась з оголошеними результатами і вийшла на приотест. Більша частина всієї комунікації та координація протестного руху йшла через месенджер Telegram. Практика використання стала настілки масовою, що поліція перевіряла громадян на предмет встановлення месенджеру в телефоні, а лише один з опозиційних каналів встановлював рекорди з кількості підписників, на той час головний інформаційний білоруський Telegram-канал досягав більше 2,2 мільйонів користувачів.

Виділяють дві основні форми політичної активності в соціальних мережах: персональний профіль політика, аккаунт державної структири (ведеться прес-службою та помічниками). Twitter частіше за все використовується у другій формі, звичайною нормою стало налагодження контактів або «публічне спілкування» міністерств закордонних справ між собою.

Таким чином, можна прогнозувати подальше збільшення активності світових політиків в соціальних мережах. Як для зручнішої комунікації з громадянами та колегами, так і для власних політичних цілей.

1.3.5 Інноваційні шляхи розвитку

Сучасні соціальні мережі починають вкладати кошти в розробку новітніх технологій. Провідним напрямком сьогодні є розвиток доповненої реальності, штучного інтелекту та метавсесвітів.

Соціальні мережі оперують величезними даними про користувачів, їх зв’язки, інтереси, вподобання тощо. Вдосконалення штучного інтелекту дозволить набагато швидше і ефективніше обробляти такі дані і використовувати в рекламних цілях, а отже і збільшити прибутки.

Компанія Facebook в 2021 році на своїй конференції представила своє бачення майбутнього соціальних мереж, провела ребрендінг на Meta, а також запустила свій новий проект Metaverse (з англ. – «метавсесвіт»).

Метавсесвіт – це простір у віртуальній реальності, яке люди використовують за допомогою технологій віртуальної (VR) та доповненої (AR) реальності для взаємодії та комунікації. Людьми створюються їх віртуальні образи (аватари), якими вони будуть керувати всередині віртуального світу (рисунок 1.6). Для «входу» у віртуальну реальність застосовують додаткові пристрої, перше за все спеціальну VR-гарнітуру, яка за допомогою камерам з високою роздільною здатністю, оптикою та сенсорами будуть відслідковувати людську міміку та жести.

Для розробників власник Facebook Марк Цукерберг представив ряд інструментів Presense Platform для створення віртуальних світів. Вона включає в себе засоби для розробки програмного забезпечення [21]:

- Insight SDK – є інструментом для оточення, розробник може керувати віртуальними об’єктами і взаємодіяти з навколишнім середовищем;
- Interaction SDK – набір інструментів для обробки жестів;
- Tracked Keyboard SDK – використовується для взаємодії з клавіатурою під час знаходження всередині віртуального світу;
- Voice SDK – інструмент для впровадження голосового вводу, за допомогою якого можливий голосовий пошук, навігація та контроль.

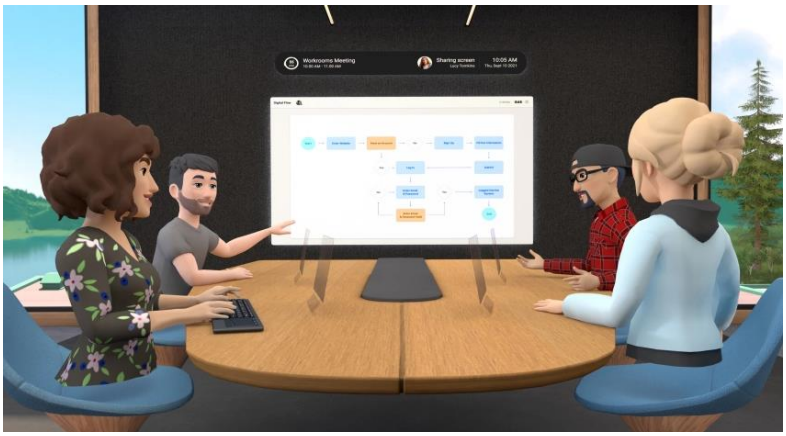


Рисунок 1.6 – Віртуальні аватари людей всередині метавсесвіту

Власники соціальних мереж бачать перспективи у розвитку віртуальних всесвітів. Це відкриє для людей нову величезну індустрію розваг, люди зможуть подорожувати, займатися спортом та отримувати новий досвід, сидячи на власному дивані. Крім того, прогнозується, що в майбутньому люди зможуть торгувати віртуальними активами та нерухомістю, компанії будуть переводити своїх працівників на віртуальні робочі місця, а віртуальні копії (аватари) можуть стати повноцінними замінниками людей.

Висновки за розділом 1

Соціальні мережі пройшли свій шлях розвитку від простих комунікаційних структур до великих інформаційних гігантів, які охоплюють увесь світ. Сучасні соціальні мережі надають своїм користувачам можливості створення персоніфікованого профілю, пошук та створення списку для спілкування, можливість поширення інформації та даних у відео-, аудіо- та інших форматах. Дослідження показують невпинне зростання кількості користувачів соціальних мереж по всьому світу. Наслідком цього є як позитивні, так і негативні ефекти для людини (соціалізація, самовираження, погіршення фінансового стану, залежність). Розвиваючись, соціальні мережі все глибше проникають у інші сфери життя людини, інтегруються в сторонні продукти. Значний вплив соціальних мереж відмічається в розвитку онлайн-бізнесу, віртуальному грошовому обігу та політичному житті людини. Можна очікувати, що в майбутньому дані тенденції будуть посилюватись, а також спроби впровадження новітніх технологій (віртуальні світи та штучний інтелект).

РОЗДІЛ 2
АНАЛІЗ ІСНУЮЧИХ ЗАГРОЗ ПЕРСОНАЛЬНИМ ДАНИМ В СОЦІАЛЬНИХ МЕРЕЖАХ

2.1 Поняття персональних даних

Питання забезпечення безпеки персональних даних є одним з актуальних проблем в сучасному світі. Кожного разу, коли користувач відвідує будь-який онлайн ресурс (веб-сайт, соціальна мережа, поштовий клієнт, мобільний додаток тощо) він надає деяку кількість персональної інформації про себе.

Одним із способів збирання персональних даних є cookies. Cookies – це файли, які зберігаються на пристрої користувача, які містять інформацію про попередні дії людини на веб-сайтах. Cookies використовуються для зручного користування ресурсом та швидкої авторизації. Окрім цього, вони зберігають такі дані як: встановлену мову, шрифти, валюту; ip адресу та місце знаходження; введений текст, дату та час відвідування, версію ОС, кліки на сайті.

Людина добровільно надає персональну інформацію соціальній мережі коли проходить процес реєстрації (мобільний номер, електронна пошта, ip адреса), а потім ще більше при заповненні профілю (ПІБ, дата народження, місце проживання, фото). Онлайн-сервіси та мобільні додатки збирають таку інформацію як геолокація, маршрути пересування, дані банківських карт.

Згідно із Законом України «Про захист персональних даних», персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [22]. Закон визначає основні терміни та регламентує порядок використання, поширення і забезпечення захисту персональних даних. Відповідальність за порушення законодавства про захист персональних даних визначено Кодексом про адміністративні порушення, і передбачає накладення грошового штрафу.

