НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

До захисту допущено
Завідувач кафедри

_____ **Дмитро ЛАНДЕ**

(підпис)

«_____»_____ 2023 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Системи, технології та математичні методи кібербезпеки»
спеціальності 125 «Кібербезпека»

на тему: Виявлення фейкових сторінок соціальної мережі Instagram

Виконав (-ла): здобувач вищої освіти **IV** курсу, групи ФБ-93
(шифр групи)

Приходько Андрій Русланович
(прізвище, ім'я, по батькові) (підпис)

Керівник к.ф.-м.н., с.н.с., доцент кафедри Інформаційної безпеки

Смирнов Сергій Анатолійович
(посада, науковий ступінь, вчене звання, прізвище, ім'я, по батькові) (підпис)

Рецензент
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище, ім'я, по батькові) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Здобувач вищої освіти _____
(підпис)

Київ – 2023 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

Рівень вищої освіти – перший (бакалаврський)
Спеціальність – 125 «Кібербезпека»
Освітньо-професійна програма «Системи, технології та математичні методи кібербезпеки»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Дмитро ЛАНДЕ
(підпис)

«___»_____2023 р.

ЗАВДАННЯ
на дипломну роботу здобувачу вищої освіти

Приходько Андрій Русланович
(прізвище, ім'я, по батькові)

1. Тема роботи: Виявлення фейкових сторінок соціальної мережі Instagram

керівник роботи: к.ф.-м.н., с.н.с., доцент кафедри Інформаційної безпеки Смирнов Сергій Анатолійович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «26» травня 2023 р. No 2028-С

2. Термін подання здобувачем вищої освіти роботи 9 червня 2023 р.

3. Вихідні дані до роботи : Відомості про фейкові сторінки соціальних мереж, основи машинного навчання

4. Зміст роботи: Ознайомлення з об'єктом дослідження, а саме - соціальною мережею Instagram; Проведення аналізу та виокремлення головних ознак підозрілих сторінок; Побудова власної моделі виявлення фейкових сторінок за допомогою методів машинного навчання;

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): Презентація

6. Дата видачі завдання: 10.02.2023

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів дипломної роботи	Примітка
1	Отримання завдання	10.02.2023	
2	Огляд існуючих публікацій та літературних джерел	11.02.2023 - 20.02.2023	
3	Робота над першим розділом дипломної роботи	20.02.2023 - 12.03.2023	
4	Аналіз головних ознак підроблених сторінок	13.03.2023 - 28.03.2023	
5	Робота над другим розділом	29.03.2023 - 16.04.2023	
6	Проходження переддипломної практики	17.04.2023 - 21.05.2023	
7	Створення програмної реалізації та її тестування	22.05.2023 - 30.05.2023	
8	Написання третього розділу дипломної роботи та висновків	31.05.2023 - 08.06.2023	
9	Створення презентаційного матеріалу	09.06.2023 - 11.06.2023	
10	Передзахист дипломної роботи	12.06.2023	
11	Доопрацювання роботи та виправлення зауважень комісії	13.06.2023 - 18.06.2023	
12	Захист дипломної роботи	19.06.2023	

Здобувач вищої освіти _____ Андрій ПРИХОДЬКО
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

Керівник роботи _____ Сергій СМИРНОВ
(підпис) (**Власне ім'я, ПРІЗВИЩЕ**)

РЕФЕРАТ

Дипломна робота має обсяг 73 сторінок, містить 22 рисунків, 4 додатків, 1 таблицю та 16 джерел посилань.

Соціальні мережі стали невід'ємною частиною життя більшості людей сьогодення у зв'язку з стрімкою діджиталізацією суспільства. Це є причиною для збільшення шляхів проведення різного типу шахрайських злочинів спрямованих на одного користувача або великої групи людей, наприклад, країни. Фейкові сторінки - головний інструмент для здійснення таких дій, тому наразі гостро стоїть питання забезпечення механізму виявлення підроблених сторінок у соціальних мережах.

Дана робота містить аналіз головних загроз, які пов’зані з використанням фейкових сторінок у соціальних мережах. У ході роботи було виділено головні ознаки, за якими можна стверджувати, що дана сторінка є підробленою. Була побудована програмна реалізація виявлення фейкових сторінок за допомогою методів машинного навчання. Отримані результати дослідження можуть бути використані для подальшого впровадження механізму виявлення та блокування фейків у соціальній мережі Instagram.

Ключові слова: фейк, профіль, сторінка, Instagram, машинне навчання

ABSTRACT

The thesis has a volume of 73 pages, contains 22 figures, 4 appendices, 1 table and 16 sources of references.

Social networks have become an integral part of the lives of most people today due to the rapid digitalization of society. This is the reason for the increase in the number of ways to conduct various types of fraudulent crimes aimed at a single user or a large group of people, such as a country. Fake pages are the main tool for such actions, so the issue of providing a mechanism for detecting fake pages on social networks is now acute.

This work analyzes the main threats associated with the use of fake pages on social media. During the work, the main features that can be used to assert that a given page is fake were identified. A software implementation for detecting fake pages using machine learning methods was built. The obtained results of the study can be used for further implementation of the mechanism for detecting and blocking fakes on the social network Instagram.

Keywords: fake, profile, page, Instagram, machine learning

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Аккаунт, профіль, сторінка - позначення облікового запису користувача в певній системі

Фейкова сторінка - сторінка, яка намагається підробити легітимний вигляд автентичної організації, бренду, людини або сервісу з метою обману користувачів.

API - Application program interface.

ML - Machine learning.

AI - Artificial intelligence.

KNN - K nearest neighbors.

EDA - Exploratory data analysis

LR - Linear regression;

.

ВСТУП

Завдяки стрімкому розвитку інформаційних технологій нам все важче уявити своє життя без використання соціальних мереж. Така мережа являє собою веб-сайт чи мобільний застосунок, який дозволяє користувачам, які пройшли процес реєстрації, користуватися ним. Застосунки користуються великою популярністю, адже надають змогу підтримувати зв’язок з іншими користувачами незалежно від місця їх перебування. Знайомства можуть як просто розширити коло спілкування, так і дають змогу знайти нову роботу чи партнерів. Також платформи соціальних мереж стали великим місцем для реклами товарів, просування та продажу послуг. Звісно, найпопулярніша причина чому соціальні мережі користуються великою популярністю - це широка опція проведення дозвілля. Серед них можна виділити перегляд відео та смішних картинок-мемів, читання новин та навчальні відео. Проте, за великими зручностями ховаються великі небезпеки та ризики, що пов’язані з їх використанням. Соціальні мережі мають можливість викликати залежності у користувачів, наслідком яких можуть бути соціальна ізоляція та закритість, фізичні проблеми зі здоров'ям. Проте, найголовніші виклики та загрози тримають у собі кіберзлочинці, які можуть використовувати соціальні мережі як засіб для вчинення протиправних дій. Всіх шахраїв у більшості випадків об'єднує одна спільна річ - це використання фейкової сторінки у соціальній мережі. При спілкуванні з невідомою до цього моменту особою користувачеві перш за все необхідно встановити чи його співрозмовник той, за кого він себе видає. Більшість користувачів Інтернету підтверджують, що хоча би раз у житті мали досвід, коли їх хотіли обманути в соціальній мережі.

Тому, ***метою даної роботи*** є створення алгоритму перевірки сторінок користувачів мережі на справжність.

Актуальність роботи підтверджується тим, що згідно дослідження, застосунок Instagram займає 2 місце серед найпопулярніших соціальних мереж серед українців та 4 у цілому світі. Зручність для користувачів, можливості для бізнесу та різноманітність контенту є одними з головних причин, чому Instagram став такою популярною платформою соціальних мереж. В свою чергу, стати жертвою злодіїв у соціальній мережі стає все простіше через більшу кількість сторінок та методів обману.

Для досягнення мети дипломної роботи поставлено наступні завдання:

- Дослідити найбільш популярні методи обману в Instagram;
- Дослідити наявні методи перевірки сторінок на справжність;
- Спроектувати власний алгоритм перевірки сторінки на справжність;
- Програмна реалізація алгоритму;
- Виконати тестування програми та оформити висновки до роботи.

Об'єктом дослідження - сторінки користувачів у соціальній мережі Instagram.

Предмет дослідження - виявлення фейкової сторінки у соціальній мережі Instagram.

Дипломна робота складається з: 72 сторінок, 3 розділів, містить 22 рисунків, 4 додатків, 1 таблицю та 16 джерел посилань.

Апробація результатів роботи

Дослідження було представлено у вигляді доповіді на XXI Всеукраїнській науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики».

Публікації

Робота була опублікована у збірнику матеріалів XXI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» [1].

1 ОЗНАЙОМЛЕННЯ З ОБ'ЄКТОМ ДОСЛІДЖЕННЯ

1.1 Соціальна мережа Instagram

Соціальна мережа Instagram - сервіс, який був створений у 2010 році Кевіном Сістром і Майком Крігером. За словами авторів, їх ідея була створити платформу для поширення фото та відео між друзями. Застосунок виявився напрочуд вдалим і набирав стрімкої популярності, а у 2012 році він був викуплений корпорацією Facebook і став однією з найбільш популярних соціальних мереж серед усього світу. До найкращих можливостей мережі користувачі відносять [2]:

- Стрічка, на якій користувачі можуть дивитися відео та фото під профілів, на які вони підписані, у хронологічному порядку;
- Історії: короткі 15-ти секундні відео, які зникають після 24 годин з моменту їх публікації. Історії дозволяють поширювати фотографії, відео та текст, і можуть бути покращені за допомогою наклейок, фільтрів та інших творчих інструментів.;
- Приватні повідомлення: ця опція дозволяє надсилати повідомлення іншому користувачеві;
- Використання хештегів дозволяє розбити контент по категоріям, тим самим отримати аудиторію, яка є зацікавленою у даній тематиці.
- Вкладка "Дослідження" в Instagram дозволяє користувачам відкривати новий контент та облікові записи на основі їхніх інтересів. Вона містить персоналізовані рекомендації, популярні дописи облікових записів, на які користувач ще не підписався.

Це все дозволило Instagram отримати шалену популярність та більш ніж 1 мільярд активних користувачів щодня.

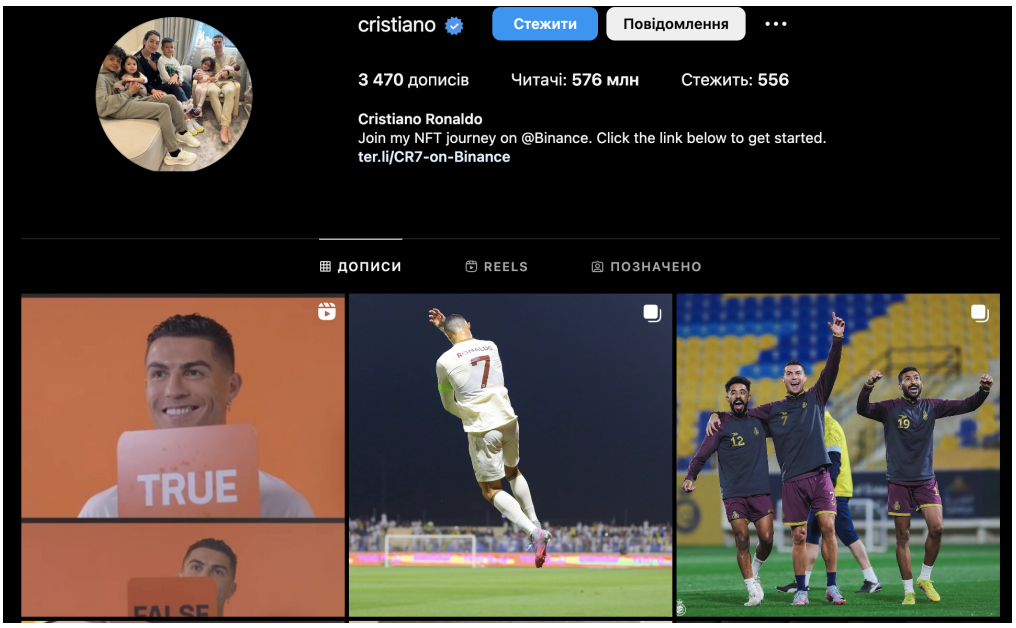

Рисунок 1.1 - Приклад Instagram сторінки

Епідемія коронавірусу, а також повномасштабне вторгнення рф в Україну суттєво збільшила кількість українців, що почали використовувати дану соціальну мережу. За результатами дослідження [3], Instagram займає друге місце по популярності серед соціальних мереж, якими користуються українці - більш ніж 16 мільйонів користувачів.

Збільшення популярності прямо пропорційно підвищує кількість можливих загроз, оскільки часто користувач, що лише зареєструвався у соціальній мережі, має брак знань та потрібних правил поведінки в Інтернеті. Це дозволяє шахраям без особливих зусиль провести злочинні дії та отримати гроші, особисті дані користувача, приватні повідомлення використовуючи фейкові сторінки. Щоб захистити себе, новачки повинні бути обережними щодо інформації, якою вони діляться в Інтернеті, і знати про ризики, пов’язані з соціальними мережами. Їм також слід уважно ставитися до запитів друзів або повідомлень від невідомих осіб.

1.2 Проблема фейкових сторінок

Фейкова (несправжня) сторінка у соціальній мережі - це сторінка, автор якої видає себе за іншу особу, магазин чи компанію. Створити таку сторінку в мережі Instagram, не є проблемою, оскільки при реєстрації єдиний засіб перевірки користувача відбувається за його номером телефону. Тобто, для реєстрації необхідно ввести код, який система надішле на ваш телефон. Враховуючи ціну найдешевшого стартового пакету послуг операторів мобільного зв'язку в Україні для шахраїв не є проблемою створювати нові сторінки бодай кожного дня у великій кількості. Розглядаючи фейкові сторінки магазинів, то вони майже у всіх випадках є копією справжньої сторінки. Це робиться для того, щоб при першому погляді у користувача не виникло жодних підозр про те, що дана сторінка є обманом і може бути використана для злочину. В свою чергу, коли злочинець хоче видати себе за іншу людину, то точна копія оригінальної сторінки в більшості випадків не є обов’язковою, адже майже завжди жертва не знала до цього моменту людину, яка розміщена на ній.

Існує декілька типів фейкових акаунтів, що існують у соціальних мережах. Найпоширеніші 2 типи це [4]:

- Боти: це сторінки, які процес створення яких та контролювання відбувається автоматично за допомогою програмного забезпечення. Здебільшого, які сторінки використовуються для підписки на інші сторінки задля просування їх, залишення коментарів, лайків під дописами. В коментарях боти часто можуть залишати посилання на зловмисні сайти чи сервіси.
- Зловмисні сторінки: контролюються реальними людьми та мають за мету отримати вигоду від інших користувачів шляхом їх обману.

Варто зазначити, що створення фейкових сторінок не завжди відбувається лише заради матеріального прибутку. Найбільш популярними причинами створення користувачем фейкового аккаунту це:

- Анонімність та приватність: деякі користувачі бажають мати несправжні сторінки для того, щоб залишатися анонімним у соціальній мережі та не бути ідентифікованим. Як приклад, вони можуть користуватися цим при дискусіях на онлайн форумах;
- Обман: інші створюють підроблені облікові записи з наміром ввести в оману інших. Ціллю таких дій можуть стати особисті дані, паролі користувачів.
- Знайомство з платформою: деякі користувачі при своїй першій взаємодії з деякою соціальною мережею часто створюють несправжні сторінки.
- Поширення фейкових новин: такі новини є одним з механізмів інформаційної війни проти України, яка триває вже не один рік. Головною метою є поширення неправдивої інформації та маніпулювання громадською думкою.

Одним з прикладів маніпуляцій є російське втручання у президентські вибори США 2016 року за допомогою ботоферм. Ботоферма являє собою автоматизовану мережу облікових записів які, як правило, використовуються для штучного збільшення кількості підписників, лайків і коментарів в соціальній мережі Instagram. Вони часто використовуються для підвищення соціального статусу облікового запису або для маркетингових цілей. Росіяни створювали фейкові акаунти на відомих платформах, у тому числі й Instagram, для того, щоб поширювати публікації сумнівного змісту, яке б змусило виборців віддати свій голос за Дональда Трампа. Ці облікові записи часто видавали себе за американців, використовуючи вкрадені особи чи фальшиві особи, щоб виглядати більш

достовірними. Завдяки великій кількості сторінок у простих американців складалось враження, що така думка є правдивою. Контент, який був опублікованим фейками мав за мету посіяти розбрат серед виборців та поділити Америку на два табори. Для більшого поширення таких публікацій росіяни використовували таргетовану рекламу, що дозволяє суттєво збільшити охоплення публікації. Це втручання у вибори лише ще раз підкреслює потенційну небезпеку, яку можуть нести в собі фейкові сторінки та необхідність для соціальних мереж вживати заходи задля боротьби з ними.

Щоб уберегти себе від можливих проблем, що пов'язані з використанням підроблених сторінок, користувачі повинні притримуватися базових правил поведінки в Інтернеті, а саме:

- бути обережними, натискаючи посилання або завантажуючи вкладення з невідомих або підозрілих джерел;
- перевірити, що адреса WEB-сайту на який вони переходять є ідентичною до справжньої сторінки, яка розміщена в пошукових системах;
- не поширюйте особисту чи фінансову інформацію співрозмовнику, у справжності якого не впевнені;
- бути уважними до запитів друзів або повідомлень від невідомих осіб. Завжди перевіряти особу облікового запису, перш ніж приймати запит або брати участь у розмові;
- використовуйте двофакторну аутентифікацію там, де це є можливим. Це надасть вам додатковий рівень захисту;
- перевіряти відгуки про магазини на справжність, тобто бути впевненим що коментар залишає справжня особа;

Зі свого боку соціальна мережа також вживає заходів для того, щоб блокувати фейкові сторінки на своїй платформі. Одним з найпростіших

методів є верифікація акаунтів: вона використовується для користувачів з великою кількістю підписників, на кшталт політиків, зірок естради, відомі бренди. Верифікована сторінка має біля свого ім’я синю галочку, яку можна отримати пройшовши процедуру перевірки з боку мережі.

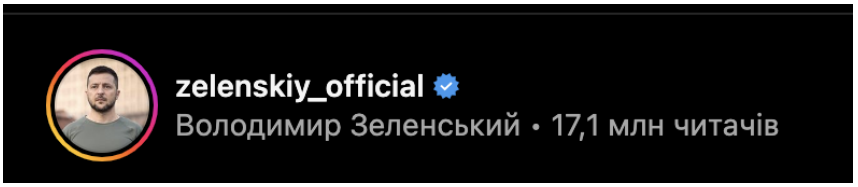

Рисунок 1.2 - Приклад верифікованої сторінки

Наступним методом захисту виступають автоматизовані системи перевірок та машинне навчання. Такі системи дозволяють аналізувати підозрілу активність користувачів, наприклад, реєстрація багатьох нових сторінок з однієї IP адреси. В свою чергу, методи машинного навчання дозволяють використовувати алгоритми, які дозволяють визначати та видаляти дані сторінки. Для аналізу використовуються різні моделі активності користувача в мережі.