В Європейському Союзі в 2018 році почали застосовуватись нові правила обробки персональних даних [23]. GDPR (General Data Protection Regulation) – це

набір правил які регулюють діяльність компаній, які займаються збором та обробкою інформації в мережі Інтернет. Компанії обов’язково повинні запитувати дозвіл на опрацювання персональних даних. Також обов’язком є чітко та зрозуміло інформувати користувачів про те які дані збираються та мету збору цієї інформації. Права користувача включають в себе:

- право знання цілі та суб’єкту збору даних;
- право доступу до своєї інформації;
- право на видалення або виправлення інформації;
- право переносу даних;
- право незгоди на обробку.

Невиконання правил регламентованих в GDPR загрожують компанії штрафом 20 млн. євро, або до 4 % від глобального річного обороту.

2.2 Традиційні загрози

2.2.1 Фішинг

Фішинг – це вид атаки, ціллю якої є обманним шляхом дізнатись персональні або конфіденційні дані жертви (ім’я, дані кредитної карти, дані від облікового запису). Назва атаки походить від слова «Fishing» (з англ. – риболовля), основою цього виду атаки є «приманка» (фальшивий веб-сайт, смс-повідомлення, електронні листи) яку зловмисник надсилає потенційній жертві. Якщо жертва «клює» і переходить по підробленому посиланню, вона потрапляє на веб-сайт який контролюється зловмисником і виглядає як повна копія легального сайту. В таких випадках може використовуватись «реєстраційна форма», де жертві запропоновується заповнити її персональними даними. Також часто використовується фальшива форма авторизації (для викрадення логіну та паролю) та форма оплати (для викрадення даних банківської карти).

Кількість фішингових атак постійно збільшується. За даними дослідження ресурсу APWG з початку 2020 по 2021 рік кількість фішингових атак виросла майже в три рази, зображено на рисунку 2.1:

Рисунок 2.1 – зростання кількості фішингових атак в 2021 році [24]

Фішинг є одним з найпростішою, але водночас небезпечною і ефективною кібератакою. У векторі розвитку фішингової атаки через соціальну мережу зловмисник часто застосовує методи соціальної інженерії, а отже «атакується мозок» жертви. Зловмисник часто може прикидатися іншою людиною, а також розраховує на людську неуважність, цікавість або жагу легкої наживи.

2.2.2 Шкідливий код

Шкідливий код або шкідлива програма (Malware) – це шкідлива програма, призначена для реалізації загроз інформації в комп'ютерній системі, для прихованого використання ресурсів системи в своїх цідях, або перешкоджання працездатності системи.

Сучасні шкідливі програми можуть комбінувати різні види шкідливого коду, та бути використані для порушення конфіденційності, цілісності та доступності інформації. Виділяють такі основні типи шкідливого коду:

- Хробаки – використовуються для проникнення на віддалені системи, швидкої реплікації і розповсюдження в мережі. Більшість хробаків

розповсюджуються у вигляді файлів, можуть розповсюджуються через вкладення, електронну пошту, файлообмінні, LAN та мобільні мережі.

- Віруси – розповсюджуються по ресурсах локальної системи з ціллю подальшого запуску та проникнення до інших ресурсів. Часто не розповсюджуються самостійно в мережах системи, можуть мати функції бекдору.

- Троянські програми – маскуються під легальні програми, часто можуть не завдавати видимої шкоди комп'ютерній системі, а використовуватись в ботнеті для подальших DDoS атак. Можуть мати функції вірусів та збирати, передавати та проводити інші маніпуляції з даними в системі.

Соціальні мережі, як величезні онлайн-ресурси з високим трафіком, стали популярним засобом розповсюдження шкідливих програм. Більшість соціальних мереж мають функції поширення файлів, тому зловмисниками активно застосовується комбінація методів соціальної інженерії та фішингу для поширення вірусів.

Одним із способів розповсюдження шкідливого ПО в соціальних мережах є реклама. Компанії-власники соціальних мереж часто надають перевагу додатковим доходам ніж безпеці користувачів. Тому, іноді користувачі переходячи по заманливим пропозиціям, розміщеним зловмисниками, можуть потрапити на сторонній сайт із подальшим завантаженням шкідливого коду. Також нерідко зловмисники користуються бізнес-функціями соціальних мереж, де під виглядом корисного софту продають користувачам шкідливі програми.

2.2.3 Спам атаки

Спам – це атака, яка полягає в масовій розсилці шкідливих електронних повідомлень. Традиційним способом для проведення спам-атак є сервіси електронної пошти, але соціальні мережі стають все більш використовуваними платформами в розповсюдженні спаму та є більш ефективними [25]. Це пов'язано з тим, що на соціальні мережі люди витрачають більше часу, а також доставка повідомлень проходить швидше та легше.

Спам-атаки часто застосовуються в комбінації з іншими типами атак. Більшість спаму є комерційною рекламою, але часто спам-повідомлення містять в собі шкідливі посилання або програми. Для розсилання можуть використовуватися вже скомпрометовані облікові записи, спам-боти та спеціальне програмне забезпечення.

Спам-атаки часто працюють «не на якість, а на кількість», тобто ціллю є невибірково розіслати матеріал якомога більшій кількості потенційних жертв. Також існують вектори атак при використанні цілеспрямованого спаму в комбінації з іншими типами атак, коли спам виконує відволікальну функцію або функцію забивання каналу входу інформації.

2.2.4 Міжсайтовий скриптинг (XSS)

Міжсайтовий скриптинг (Cross-site scripting – XSS) – це тип атаки, в якій зловмисник впроваджує шкідливий код або скрипт в сторінку веб-сайту. Коли відкриває «заражену» сторінку, шкідливий код взаємодіє з віддаленим сервером зловмисника.

Проводячи атаку міжсайтового скриптингу, зловмисник не атакує жертву напряму. Він використовує уразливості веб-сайту та впроваджує туди JavaScript (Java, Ajax, HTML) код. Браузер жертви приймає такий код як звичайну частину веб-сторінки, тому сама жертва може не підозрювати, що її дані було скомпрометовано.

Виділяють три основні категорії атак міжсайтового скриптингу: Stored XSS, Reflected XSS та DOM-моделі.

- Stored XSS – тип XSS який є найбільш шкідливим та небезпечним, оскільки зловмисник має доступ до сервера веб-сайту. В такому випадку зловмисник може довільно модифікувати веб-сторніку і шкідливий код буде спрацьовувати автоматично при заході на неї. Шкідливі скрипти можуть бути вмонтовані в будь-які об’єкти на сайті, текст та рисунки.

- Reflected XSS – тип атаки, коли зловмисник має самостійно створити та доставити до жертви URL-посилання, яке містить шкідливий скрипт. В такому

випадку зловмисник застосовує фішинг або прийоми соціальної інженерії та переконує жертву перейти по посиланню. При вході веб-сайт надсилає відповідь, а в браузері жертви спрацьовує шкідливий код.

- DOM-моделі (Document Object Model XSS) – атака, при якій корисне навантаження спрацьовує в результаті модифікації середовища DOM (вигляд документу у якому подається HTML до браузеру) у браузері жертви, так що клієнтська сторона коду спрацює непередбачуваним чином. Тобто вигляд HTML сторінки не зміниться, але код який знаходиться на сторінці буде виконуватись по іншому в результаті модифікацій.