Під час виборів президента США 2020 року компанія Facebook (Instagram є продуктом цієї компанії) створила механізм, який мав попередити ситуацію, яка сталась на виборах у 2016 році. Для цього соціальна мережа почала приховувати від користувачів публікації, які були позначені як фейкові. А користувачам, що хочуть надіслати пост, який був визнаним шкідливим будуть показувати вікно з повідомленням про це. Фейкові повідомлення й далі будуть доступні в стрічці, але для їх перегляду необхідно буде натиснути на додаткову кнопку.

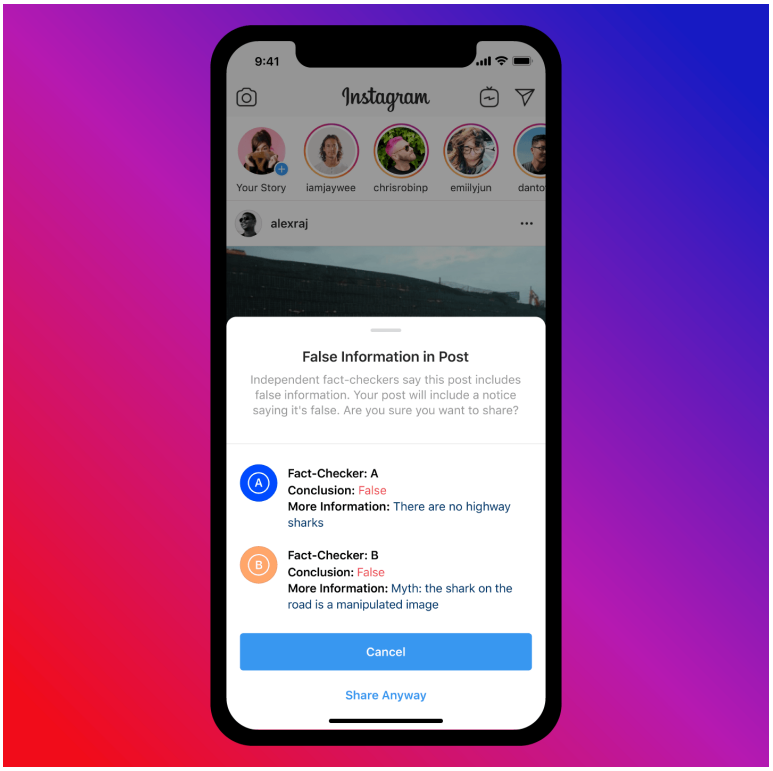

Рисунок 1.3 - Приклад повідомлення про поширення фейку

З користувацької сторони, натрапивши на фейкову сторінку, у вас є змога повідомити про це до служби підтримки мережі. Ці скарги будуть оглянуті у найкоротший час командою Instagram.

Загалом Instagram постійно вдосконалює методи боротьби з фейковими аккаунтами. Хоча жодна система не є надійною, ці заходи допоможуть зменшити поширеність підроблених облікових записів і забезпечать безпечний користувацький досвід для людей.

1.3 Найпоширеніші способи обману шляхом використання фейкової сторінки у мережі Instagram

Як вже було зазначено мною раніше, використання фейкових сторінок часто має за мету отримання персональної вигоди для злочинця. До найбільш частих методів, які використовують злочинці слід віднести:

фейкові магазини, пропозиція спонсорства, перемоги у розіграшах, обмани, які засновані на особистих почуттях та багато інших подібних [5].

Якщо дана атака виявляється успішною, то злодій може:

- змінити ваші дані для входу;
- за допомогою Instagram сторінки отримати доступ до інших сторонніх додатків;
- продовжити фішингову розсилку вашим друзям - це є напрочуд небезпечна дія, оскільки ваш товариш отримає повідомлення думаючи, що йому пише справжня людина. У нього не виникне жодних підозр про потенційний обман;
- викладання реклами чи сумнівних постів на вашій сторінці;
- отримати доступ до особистих повідомлень;

Фейкові магазини можуть використовувати інструменти Instagram задля поширення профілю за допомогою реклами, отримання нових підписників та клієнтів. Злочинці позиціонують за справжнього продавця, обіцяючи великі знижки на товари чи унікальні пропозиції. На мою думку, варто завжди уникати рекламних оголошень, які обіцяють продати якісні брендові речі за дешеву ціну. На жаль, при купівлі речей у такому магазині їх Ви, звісно, не отримаєте. Максимум, що можна зробити - це подати скаргу до підтримки мережі. Але, навіть у випадку блокування сторінки магазину, її власнику ніщо не завадить створити новий аккаунт та продовжити обманювати користувачів.

Також, великої популярності набирають обмани, які засновані на особистих почуттях користувача. Цей метод потребує від злочинця терпіння, оскільки сам злочин можливий лише після деякого часу, коли він завоює довіру жертви. Як правило, такий обман починається зі встановлення контакту з жертвою та початком листування. Згодом, коли

злочинець відчуває, що жертва йому довіряє, він починає просити у неї гроші. Причини можуть бути будь-які: погане становище, термінова медична операція, борги, тощо. При потраплянні у таку ситуацію жертві необхідно звертати увагу на граматичні та лексичні помилки, оскільки часто зловмисник є іноземцем, який спілкується вашою мовою лише використовуючи онлайн перекладач. Також, необхідно бути уважним до користувачів, які відмовляються записувати голосові чи відеоповідомлення. У більшості випадків це означає що ваш співрозмовник не той за кого він себе видає.

Наступним прикладом є обман з використовуючи перемогу у конкурсі чи розіграші. Злочинець проводить розсилку повідомлень у який дає знати користувачам, що вони стали переможцями та виграли дороговартісний приз. Під час розмови з користувачем злочинець може просити у нього особисті дані для відправлення подарунку чи то оплату за послуги доставки поштою.

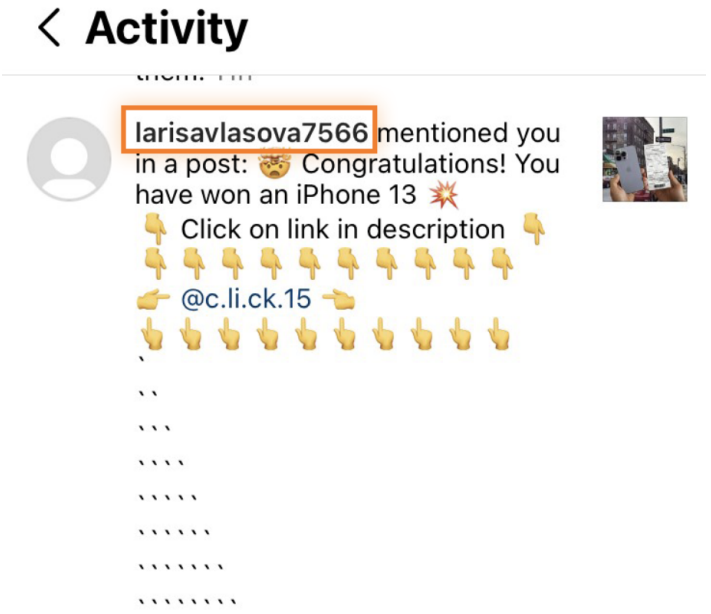

Рисунок 1.4 - Приклад повідомлення про перемогу у розіграші

Вважаю за необхідне зазначити такий вид махінацій як інвестиція у прибуток. Для такого злочину користувач, який володіє фейковою сторінкою оформлює її у такому стилі, щоб дати всім зрозуміти що у нього є кошти і це дозволяє йому вести багате життя ні в чому не відмовляючи собі. Після цього робиться розсилка повідомлень мережею та пропонується жертві зробити маленький грошовий внесок. В свою чергу злочинець обіцяє їй, що він ці гроші примножить в декілька разів, оскільки знає способи як це робити. На жаль, через недостатню грамотність в інтернеті та низький соціальний стан, багато людей стають жертвами такої афери.

В силу того, що багато роботи зараз можна виконувати дистанційно працюючи з дому - у соціальних мережах, включно з Instagram, активізувались злочинці, які видають себе за роботодавців. Вони ставлять за мету отримання особистих даних, в тому числі копії документів. Для такої атаки злочинець пише жертів та пропонує їй не існуючу роботу з дуже високою заробітною платою. Для того, щоб отримати бажану роботу, користувач має надіслати великий перелік особистих даних, які можуть включати в себе копію паспорту та індивідуального ідентифікаційного номеру, телефонні номери, адреса проживання, склад сім'ї, тощо. Така широка кількість даних дозволить злодію в теорії брати мікрокредити та займи на ім'я жертви, чи то просто продати їх на чорному ринку.

Мною були наведені лише деякі з багатьох прикладів обману у соціальній мережі Instagram. Проте, у більшості випадків всіх їх об'єднують спільні речі, а саме:

- використання зловмисником фейкових акаунтів;
- бажання отримати від жертви її особисті дані чи гроші;
- обіцянка легкого заробітку великої суми грошей;

Висновки до розділу 1

У даному розділі я ознайомився з об’єктом дослідження даної дипломної роботи, а саме природою фейкових сторінок у соціальній мережі Instagram. Розглянуто соціальну мережу та її особливості. Досліджено проблему існування та можливі загрози фейкових сторінок у Instagram. Наведено найпоширеніші способи вчинення злочинів з використанням підроблених сторінок.

2 ВИЯВЛЕННЯ ОЗНАК ФЕЙКОВОЇ СТОРІНКИ

2.1 Аналіз підписників сторінки

Підписником сторінки в Instagram вважається користувач, який підписався на сторінку іншого користувача. Тепер вона може спостерігати за його активністю - дивитися нові фото, читати дописи, які публікуються на сторінці. Підписники є важливою метрикою для сторінки будь-якого користувача, адже вони визначають наскільки сторінка є популярною чи актуальною.

Підписники є важливою метрикою для перевірки сторінки та виявлення фейків на платформі [6]. Грунтуючись на ній можливо виділити основі маркери, які можуть свідчити про те, що аккаунт є несправжнім, а саме:

- Кількість підписників. Якщо сторінка має велику кількість підписників, проте їх активність на сторінці вкрай низька чи взагалі відсутня, це може свідчити про те, що автором сторінки є не той, за кого він себе видає.
- Якість сторінок підписників. Навіть, якщо кількість підписників на сторінці є прийнятною та цілком реальною, чудовим маркером для перевірки аккаунту є якість сторінок підписників. Якщо такі профілі виглядають неякісно та штучно - це може бути ознакою фейку. Такі підписники можуть мати однакові шаблони назви профілю, бути що може означати, що вони були штучно додані до досліджуваної сторінки. Якщо ж сторінка належить реальній людині, то її підписники теж є справжніми особами - її друзями, знайомими.
- Відношення кількості підписників та підписок користувача. Суттєва різниця даних значень може свідчити про те, що сторінка є фейковою. При цьому можуть існувати випадки, коли власниками

сторінки є дуже відомі люди, але шанс того, що це є фейком зводиться до нуля за допомогою інструменту верифікації Instagram (значок синьої галочки, який був описаний у першому розділі).

Звісно, при аналізу можуть виникати питання про те, звідки фейкові сторінки можуть набирати собі нових підписників. Це можна зробити завдяки онлайн сервісам для накрутки підписників Instagram. Для прикладу я вирішив узяти свою власну сторінку та користуватися сайтом Instasamer [7]. Даний ресурс дозволяє безкоштовно накрутити собі 10 підписників та 10 лайків на допис кожні 30 хвилин або 20 підписників та 20 лайків кожні півгодини за умови, що сторінка сайту залишається відкритою на цей час.

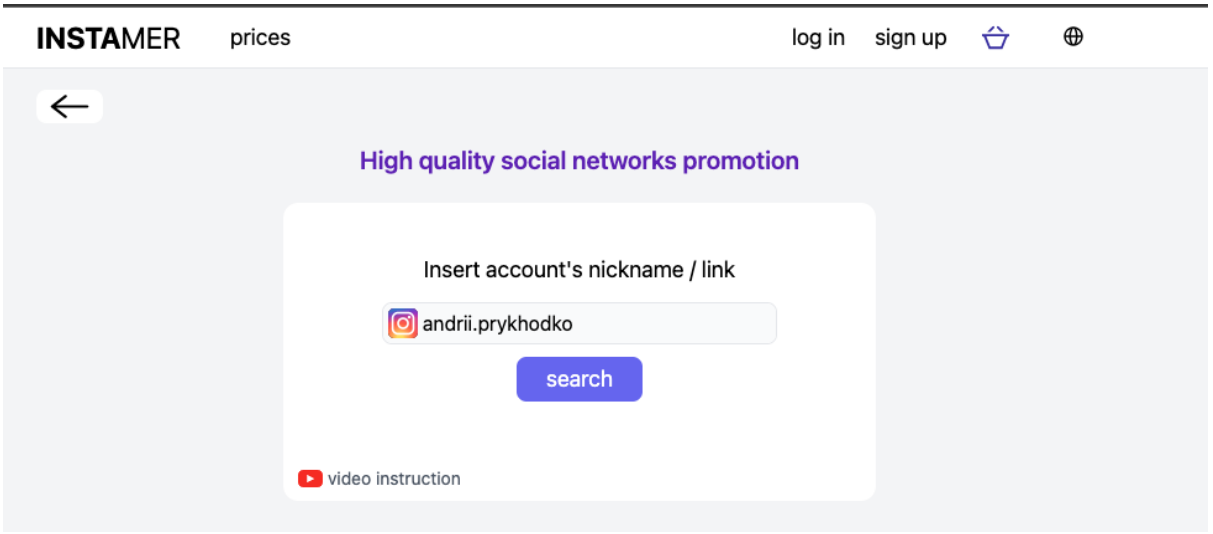

Рисунок 2.1 - Головна сторінка сайту instasamer.com

За окрему плату можна збільшити кількість підписників у багато разів. Наприклад, 200 підписників та 100 лайків на сторінці будуть коштувати усього 55 гривень (1.5$).

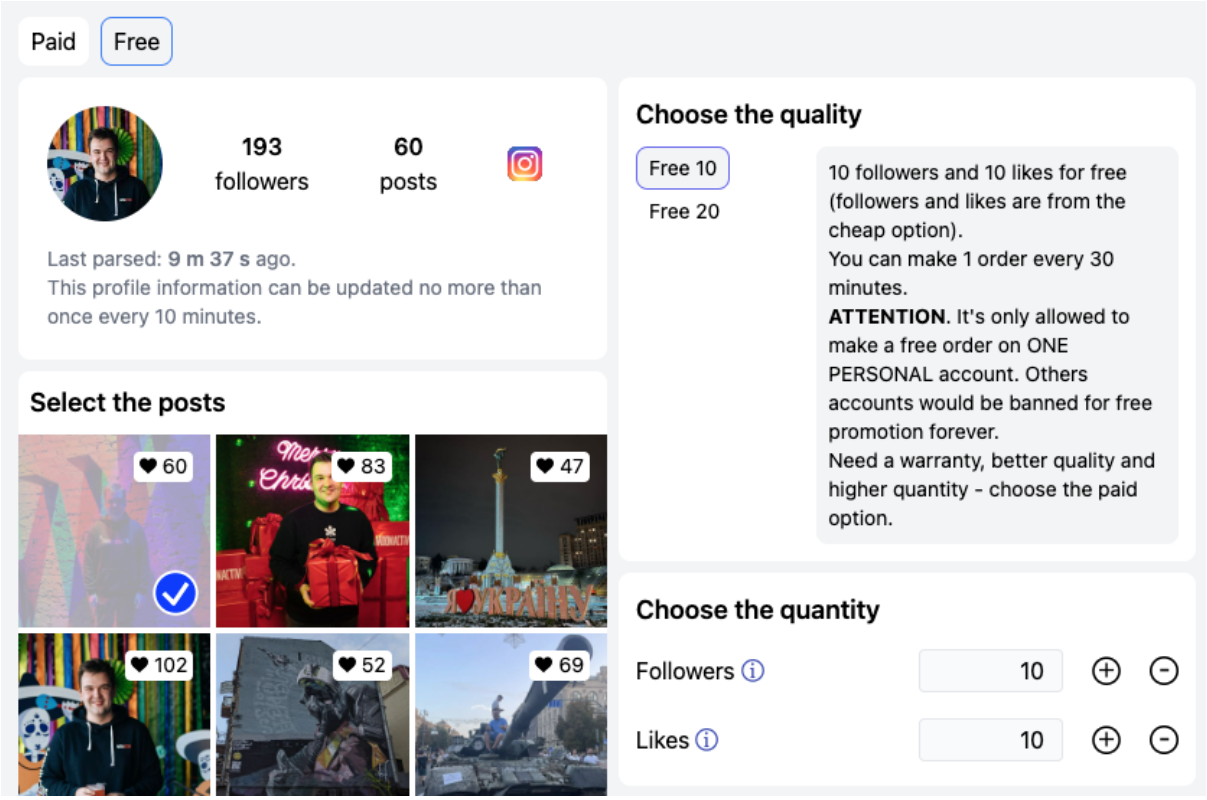

Рисунок 2.2 - Форма для безкоштовної накрутки підписників

Після того, як бажана кількість була обрана, можливо запустити процес долучення нових підписників до сторінки. Майже за 1 хвилину на моєму особистому Instagram профілю з'явились нові фоловери. При цьому, якість даних користувачів є максимально низькою - всі акаунти у більшості випадків мають однаковий шаблон імені у форматі:

ім'я+прізвище+число

А користувачі, які на мене підписались, не мають навіть фото профілю. Якщо переглянути кожного окремо, можна побачити, що всі вони мають лише декілька підписників та зовсім не мають дописів на сторінці. Це може свідчити лише про те, що ці аккаунти також є фейковими.