XSS-атаки є одними з найпоширеніших веб-атак. За даними відкритого проекту з безпеки веб-застосунків (OWASP) за 2021 рік міжсайтовий скриптинг посідає 3 місце по популярності [26]. Основною ціллю таких атак є викрадення cookies з подальшим використанням в інших типах атак, а також XSS використовується для поширення шкідливого ПЗ та фішингу.

2.3 Мультимедіа та метадані

Найголовнішою функцією соціальних мереж є обмін інформацією. Мультимедійні дані, фото та відео вже є невід’ємною складовою такого обміну. Кількість мобільних пристроїв збільшується, а якість камер, встановлених в них, вдосконалюється. Тому фото та відео які поширюються в соціальних мережах є переважно високої якості. В той же час, методи пошуку та аналізу мультимедіа, таких як розпізнавання обличь, геомітки, місце розташування розвиваються. Тому, ризики поширення та незаконного подальшого використання персональних даних зростають.

Як правило, користувачі є обережними, та не публікують в мережі фото своїх паспортів та домашні адреси. Однак, не у всіх користувачів є розуміння, що при публікації деяких фото чи відео файлів вони видають свої персональні дані. Наприклад, якщо користувач викладає мультимедійні матеріали зі свого будинку чи виду з вікна, зловмисник проаналізувавши такі дані може знайти знайти домашню адресу.

Причиною витоку персональної інформації також можуть бути і колективні мультимедійні дані. В такому випадку, вони можуть бути опубліковані без відомості чи згоди користувача, що в поєднанні з технологіями розпізнавання обличь може призвести до порушення приватності.

Метадані – це дані про дані, тобто інформація, яка описує будь-який файл, документ, сторінку, мультимедіа. Метадані можуть містити таку інформацію як дату та час створення документу чи фото, тип, розмір та інші технічні дані. Така інформація може бути цінною для атак на користувача. Приклад метаданих, які містяться в фотографії зображено на рисунку 2.2:

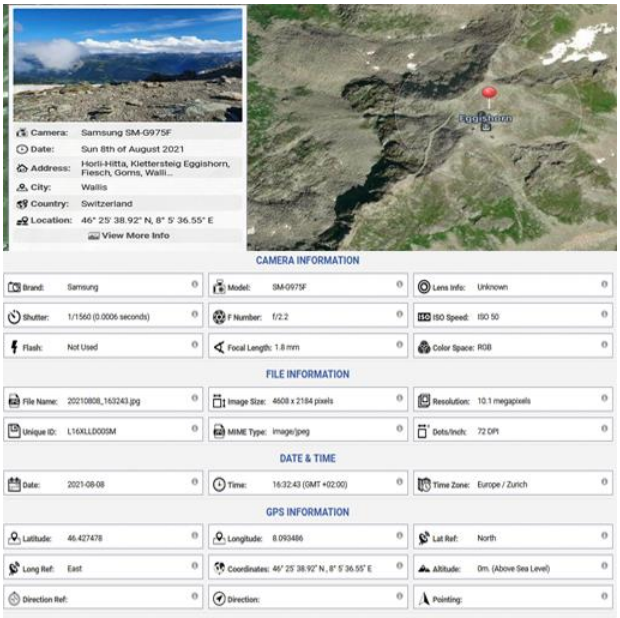


Рисунок 2.2 – Метадані фотографії

Одним з типів метаданих які можуть містити мультимедіа є місце розташування та координати GPS. Для зловмисника є корисними не тільки дані про фактичне місце перебування користувача. Аналіз даних про місце розташування та пересування людини може розкрити іншу чутливу персональну інформацію, таку як релігійні, політичні переконання, стан здоров’я і багато іншого.

Різні соціальні мережі мають різну політику щодо метаданих. Наприклад Facebook видаляє метадані перед завантаженням на сервер. Twitter, Google+

зберігають всі метадані окрім GPS координат, а деякі тематичні соціальні мережі про подорожі зберігають GPS та розташування за замовчуванням. Окремі соціальні мережі та форуми надають налаштування метаданих користувачу.

2.4 Фальшиві профілі

Типовими атаками в соціальних мережах є атаки з використанням підроблених профілів. Такі атаки полягають в тому, що зловмисник створює аккаунти з фальшивими даними, «додається в друзі» до користувачів та відправляє повідомлення. Зазвичай такі атаки автоматизовані або напів-автоматизовані для імітації реальної людини. Ціллю таких атак є збір інформації з закритих профілів, розсилка спаму та рекламних повідомлень.

Одним з векторів атак фальшивих профілів є «викрадення» та копіювання чужої сторінки в соціальній мережі. Клонування профілю може бути з використанням даних з вже існуючої сторінки в іншій мережі, або створення нової сторінки з наповненням із викрадених даних. Одним з визначень такої атаки є «атака клонів ідентичності» [27]. Ця атака зазвичай є цілеспрямованою і потребує деяких знань про потенційну жертву. Використовуючи клонований профіль, зловмисник намагається встановити довірливі стосунки з друзями реального користувача та за допомогою методів соціальної інженерії збирати персональну або конфіденційну інформацію. Отримані дані зловмисник може використати в розвитку подальшої атаки, може продати отриману інформацію або шантажувати жертву.

2.5 Деанонімізація

Більшість соціальних мереж дозволяють своїм користувачам приховувати свою особистість, використовуючи псевдоніми або вигадані імена. Атака деанонімізації полягає в тому, щоб при використанні даних про користувача отриманих з відкритих або закритих джерел, проаналізувавши та співставивши, розкрити особистість користувача.

Користувачів в соціальних мережах можна представити у вигляді вузлів з багатьма атрибутами (стать, вік, ім'я, інтереси, розташування і т.д), а взаємодію між

ними – у вигляді ребер. Тоді соціальна мережа може бути у вигляді графа з інформацією про відносини між вузлами. Схематично процес денонімізації можна представити як рисунок 2.3. Повна мережа позначена як *(a)*, анонімна з місцем розташування – *(c)*, мережа з іменами – *(b)*. Процес деанонімізації полягає в тому, щоб співставити вузли *(b)* і *(c)* для ідентифікації користувача в мережі та встановленні відповідного місця розташування. Тобто, необхідно знайти пари вузлів (u_1,v_1), (u_2,v_2), (u_3,v_3) та (u_4,v_4).