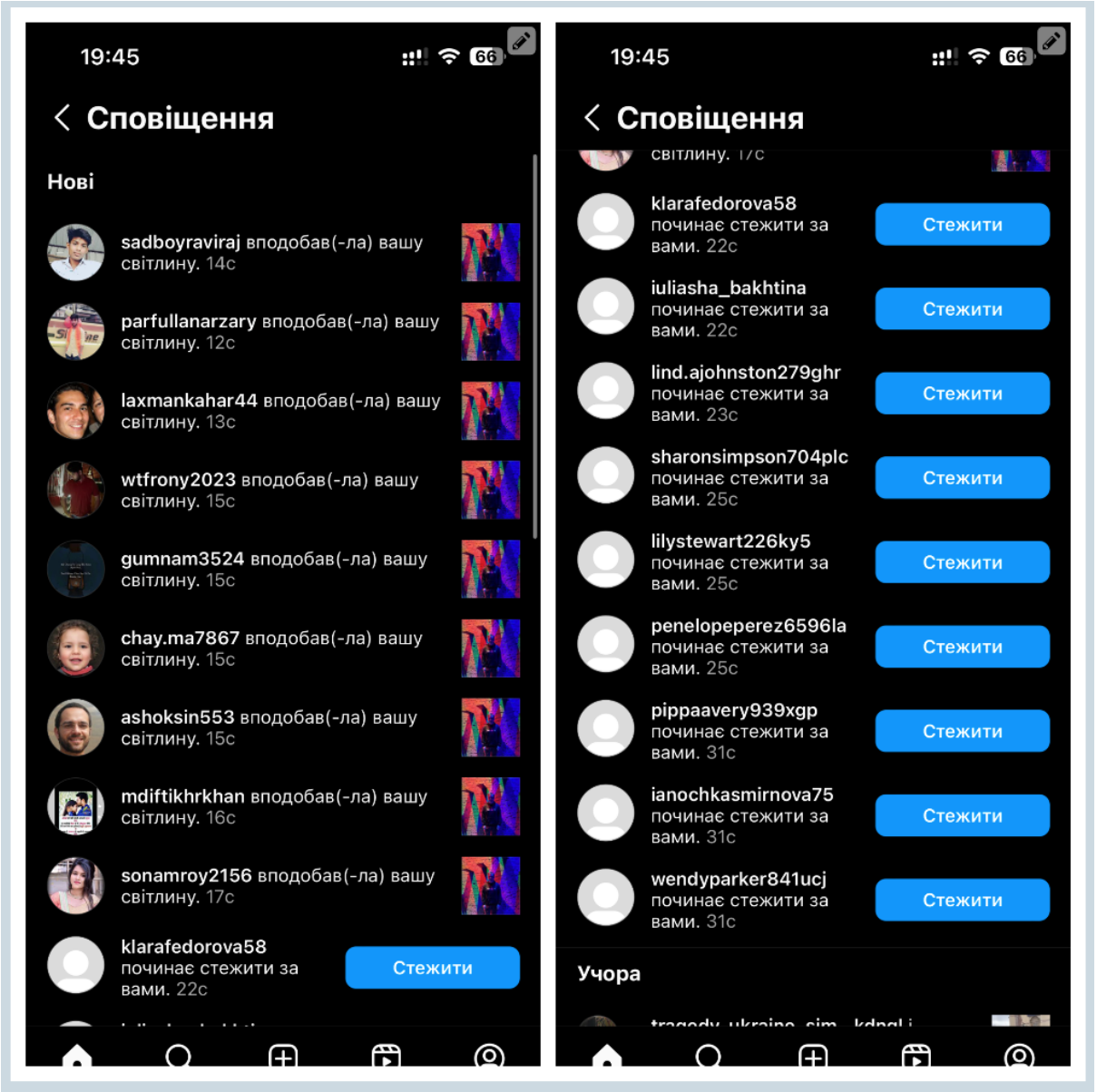

Рисунок 2.3 - Результат накрутки сайтом instasamer.com

З цього можна зробити висновок, що дані сервіси є гарним способом для залучення підписників на фейкову сторінку, але переглянувши підписників такого аккаунта можна одразу зробити припущення про те, що дані користувачі є штучними. Використання такого методу не забезпечить якісної аудиторії, яка буде постійно взаємодіяти з вашою сторінкою, що може негативно вплинути на показники сторінки в соціальній мережі.

2.2 Аналіз дописів користувача

Дописом (постом) в Instagram називають фото або відео, яке публікується в обліковому записі. Вони можуть містити різні хештеги, позначки для просування. В цілому, дописи в соціальній мережі є основним інструментом для ведення та просування сторінки, адже залучення активних та реальних підписників можливе, якщо вони є зацікавленими у публікаціях користувача. Аналіз дописів фейкової сторінки є корисною ознакою для виявлення ознак шахрайства, злочинства, маніпуляцій та інших поганих намірів. Звісно, власник фейкової сторінки усіма способами буде намагатися зробити так, щоб його профіль виглядав реальним. Проте, є декілька маркерів, що можуть підкреслити те, що профіль з великою ймовірністю є фейковим, а саме [8]:

- Активність сторінки. На мою думку, це є головною ознакою, за якою можна зробити висновок про справжність сторінки. Якщо власник сторінки є реальною людиною, то у нього обов'язково є друзі та знайомі, які на нього підписані. Протягом довгого періоду вони взаємодіють з цим профілем шляхом залишку коментарів та лайків на сторінці, позначком власника профілю у власних публікаціях, тощо.
- Періодичність публікацій дописів. Якщо усі дописи користувача були завантажені у один час, чи короткий проміжок - це може свідчити про те, що така сторінка є фейковою, оскільки злочинець таким чином намагається швидко заповнити сторінку контентом.
- Кількість публікацій. Мала кількість дописів, на мою думку, не завжди є ознакою того, що акаунт є фейковим, але якщо досліджувати сторінку комплексно, то такий фактор майже завжди є присутнім.
- Якість фото. Низька якість фото може свідчити про те, що вони не є оригінальними та були завантажені з інших джерел.

- Наповненість дописів. Якщо дописи сторінки не є змістовними, складаються з випадкових фото, наприклад тварин, видатних місць - це може свідчити про ймовірність того, що акаунт є підозрілим. Також вважаю за необхідне проаналізувати текстову складову допису, чи містять вони провокативні чи шокуючі звертання для привернення уваги користувачів.

Одним з варіантів перевірки аккаунт на справжність є змога перевірки оригінальності фото, які присутні у профілі. Це можна зробити за допомогою багатьох безкоштовних онлайн платформ, наприклад, Google Images - пошуковий сервіс, який був заснований та підтримується компанією Google. Він дозволяє знаходити WEB сторінки, що містять шукане фото. Для перевірки даного способу я обрав один з профілів, що підписався на мене у попередньому пункті роботи. Цей профіль містить один допис з фото дівчини.

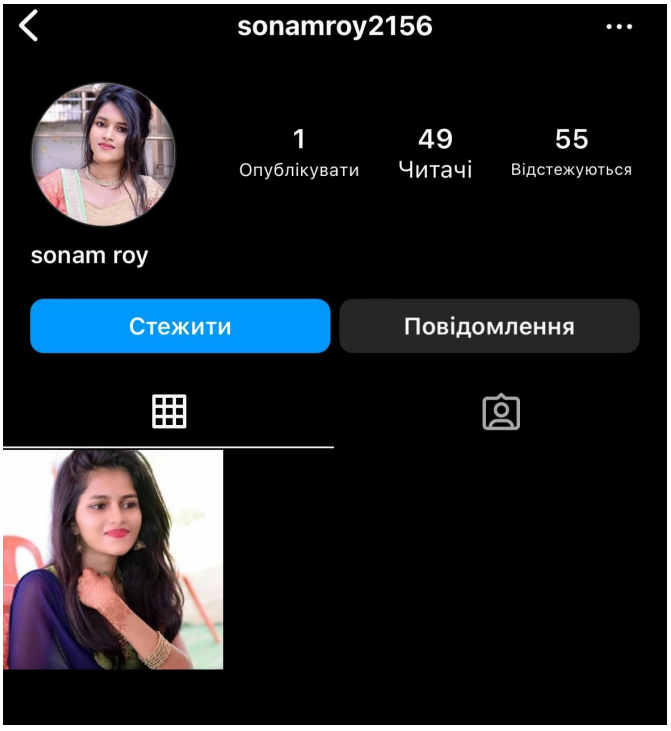

Рисунок 2.4 - Аналізована сторінка

Для подальшого аналізу я завантажую фотографію з цього профілю та відправляю її до сервісу Google Images.

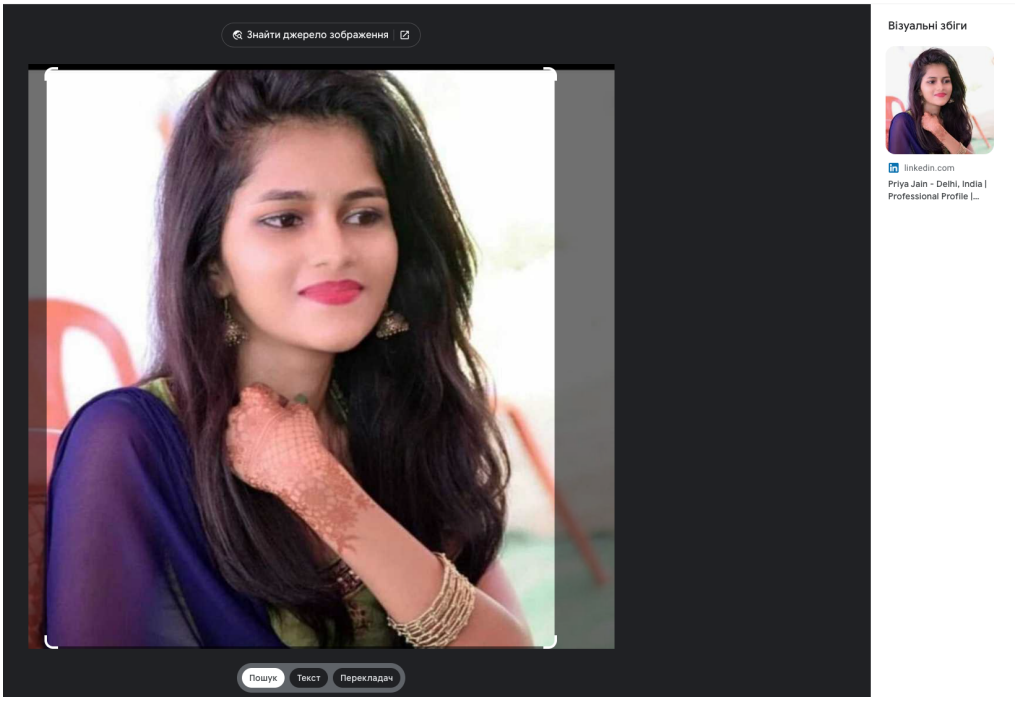

Рисунок 2.5 - Результат пошуку фото за допомогою Google Images

Як можна побачити, ми знайшли аналогічне фото, що використовується у соціальній мережі LinkedIn. Після переходу на дану сторінку ми отримуємо доволі багато інформації з неї, яка допоможе нам відшукати справжню особу на фото.