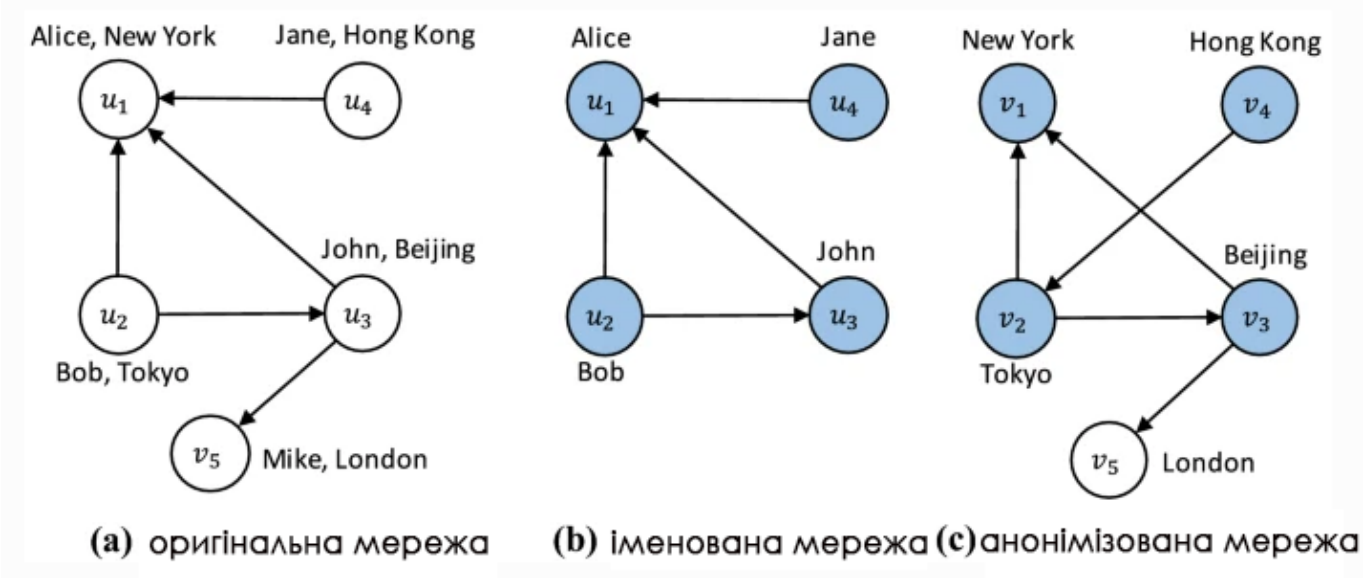


Рисунок 2.3 – Загальна схема деанонімізації на прикладі графів [28]

Загальні стратегії деанонімізації можна розділити на два типи. Перший заснований на основі початкових співставлень даних які користувач розповсюджує в мережі про себе (приналежність до груп в мережі, списки контактів, відстеження cookies, аналіз контенту). Такий спосіб є ефективним, однак для його успішної реалізації необхідна велика кількість та якість початкових даних, що в сучасних соціальних мережах через налаштування приватності не завжди вдається зібрати в достатньо. Другий тип обробляє мережі напряму без початкових відображень. Тут використовуються сигнатури вузлів та їх структурні особливості (описова інформація, схожість вузлів). Такий спосіб є більш загальним і його легше

налаштувати, однак недоліком такого підходу є низька ефективність та недостатня точність результатів аналізу.

Технічні варіанти реалізації деанонімізації в соціальних мережах є дуже різноманітними. Одним з прикладів є «таймінг атака», яка активно використовувалась спецслужбами Білорусі для становлення власників опозиційних Telegram-чатів. Суть її полягає в тому, що збираються дані про підключення та вихід із соціальної мережі, тобто ведеться логування. Функція відображення часу входу та виходу є відкритою, якщо її не вимкнути за замовчуванням. Після цього, зібраний лог активності співставляють з даними провайдерів про підключення до соціальної мережі або мережі Tor, яка не допоможе анонімному користувачу в такій атаці. Маючи дані про періоди підключень всіх користувачів та підозрюваного, крок за кроком шукають перетини цих даних, і крок за кроком коло підозрюваних стає вужче. Окрім даних про час входу, застосовувались і метадані контенту, а саме розмір мультимедіа переданих на сервер в конкретний момент часу.

2.6 Профайлінг

Захист персональних даних залежить не тільки від користувача, а і від соціальної мережі, тому користувач викладаючи свою персональну інформацію в мережу не може бути на сто відсотків впевнений за її збереження. Нерідкими є випадки коли сама соціальна мережа збирає та оброблює персональні дані користувачів з наміром складання «портрету» користувача та подальшому продажу реклами. Ця інформація може бути надана державі для проведення правоохоронних дій, а може надаватися стороннім продавцям для збільшення ефективності реклами. Такі профілі містять велику кількість особистих даних про користувача, такі як щоденні вподобання користувача, політичні, релігійні переконання, медична інформація.

Відомим є скандал з Facebook та компанією Cambridge Analytica який відбувся в 2017 році в США [29]. Відомо, що Cambridge Analytica заплатила третій стороні за створення застосунку, яке виглядало як опитування і просила надати деякі персональні дані за винагородження. Однак потім виявилось, що збирались дані не

тільки тих користувачів, які дали згоду, а і всіх його друзів. Після збору даних проводилася аналітика та складались спеціальні «психологічні портрети», які потім продавались іншим стороннім компаніям. Такі «психологічні портрети» активно використовували для визначення політичних вподобань і таргетованої реклами для приваблення потенційних виборців. Вибірка такого дослідження складала більшу частину країни, тому після цього велось судове розслідування впливу на результат виборів в США 2016 року.

Таким чином, персональні дані, які були зібрані без відома користувачів змогли вплинути на політичну ситуацію в світі.

Висновки за розділом 2

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Персональними даними користувача в соціальних мережах є інформація про власника сторінки (ПІБ, стать, дата народження, місце проживання, фото та інша особиста інформація) а також телефонний номер, адреса електронної кошти або cookies.

За визначення та регуляцію персональних даних в Україні відповідає Закон України «Про захист персональних даних». В Європейському Союзі за регулювання збору та обробки персональних даних з 2018 року відповідає GDPR (General Data Protection Regulation).

Загрози персональним даним створюють зловмисники, які користуються як традиційними способами атак в кіберпросторі (фішинг, шкідливий код, спам), використання вразливостей соціальних мереж (міжсайтовий скриптинг XSS) так і направлені та цілеспрямовані атаки.

Загрозою для своїх персональних даних може бути і сам користувач. Поширення мультимедіа може спричинити витік інформації через метадані, а збір та аналіз поширеної про себе інформації може привести до деанонімізації користувача. Людина є соціальним створінням, тому на неї може бути здійснений вплив за допомогою методів соціальної інженерії та атак «фальшивих профілів». Захищеність персональних даних в соціальних мережах є достатньо відносною характеристикою,

тому для її підвищення варто дозволяти поширювати собі лише ту інформацію, яка вже відома великій кількості осіб, або ту яку готовий втратити.

РОЗДІЛ 3
ЗАЛЕЖНІСТЬ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ВІД ДОВІРИ В СОЦІАЛЬНИХ МЕРЕЖАХ

3.1 Поняття довіри в соціальних мережах

Термін «довіра» можна трактувати по різному, але у більшості людей він буде викликати схожі асоціації. В загальному, довіру можна описати як впевненість суб'єкта в тому, що об'єкт функціонує так як очікувалось, не маючи при цьому можливості відслідковувати і контролювати дії об'єкту. В різних сферах поняття довіри та її властивостей і аспектів визначається по різному. В психології – це стан людини, в якому вона приймає або ігнорує можливість бути уразливим перед об'єктом довіри, основуючись на позитивних очікуваннях. На соціальному рівні довіра є властивістю деякої соціальної групи, яка передбачає що інші члени групи заслуговують довіри і очікують довіри до себе, а також приймати рішення виходячи із взаємної довіри.

Поняття довіри в контексті соціальних мереж можна розділити на дві категорії: довіра користувача та довіра системи. Довірою користувача є суб'єктивне очікування об'єкта у відношенні майбутньої поведінки. С соціальних мережах довіра формується на зворотньому зв'язку, який виникає в результаті взаємодії користувачів. Така довіра є відносною, чим частішою є взаємодія користувачів тим більше зміцнюються відносини, а довіра збільшується з позитивним досвідом, і зменшується з негативним. Довіра може бути прямою або «рекомендованою». Пряма довіра виникає в результаті прямої взаємодії людини з іншим користувачем і отриманого від неї досвіду, після цього людина може рекомендувати даного користувача іншим своїм знайомим. В наслідок цього формуються «реферальні ланцюжки», в яких користувач оцінюється іншими за такими параметрами: надійність в наданні послуг/допомоги/в спілкуванні, та надійність в якості рекомендовувача. Після кожної взаємодії досвід користувачів буде оновлюватись, що призводить до збільшення або зменшення довіри серед інших суб'єктів.

Системна довіра виходить із області безпеки і представляє собою очікування, що система або пристрій будуть вести себе визначеним чином, щоб виконати своє завдання. Концепція довіри до системи підтримується програмними та апаратними рішеннями. Наприклад, комп'ютерна система яка виконує свої програмні та апаратні функції так як очікується, а сервіси надає стабільно і без перешкод, можна назвати системою яка заслуговує довіру.

В цілому моделі оцінки довіри в соціальних мережах можна розділити на три основні категорії:

- на основі топології мережі – основними параметрами визначення довіри є розміри, щільність мережі;
- на основі взаємодії – параметрами визначення довіри є дослідження поведінкових паттернів взаємодії між користувачами;
- гібридні моделі – комбінація двох перших методів, параметрами є дослідження контенту та поведінки користувачів, а також динаміку розповсюдження топології мережі.

Проводяться дослідження в області довіри користувачів в соціальних мережах. Дослідження команди з Університету штату Північна Кароліна в 2020 році проводили опитування в мережі Facebook[32]. В опитуванні приймало участь 661 людини, і відповідали на питання чи довіряють вони соціальній мережі, чи вірять вони публікаціям та що думають про дезинформацію і розпізнавання фейків.

Результати показали, що якщо користувач думає що вміє розпізнавати неправдиву інформацію, то він більше довіряє соціальній мережі, а чим більше ви довіряєте мережі тим більше шансів, що людина стане активним користувачем цієї мережі.

Було виявлено, що користувачі які менше довіряють платформі більш критично ставляться до інформації та перевіряють її. Виявилось, що довіра є більш когнітивна (заснована на розумовому осмисленні та аналізу отриманої інформації), а недовіра – більше залежить від відчуттів користувача.

Команда дослідників вважає, що для підтримування або збільшення популярності соціальна мережа має укріплювати довіру користувачів, проте головною проблемою є надання гарантії достовірності контенту який публікується.

3.2 Метод визначення захищеності персональних даних від довіри

В даному підрозділі розглядається метод визначення захищеності персональних даних від довіри в соціальних мережах, розроблений в 2021 році Лаптєвим О., Савченко В., Котенко А., Ахрамович В., Самосюк В., Шуклін Г., Бігун А. [31].

Загрози втрати довіри між користувачами представляються у вигляді залежності з чотирма параметрами довіри:

$$T_i = [D_j, D_n, D_m, D_k], \qquad (3.1)$$

де T_i – набір загроз втрати довіри користувачами;

D_j – довіра в надаванні послуг (довіра до поставника якісних послуг або ресурсів);

D_n – довіра делигування (довіра до користувача який приймає рішення та діє від імені суб'єкта);

D_m – довіра постачальника до користувача, якому надається доступ до ресурсів;

D_k – «контекстуальна довіра» визначає рівень довіри користувача до системи і механізмів, які забезпечують транзакції і мережеву безпеку.

Втрата довіри – це процес який відбувається на протязі деякого інтервалу часу. Кількість інформації позначається в методі як I, потік інформації поза межами інформаційної системи як *dI*, а швидкість змін в потоці - $\frac{dI}{dt}$. Якщо потік і швидкість змін в потоці рівна 0, то витоку інформації немає:

$$dI = 0; \frac{dI}{dt} = 0 \qquad (3.2)$$

В методі визначається, що витік інформації може залежати від таких факторів як безпека системи, комплекс мір та заходів які приймаються для нейтралізації загроз безпеці персональних даних. Показник захищеності інформаційної системи позначається як Z. Витік інформації залежить від параметрів захищеності інформаційної системи можна відобразити у рівнянні:

$$\frac{dI}{dt} = Z_p Z + (C_V + C_k) I \text{ ,(3.3)}$$

де Z_p – це коефіцієнт впливу засобів захисту інформації;

C_v – коефіцієнт впливу швидкості витоку персональних даних;

C_k – фактор впливу об'єму персональних даних на їх витік.

Виходячи з цього можна зробити висновок, що в даній моделі витік інформації залежить від:

- розміру інформаційної системи (і як наслідок кількості персональних даних);
- швидкості витоку персональних даних;
- засобів захисту та мір нейтралізації загроз інформаційній системі.

Безпека системи визначається як здатність системи протидіяти несанкціонованому доступу до конфіденційних даних. Захищеність системи буде залежати від: розміру системи, загрози інформаційній безпеці від втрати довіри між користувачами. Рівняння залежності захищеності системи:

$$\frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \text{ ,} \qquad (3.4)$$

де D_i – коефіцієнт впливу загроз безпеці персональних даних від втрати довіри між користувачами;

C_{d2} – коефіцієнт впливу розміру системи на безпеку;

C_{d1} – коефіцієнт впливу безпеки системи на витік персональних даних.

Об'ємо рівняння (3.3) і (3.4):

$$\begin{cases} \frac{dI}{dt} = Z_p Z + (C_V + C_k) I \\ \frac{dZ}{dt} = D_i - I(C_{d2} + C_{d1}) \end{cases}, \quad (3.5)$$

$$dI = 0; \frac{dI}{dt} = 0 . \quad (3.6)$$

З другого рівняння системи (3.5) виходить, що:

$$\overline{I} = \frac{D_i}{(C_{d1}+C_{d2})} . \quad (3.7)$$

З першого рівняння системи (3.5) знаходиться $\overline{Z}$:

$$Z_P \overline{Z} - \frac{(C_V+C_k)D_i}{(C_{d1}+C_{d2})}, \quad (3.8)$$

$$\overline{Z} = \frac{(C_V+C_k)D_i}{(C_{d1}+C_{d2})Z_P} . \quad (3.9)$$

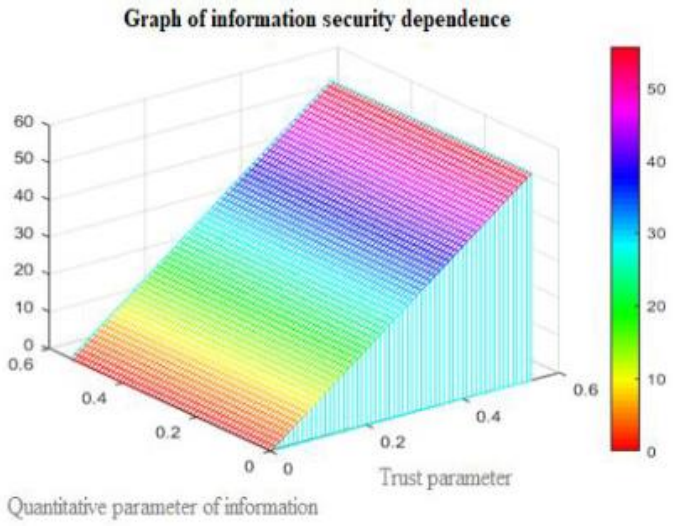
Параметри довіри між користувачами соціальної мережі впливають на надійність системи захисту.