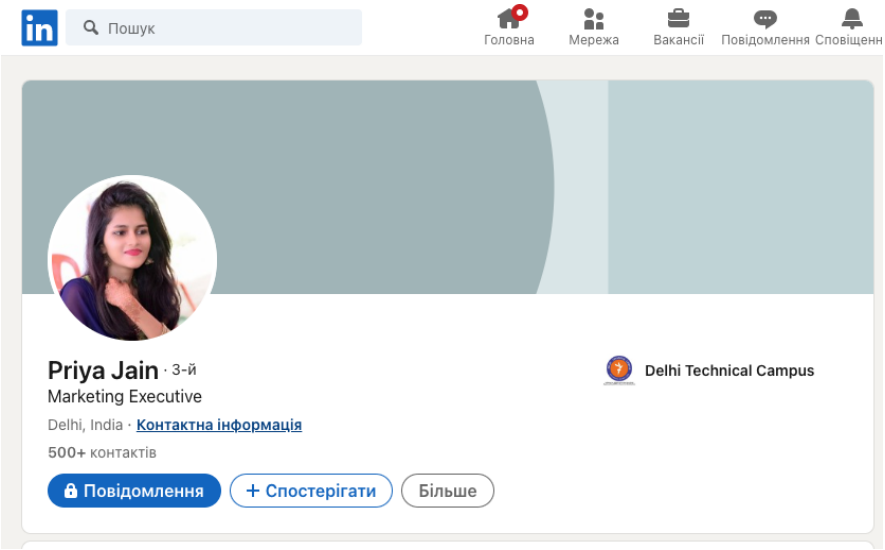

Рисунок 2.6 - Знайдений профіль соцмережі LinkedIn

Серед особистої інформації на даній сторінці можна побачити і’мя та прізвище, місто проживання, освіта у галузі фінансів. Так, зробивши пошук по імені в Instagram, мені вдалось швидко знайти оригінальний профіль, який повністю відповідає інформації, яка вже була знайдена до того використовуючи відкриті джерела:

Рисунок 2.7 - Оригінальний профіль Instagram

Звісно, необхідно взяти до уваги, що пошук людини по фото часто є важкою справою, особливо якщо дане фото є унікальним та не було до цього завантажене на інших Інтернет ресурсах. Проте, це є одним з найпростіших способів перевірки профілю на предмет того чи є він фейком.

2.3 Аналіз оформлення сторінки

Задля проведення аналізу сторінки на справжність можна перевірити дизайн та оформлення сторінки користувачем. Серед найголовніших ознак, на мою думку, можна виділити [9]:

- Наявність аватару на сторінці. Аватар - маленьке кругле зображення, що присутнє у кожному профілю та допомагає ідентифікувати його серед інших під час пошуку та перегляду контенту в Instagram. Його

завжди рекомендується завантажувати задля того, щоб зробити профіль більш привабливим та більш впізнаваним. Відсутність такого зображення може свідчити про те, що сторінка з деякою ймовірністю є не справжньою.

- Наявність оформленої біографії. Біографія (або розділ “Про себе”) - це невеликий текстовий опис того що містить дана сторінка, розповідає інформацію про її володаря. У ній можна вказувати різні подробиці, а саме: місце проживання власника сторінки, його вік, місце роботи, тощо. Наявність посилань у біографії також може свідчити про те, що аккаунт є робочим (тобто магазином для ведення бізнесу)
- Ім’я користувача являє собою унікальний (єдиний у всій мережі) підпис акаунту. Дивлячись на нього теж можна зробити висновок про те, чи є сторінка справжньою. Як вже було сказано мною раніше, фейкові сторінки часто використовують у своєму ім’ї велику кількість цифр. Тому це теж може слугувати одним з маркерів під час аналізу профілів мережі Instagram.
- Приватний профіль - це такий, доступ до якого обмежений для всіх користувачів та дозволений лише для тих, кому дозволив безпосередньо автор. Якщо сторінка є приватною, то це може свідчити про те, що вона є справжньою. Головна причина того, чому такі сторінки існують - бажання ділитися дописами, відео лише з обмеженим колом людей та не дозволяти переглядати її постороннім юзерам.
- Верифікація профілю. Як вже було наведено у першому розділі, наявність синьої галочки для імені сторінки однозначно свідчить про те, що автор сторінки є справжній.

Висновки до розділу 2

Під час роботи над другим розділом дипломної роботи я дослідив головні ознаки фейкових сторінок мережі Instagram. Були розглянуті такі аспекти акаунтів як підписники і підписки користувача, його публікації та загальне оформлення сторінки. Був складений перелік основних маркерів, які будуть взяті за основу для створення алгоритму виявлення сторінок у наступному розділі.

3 РОЗРОБКА ПРОГРАМНОЇ РЕАЛІЗАЦІЇ ТА ЇЇ ТЕСТУВАННЯ

Для реалізації програмного алгоритму виявлення фейкових сторінок у соціальній мережі “Instagram” мною було прийняте рішення скористатися методами машинного навчання для побудови класифікатора, що може прогнозувати те, чи є акаунт справжнім, чи є підробкою. Для досягнення мети була обрана мова програмування Python 3.10.6 - ця мова програмування є однією з найпопулярніших у світі та дозволяє використовувати бібліотеки, які чудово підійдуть під моє завдання. Написання програми буде виконуватися у середовищі програмної розробки PyCharm.

3.1 Використання методів машинного навчання для реалізації алгоритму

У статті від IBM [9] було зазначено, що машинне навчання – це галузь штучного інтелекту (Artificial intelligence) та інформатики, яка зосереджується на використанні даних і алгоритмів для імітації способу навчання людей, поступово покращуючи його точність. Воно ділиться на декілька типів, а саме:

- Машинне навчання з учителем (Supervised machine learning) - такий тип визначається використанням позначених наборів даних для навчання алгоритмів для класифікації даних або точного прогнозування результатів. Після проведення навчання, модель стає готовою до використання на реальних, невивчених до того, прикладах.
- Машинне навчання без учителя (Unsupervised machine learning) - використовує алгоритми машинного навчання для аналізу та

кластеризації непозначених наборів даних. Ці алгоритми виявляють приховані шаблони або групи даних без втручання людини.

- Напівконтрольоване навчання (Semi-supervised machine learning) - є чимось середнім між двома наведеними вище методами. Під час навчання він використовує менший набір даних з мітками, щоб керувати класифікацією та виділенням ознак із більшого набору даних без міток.

Для моєї роботи чудово підійде метод навчання з учителем. До найбільш популярних алгоритмів навчання з учителем відносять:

- Лінійну регресію (linear regression)
- K-найближчих сусідів (K-nn neighbors)
- Дерева рішень (Random Forest)
- Метод опорних векторів (Support Vector Machines)

3.2 Створення навчального набору даних

Для створення навчального набору даних я вирішив написати скрипт мовою Python generate_data.py (повний код наведено в додатку А) який буде записувати дані про користувацький профіль у окремий CSV файл.

Засновуючись на отриманих результатах другого розділу дипломної роботи, я обрав найголовніші ознаки фейкових сторінок, які можливо програмним чином зібрати та продовжити своє дослідження. Тому, стовпці створеного CSV файлу мають такі характеристики:

- Username - ім’я користувача;
- Followers - кількість підписників користувача;
- Follows - кількість підписок користувача;
- Post count - кількість публікацій користувача;
- Full name len - довжина повного імені користувача;
- Biography len - довжина біографії користувача;

- Numbers ratio in username - відношення цифр до літер у імені користувача;
- Has profile picture - наявність аватару;
- Has external url - наявність стороннього посилання у біографії;
- Is fake - чи є користувач фейком;

Для навчання моделі було вирішено заповнити датасет даними, що містять інформацію про 110 реальних користувачів (їх реальність підтверджується тим, що це або мої знайомі, або відомі зірки), а також 110 фейків, які були виявлені через сервіс по накрутці лайків, приклад якого наведений у 1 розділі роботи. Їх користувацькі імена були записані у окремий файл, що містить назву “profiles.txt” на рисунку 3.1 (повний зміст файлу наведений у додатку Б)

Рисунок 3.1 - Приклад імен користувачів з тренувального набору даних

Для подальшого виконання завдання було використано мову програмування Python, та бібліотеки:

- CSV - модуль, який забезпечує читання та запис файлів формату CSV. Такий формат зазвичай використовується для зберігання табличних даних та складається з рядків даних, кожен розділений роздільником.

- Instaloader - це інструмент для завантаження зображень (або відео) разом із їхніми підписами та іншими метаданими з соціальної мережі Instagram.