Відповідно, початковий стан захищеності системи визначається системою рівнянь:

$$\begin{cases} \overline{I} = \frac{D_i}{(C_{d1}+C_{d2})} \\ \overline{Z} = \frac{(C_V+C_k)D_i}{(C_{d1}+C_{d2})Z_P} \end{cases} . \quad (3.10)$$

Продовжуючи розрахунки, автори даного методу диференціюють перше рівняння системи (3.10), та вирішуючи отримане рівняння отримують три варіанти розв’язку та графіків залежності захисту персональних даних від довіри. В трьох випадках прослідковується зростання рівню захищеності персональної інформації за збільшенням параметрів довіри [,18 с.].

В цілому, результати дослідження показали, що залежність захищеності особистих даних від довіри є прямо пропорційна постійним параметрам захисту системи, і збільшується зі збільшенням факторів і параметрів довіри, що зображено на графіку:



3.3 Розрахунок переваг запропонованого методу

Для того, щоб розрахувати переваги запропонованого методу із додаванням додаткового коефіцієнту довіри зробимо наступні припущення:

- кожний з коефіцієнтів дає чітке значення імовірності захисту;
- усі коефіцієнти брали для одного випадку, з аналізу літературних джерел (самостійно коефіцієнти та імовірності не розраховувались);
- усі коефіцієнти впливають послідовно, тобто загальна імовірність є сумою усіх часткових імовірностей. Кореляцію та взаємовплив не враховувалась.

Розрахуємо ймовірність захисту початкового методу, який складається з трьох параметрів довіри:

$$T_i = [D_j, D_n, D_m],$$

де $P_{Dj} = 0{,}25$;

$P_{Dn} = 0{,}23$;

$P_{Dm} = 0,24;$

$P_{загальна} = P_{Dj} + P_{Dn} + P_{Dm} = 0,25+0,23+0,24 = 0,72$

Тепер розрахуємо ймовірність захисту виходячи із вищенаведених припущень та додаванням параметру довіри D_k:

$$T_i = [D_j, D_n, D_m, D_k],$$

де $P_{Dj} = 0,25;$

$P_{Dn} = 0,23;$

$P_{Dm} = 0,24;$

$P_{Dk} = 0,15;$

$P_{загальна} = P_{Dj} + P_{Dn} + P_{Dm} + P_{Dk} = 0,25+0,23+0,24+0,15 = 0,87$

Таким чином, перевага запропонованого методу складає 15 відсотків.

3.4 Рекомендації щодо удосконалення методу

В даному методі визначено чотири параметри довіри, такі як: довіра в надаванні послуг, довіра делигування, довіра постачальника до користувача і контекстуальна довіра до системи і базових механізмів її функціонування. Три з чотирьох параметрів передбачають довіру користувача до системи або до того хто за нею стоїть, а довіра делигування передбачає собою більш «робочу» довіру на рівні замовник-виконавець.

Однак в соціальних мережах користувачі постійно стикаються з невідомими їм раніше суб’єктами мережі, тому рівень довіри до такого користувача буде встановлюватись за іншими критеріями.

Пропонується додати такий параметр довіри, який буде заснований на взаємодії між користувачами.

В загальному взаємодію користувачів можна розділити на дві основні категорії:

• класифікація дій на основі інформації, що передається (обзори, розміщені коментарі, з урахуванням таких показників як кількість та послідовність обзорів, кількість оцінок, кількість та середня довжина коментаря та ін.);

• класифікація бінарних взаємодій (можуть виникати в соціальних мережах між автором та оцінювачем, між оцінювачами або авторами та ін.).

Також можуть бути включені такі фактори як різниця у часі між реакціями користувачів. Взаємодія яка сталася щойно має більше значення ніж та, що відбулась деякий час тому, або із затримкою. Таким чином, час є важливим фактором для фіксації зміни у взаємодії між користувачами.

Запропонований параметр довіри може бути створений на базі моделі соціальної довіри в соціальних мережах. Структура такої моделі складається з наступних складових: особистий досвід, соціальний капітал, соціальна довіра, рекомендація, зображено на рисунку 3.2:

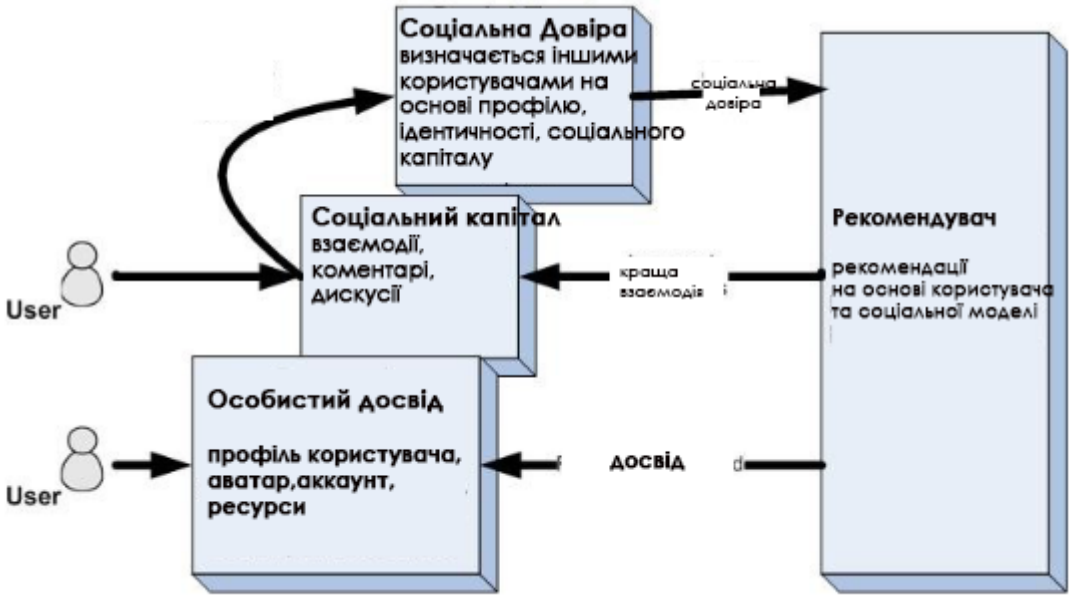


Рисунок 3.1 – Схема моделі соціальної довіри в соціальних мережах

Особистий досвід складається в самому початку користування соціальною мережею. Коли користувач реєструється, створює профіль, встановлює аватар та вказує інтереси.

Соціальний капітал користувачі набирають при взаємодії з іншими користувачами, наприклад познайомившись з кимось та відповівши на його коментар або повідомлення. Ціллю набуття соціального капіталу є створення середовища для майбутньої взаємодії.

Соціальна довіра є вихідною, і формується на основі особистого досвіду та соціального капіталу окремого користувача.

Рекомендації відповідно засновуються на соціальній довірі. Ціллю рекомендацій є створення онлайн-спільноти релевантним для її учасників, а також для збільшення та підтримки взаємної довіри, оскільки з часом вона поступово слабшає.

Виходячи з вище сказаного, новий параметр довіри в методі визначення захищеності персональних даних буде враховувати взаємодію в мережі між користувачами, що в свою чергу дозволить правильно оцінити та попередити загрози персональним даним спрямованим на людину. А саме атаки соціальної інженерії, підроблених профілів, частково фішингу.

3.5 Сфери використання методу

Розглянутий метод надає можливість оцінювати рівень захищеності персональних даних від довіри. Зараз більшість великих підприємств мають свої внутрішні корпоративні соціальні мережі. Тому реалізація та впровадження даного методу в SIEM (Security Information and Event Management) – систему підприємства, функцією якого є збір та керування інформацією про безпеку, є можливим варіантом використання.

Також однією з можливостей використання даного методу є DLP (Data Leak Prevention). Це спеціалізоване програмне забезпечення, призначене для попередження та захисту конфіденційної корпоративної інформації. Часто такі програми пропонують функціонал блокування передачі інформації через різні

канали, та моніторингу працівників в мережі, тому реалізація розглянутого методу може бути корисною.

Широкий спектр можливостей використання даного методу з'являється коли мова йдеться про аудит безпеки. Проводячи зовнішній або внутрішній аудити, компанії мають за мету визначити загальний показник захищеності компанії, а також даних які зберігаються та оброблюються. Компанії зацікавлені в захищеності персональних даних працівників та клієнтів, оскільки це є вимогою законодавства більшості країн світу.

Як відомо, онлайн-торгівля та бізнес з кожним роком все більше розвивається та інтегруються в соціальні мережі. Тому власники соціальних мереж, наряду з торговими майданчиками та банками починають використовувати «антифрод системи». Антифрод системи – це комплекс мір, які дозволяють оцінити інтернет-транзакції на предмет шахрайства. Для цього система для кожної операції застосовує деякі критерії, і якщо транзакція їм не відповідає – система перевіряє її додатково та сигналізує про це. По результату перевірки, зазвичай транзакції та обліковому запису користувача присвоюються спеціальні «мітки». Зелена якщо оплата здійснюється в межах однієї країни та сума платежу середня, жовта – якщо сума перевищує деякий ліміт або є декілька додаткових «маркерів недовіри» і транзакція потребує додаткової перевірки, і червона – коли висока вірогідність шахрайства (cookie та IP не співпадають, сума платежу є великою та на великій відстані від покупця), така транзакція відхиляється.

Сучасні антифрод системи широко використовують штучний інтелект та самонавчаються на основі аналізу Big Data. Під час проходження транзакції системою перевіряється підозрілі профілі користувачів а також cookies і їх поведінку в соціальних мережах, тому запропонований метод є актуальним до використання в даній сфері.

Висновки за розділом 3

В цьому розділі було розглянуто загальне поняття довіри в соціальних мережах. В цілому довіру в соціальних мережах можна розділити на дві основні

категорії: довіра користувачів та довіра системи. Довіра користувачів полягає в двохсторонніх та багатосторонніх зв’язків між користувачами, довіра системи полягає в забезпеченні віри користувачів у стабільне та прогнозоване функціонування системи.

Було описано метод визначення захищеності персональних даних від довіри в соціальних мережах. Загрози втрати довіри між користувачами було визначено в якості чотирьох параметрів (довіра в надаванні послуг, довіра делигування, довіра постачальника до користувача і контекстуальна довіра), а захищеність системи залежить від впливу загроз безпеці персональних даних від втрати довіри між користувачами, розміру інформаційної системи, засобів та мір спрямованих на попередження та знешкодження загроз інформаційній системі. Враховуючи параметри довіри та стан захищеності системи, було розраховано залежність захисту персональних даних від довіри між користувачами, та показано на графіку.

Було запропоновано удосконалення існуючого методу шляхом додавання додаткового коефіцієнту довіри P_{Dk}. Сам коефіцієнт а також ймовірність захисту було взято з проаналізованої літератури. В результаті порівняння показало, що додавання додаткового параметру довіри покращує розглянутий метод на 15 відсотків.

ВИСНОВКИ

Соціальні мережі стрімко поширюються та захоплюють все більше сфер життя людини. Починаючи свій шлях від простих комунікаційних структур та зроставши до величезних інформаційно-технологічних гігантів, соціальні мережі продовжують розвиток. Основними тенденціями розвитку соціальних мереж є: інтеграція зі сторонніми ресурсами, розвиток торгівлі та віртуальних валют всередині соціальних мереж, політичне застосування та інноваційні шляхи розвитку.

Оскільки соціальні мережі стають все більш відкриті та персоніфіковані виникає потреба у досконалому захисті персональних даних. Загрозами персональним даним в соціальних мережах можуть бути як традиційні атаки, так і атаки спрямовані конкретно на особистість з використанням засобів соціальної інженерії.

В практичній частині роботи було розглянуто поняття довіри та метод визначення захищеності персональних даних від довіри в соціальних мережах. Метод включає в себе такі параметри довіри як довіра в наданні послуг, довіра делигування, довіра постачальника до користувача, а також враховано загальний стан захищеності системи від розміру, швидкості витоку та засобів захисту. В роботі було запропоновано удосконалення існуючого методу шляхом додавання додаткового коефіцієнта довіри в існуючу модель. Отримавши можливі ймовірності захисту шляхом аналізу літератури було зроблено висновок, що комбінація методів, а саме удосконалення існуючих моделей за рахунок використання додаткового коефіцієнта дає перевагу. У нашому випадку отримали перевагу на 15 відсотків.

Запропонований метод з його можливостями оцінки захищеності персональних даних має широкі можливості потенційного використання у системах захисту інформації, а саме в антифрод, SIEM, DLP та інших подібних системах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Moreno J.L. Who Shall Survive? A New Approach to the Problem of Human Interrelations, 1934. (Книга «Кто должен выжить»)

2. Barnes J.A. Class and Committees in a Norwegian Island Parish // Human Relations. – 1954. Vol.7. – Pp. 39–58.

3. Богданов Д.В. Социальные функции Интернета // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Социальные науки. – 2011. – No 1 (21). – С. 114–120

4. Дужникова, А.С. Социальные сети: современные тенденции и типы пользования / Дужникова А. С. // Мониторинг общественного мнения. - 2010. - No 5 (99). - С.238-251

5. Dora Simoes Handbook of Research on Enterprise 2.0: Technological, Social, and Organizational Dimensions// (University of Aveiro, Portugal) and Sandra Filipe (University of Aveiro, Portugal). – 2014

6. Christakis N.A., Fowler J. H. Connected. The Surprising Power of Our Social Networks and How They Shape Our Lives. London: Little, Brown, 2009. P.21.

7. Патаракин, Е. Д. Педагогический дизайн социальной сети Scratch //Международный электронный журнал "Образовательные технологии и общество (Educational Technology & Society)" - 2013. - V.16. - No2. - С.505-528.

8. Тоискин, В.С. Классификация социальных сетей Интернет как элементов социальных структур [Электронный ресурс] / Тоискин В.С., Красильников В.В. // Научный электронный архив Академии естествознания. Социология информации и коммуникации, 2012.

9. https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

10. Kohut A. Internet Users Are On the Rise: But Public Affairs Interest Isn’t // Columbia Journalism Review.2000. 38(5), PP. 68–69.

11. Hoffman, D.L., & Thomas, P.N. (2011). Social media strategy. In Handbook on Marketing Strategy, Venkatesh Shankar and Gregory S. Carpenter (eds.), Edward Elgar Publishing, Ltd.

12. Buechel, E., & Berger, J. (2018). Microblogging and the value of undirected communication. Journal of Consumer Psychology, 28(1), 40-55.

13. Wilcox, K., & Andrew, T.S. (2012). Are close friends the enemy? Online social networks, narcissism, and self-control. Working Paper, Babson College, Babson Park

14. Jeffrey Lambert, George Barnstable, Eleanor Minter, Jemima Cooper, and Desmond McEwan. Cyberpsychology, Behavior, and Social Networking. 2022. https://www.liebertpub.com/doi/10.1089/cyber.2021.0324

15. Facebook, Twitter, Google+, or LinkedIn … Which should you log in with? [Електронний ресурс]. Режим доступу: https://www.comparitech.com/blog/vpn-privacy/facebook-twitter-google-or-linkedin-which-should-you-log-in-with/ (13.01.2016)

16. Anchises M. G. de Paula. (2010). Security Aspects and Future Trends of Social Networks, IJoFCS 1, PP. 60-79.

17. Shopping on Social Media Platforms Expected to Reach $1.2 Trillion Globally by 2025, New Accenture Study Finds [Електронний ресурс]. Режим доступу: https://newsroom.accenture.com/news/shopping-on-social-media-platforms-expected-to-reach-1-2-trillion-globally-by-2025-new-accenture-study-finds.html

18. How to Set Up Instagram Shopping [Електронний ресурс]. Режим доступу: https://www.facebook.com/business/learn/lessons/set-up-instagram-shopping

19. Прийнято Закон "Про віртуальні активи" [Електронний ресурс]. Режим доступу: https://www.rada.gov.ua/news/Novyny/213503.html (08.09.2021)

20. Twiplomacy study 2020 [Електронний ресурс]. Режим доступу: http://www.twiplomacy.com/ (20.07.2020)

21. Welcome to Meta [Електронний ресурс]. Режим доступу: https://about.facebook.com/meta/

22. Закон України Про захист персональних даних [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/2297-17#Text

23. What is GDPR, the EU’s new data protection law? [Електронний ресурс]. Режим доступу: https://gdpr.eu/what-is-gdpr/

24. Phishing Activity Trends Report, 4th Quarter 2021 [Електронний ресурс]. Режим доступу: https://docs.apwg.org/reports/apwg_trends_report_q4_2021.pdf

25. Bhat SY, Abulaish M (2013) Community-based features for identifying spammers in online social networks. In: Proceedings of the 2013 IEEE/ACM international conference on advances in social networks analysis and mining—ASONAM ’13, pp 100–107

26. Welcome to the OWASP Top 10 – 2021 [Електронний ресурс]. Режим доступу: https://owasp.org/Top10/

27. Kharaji, M.Y.; Rizi, F.S.; Khayyambashi, M.R. A New Approach for Finding Cloned Profiles in Online Social Networks. arXiv, 2014, arXiv:1406.7377.

28. Fast De-anonymization of Social Networks with Structural Information Yingxia Shao, Jialin Liu, Shuyang Shi, Yuemei Zhang & Bin Cui Data Science and Engineering volume 4, pages 76–92 (2019)

29. The Cambridge Analytica scandal changed the world – but it didn't change Facebook [Електронний ресурс]. Режим доступу: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook (18.03.2019)

30. Cheng, Y. and Chen, Z.F. (2021), "Encountering misinformation online: antecedents of trust and distrust and their impact on the intensity of Facebook use", Online Information Review, Vol. 45 No. 2, pp. 372-388.

31. O.Laptiev, V.Savchenko, A. Kotenko, V.Akhramovych, V.Samosyuk, G.Shuklin, A.Biehun. Method of Determining Trust and Protection of Personal Data in Social Networks. International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13, No. 1, 2021. pp.15-21.

32. Nepal, Paris, Bista, & Sherchan, (2013); A Trust Model Based Analysis of Social Networks, IJTMC.

33. Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, Iryna Manzhul. Modeling the protection of personal data from trust and the amount of

information on social networks. Number 1 (2021), «EUREKA: Physics and Engineering» pp.24–31. DOI:10.21303/2461-4262.2021.001615.

34. S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. Synergy of building cybersecurity systems: monograph / Edited by– Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

35. S.Yevseiev, O.Laptiev, O.Korol, S.Pohasii, S.Milevskyi.The metodology of automatical detection of digital illegal obtaing means of information. Scientific discussion. Praha, Czech Republic.Vol. 1, No 62, 2021. pp. 16– 22. ISSN 3041-4245

36. O. Laptiev, S. Pohasii, S. Milevskyi, R. Khmelevsky, A. Barabash, V. Ponomarenko. Information security of the eGovernment. Journal of science. Lyon. №27, 2021, pp.49-54. ISSN 3475-3281.

37. Савченко В. А. (Savchenko V. A.), Ахрамович В. М. (Akhramovych V. M.), Акулінічева М. В. (Akulinicheva M. V.). Оцінювання параметрів безпеки персональних даних у степеневих соціальних мережах на основі їх топології. Сучасний захист інформації. К. ДУТ:-2020 .-№3.- с. 6-13.

38. Савченко В.А., Ахрамович В.М. Захист персональних даних користувачів в соціальних мережах. Тези доповідей II Міжнародна науково–практична конференція «Проблеми кібербезпеки інформаційно–телекомунікаційних систем» (PCSICS), Україна, університет ім. Тараса Шевченка. 02–03 квітня 2020р.–с. 34–35

39. Чегренець В.М., Ахрамович В.М., Інформаційна безпека особистості в соціальних мережах. Тези доповідей Abstracts of IIInternational Scientific and Practical Conference Lviv, Ukraine 25–26 November2019 Pp 250–254. “Sci–conf.com.ua”.

40. Ахрамович В.М., Чегренець В.М. Дослідження характеристик особистої інформаціїї користувача в інтернет–соціальних мережах. Тези доповідей Advances of science .Proceedings of articles the international scientific conference Czech Republic, Karlovy Vary – Ukraine, Kyiv, 6 December 2019 Pp 101–110 .“Sci–conf.com.ua”.