Використовуючи бібліотеку Instaloader [12] можливо пройтися по кожному користувачеві у списку та записати у файл відповідні дані. Для початку роботи необхідно ввести логін та пароль від облікового запису з якого будуть надсилатися запити до “Instagram” (рис 3.2):

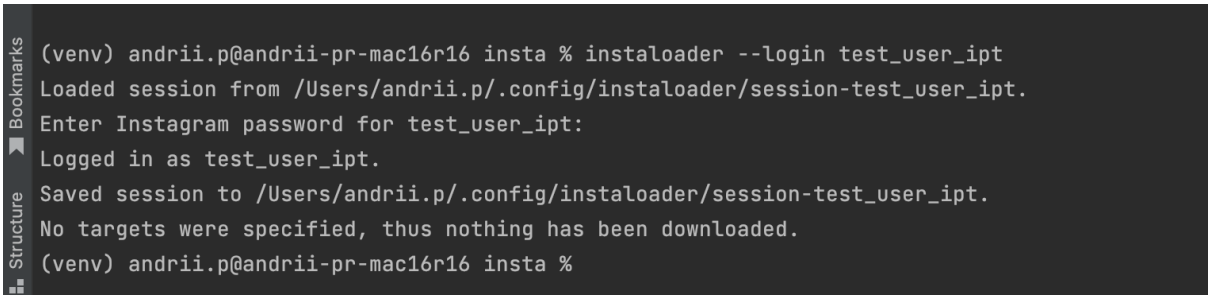

Рисунок 3.2 - Процедура логіну в Instaloader

Після того, як доступ був отриманий стає можливим запустити програму до роботи. На рис.3.3. показано приклад виводу програми під час її виконання:

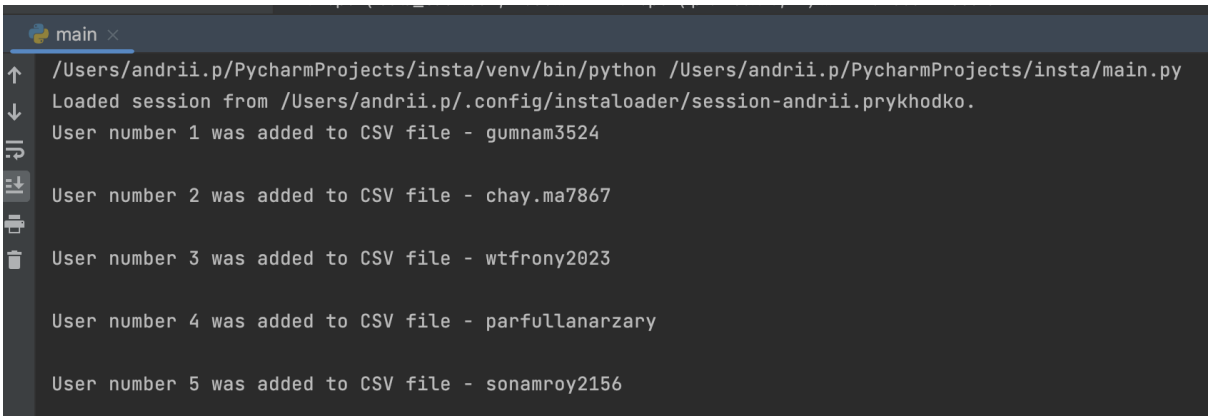

Рисунок 3.3 - Виконання скрипта

Після фінішу програма виводить повідомлення про завершення виконання, а створений датасет можна переглянути у файлі “data.csv”, частина якого наведена на рисунку 3.4 та повністю в додатку В.

```
In [144]: df
```

click to scroll output; double click to hide

	Username	Followers	Follows	Posts count	Full name len	Biography len	Numbers ratio in name	Has profile picture	Has external url	Is fake
0	gumnam3524	51	6	1	0	0	0.40	1	0	1
1	chay.ma7867	13	2	0	0	0	0.36	1	0	1
2	wtfrony2023	54	88	3	17	97	0.36	1	0	1
3	parfullanarzary	15	2	4	16	0	0.00	1	0	1
4	sonamroy2156	56	55	1	9	0	0.33	1	0	1
...	...	...	...	...	...	...	...	...	...	...
215	kavovashe	281	232	5	4	2	0.00	1	0	0
216	nekit_pap	683	607	15	10	89	0.00	1	0	0
217	ta_shcho_vidaye	356	345	92	18	111	0.00	1	0	0
218	sieedykh	419	356	108	13	51	0.00	1	0	0
219	dziub_anet	1913	1025	205	11	102	0.00	1	1	0

220 rows × 10 columns

Рисунок 3.4 - Створений набір даних

3.3 Попередній аналіз даних

Дослідницький аналіз даних є першим кроком у будь-якому процесі аналізу даних. Він дозволяє узагальнити всі основні характеристики даних за допомогою як статистичних, так і графічних засобів. EDA допомагає визначати основні властивості даних, їх розподіл, виявляти аномалії та виявлят головні закономірності [13]. Основні задачі EDA включає наступні пункти:

- Ознайомлення з даними;
- Визначення цільової змінної;
- Візуалізація даних;
- Вибір ознак;

На рис. 3.5 наведено структуру навчального набору даних:

```
In [4]: df.head()
```

Out[4]:

	Username	Followers	Follows	Posts count	Full name len	Biography len	Numbers ratio in name	Has profile picture	Has external url	Is fake
0	gumnam3524	51	6	1	0	0	0.40	1	0	1
1	chay.ma7867	13	2	0	0	0	0.36	1	0	1
2	wtfrony2023	54	88	3	17	97	0.36	1	0	1
3	parfullanarzary	15	2	4	16	0	0.00	1	0	1
4	sonamroy2156	56	55	1	9	0	0.33	1	0	1

```
In [5]: df.info()
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 100 entries, 0 to 99
Data columns (total 10 columns):
 #   Column                  Non-Null Count  Dtype
---  ------                  --------------  -----
 0   Username                100 non-null    object
 1   Followers               100 non-null    int64
 2   Follows                 100 non-null    int64
 3   Posts count             100 non-null    int64
 4   Full name len           100 non-null    int64
 5   Biography len           100 non-null    int64
 6   Numbers ratio in name   100 non-null    float64
 7   Has profile picture     100 non-null    int64
 8   Has external url        100 non-null    int64
 9   Is fake                 100 non-null    int64
dtypes: float64(1), int64(8), object(1)
memory usage: 7.9+ KB
```

Рисунок 3.5 - Структура датасету

З цього можна побачити, що всі колонки окрім “Username” мають числові значення і нам не потрібно додатково їх модифікувати. При побудові моделі колонка з іменами користувачів буде видалена.

Для проведення візуалізації даних було використано бібліотеку мови Python seaborn та matplotlib, які дозволяють дуже просто створити графіки. На рисунку 3.8 наведено графіки розподілу значень серед метрик, за якими буде робитися прогноз про те, чи є сторінка фейком:

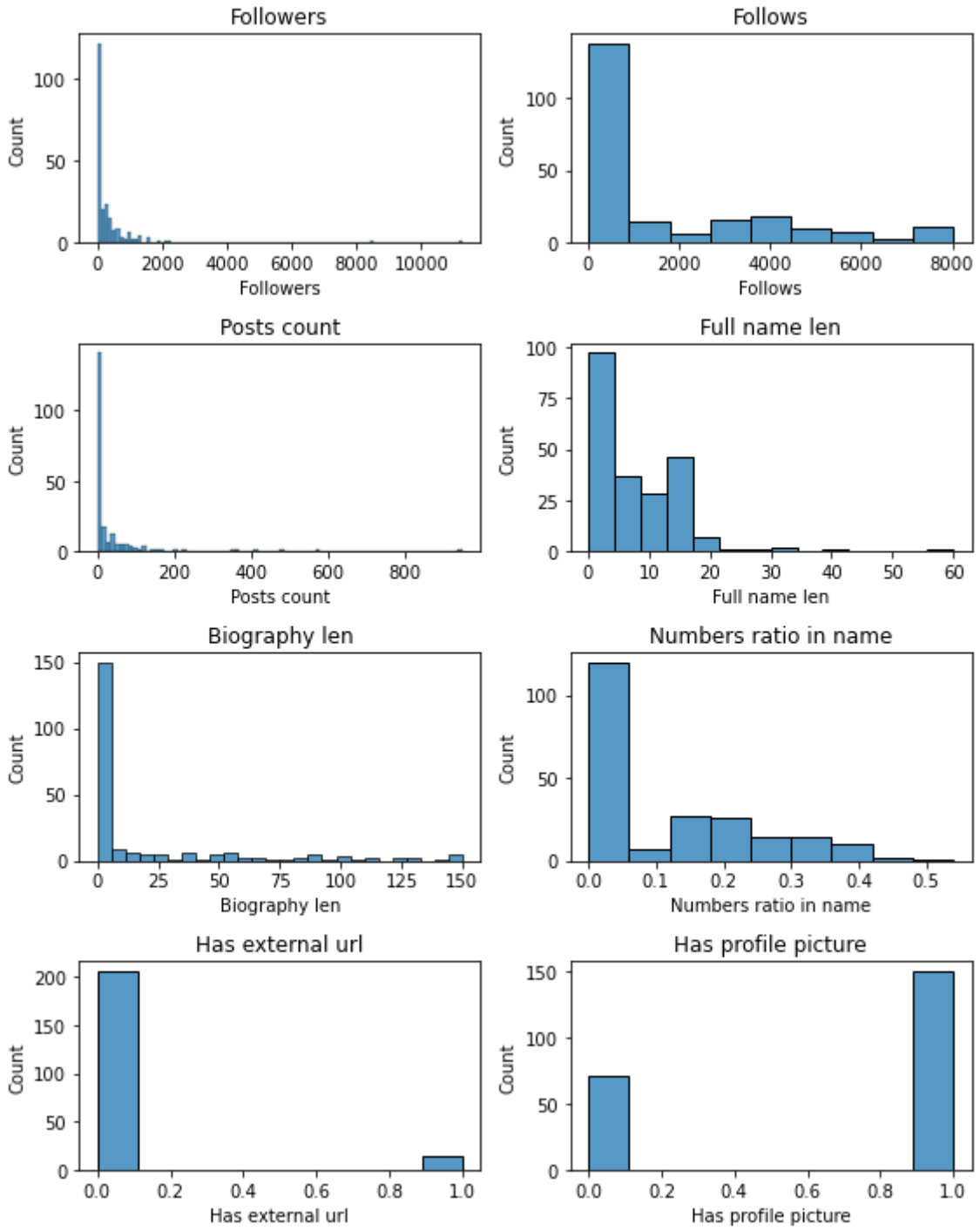

Рисунок 3.6 - Розподіл значень у датасеті

Цільовою змінною у нашому випадку виступає змінна “Is fake” - розподіл якої наведений на рисунку 3.7:

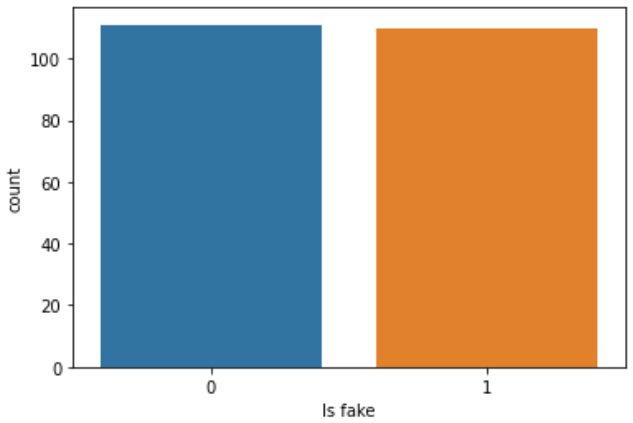

Рисунок 3.7 - Розподіл цільової змінної

Для більш точного аналізу я розподілив набір даних на два в залежності від того чи є сторінка фейком. Це допоможе мені зробити порівняння ознак таких сторінок:

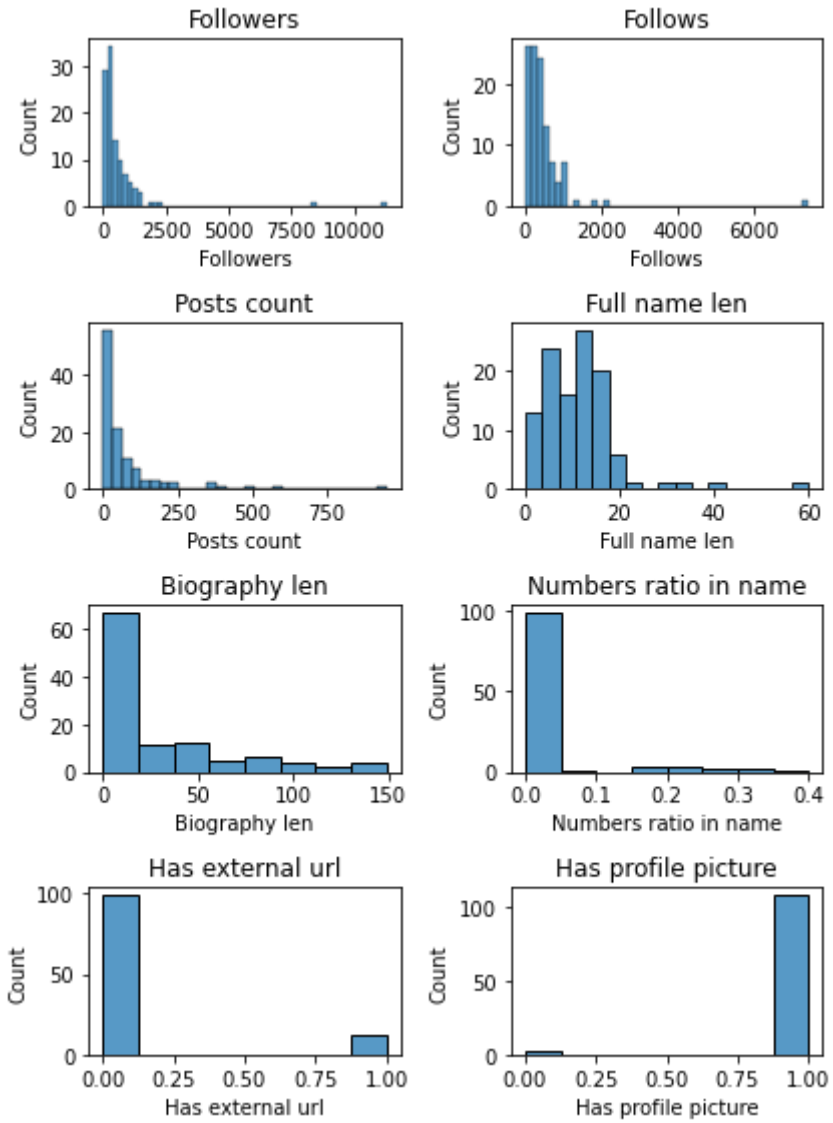

Рисунок 3.8 - Розподіл змінних для справжніх сторінок

Головні ознаки, які можна виділити для справжніх сторінок:

- кількість підписників та підписок мають приблизно рівні значення;
- профілі мають публікації на своїх сторінках;
- Довжини біографії та повного імені розподілені серед сторінок;
- Цифри у іменах користувачів майже завжди відсутні;
- Майже всі профілі мають аватар;

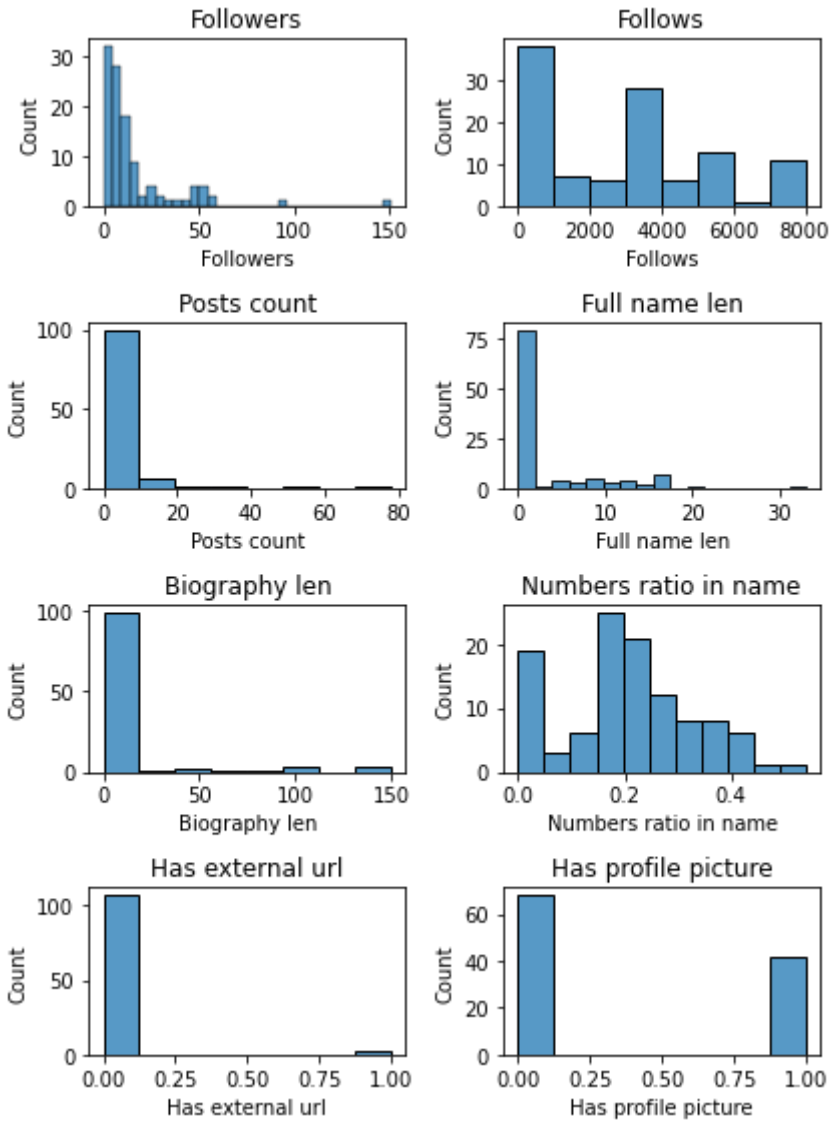

Рисунок 3.9 - Розподіл змінних для фейкових сторінок

Для фейкових сторінок можна однозначно виділити те, що:

- Кількість підписок набагато більша за кількість підписників;
- Як видно з графіків вище, підроблені облікові записи більше співвідношення числових символів в імені користувача облікового запису до їх довжини;
- Більшість підроблених облікових записів мають менше слів опису у своїй біографії;
- Середня кількість постів близька до нуля;

Для того, щоб більш детально проаналізувати залежність змінних одна від одної я скористався кореляційним аналізом. Кореляційний аналіз може бути корисним для визначення того, які змінні впливають на цільову змінну в машинному навчанні, і допомагає зрозуміти, які змінні взаємодіють між собою та як це може вплинути на результат моделювання. [14]. На рисунку 3.10 наведена побудована кореляційна матриця для нашого дослідження:

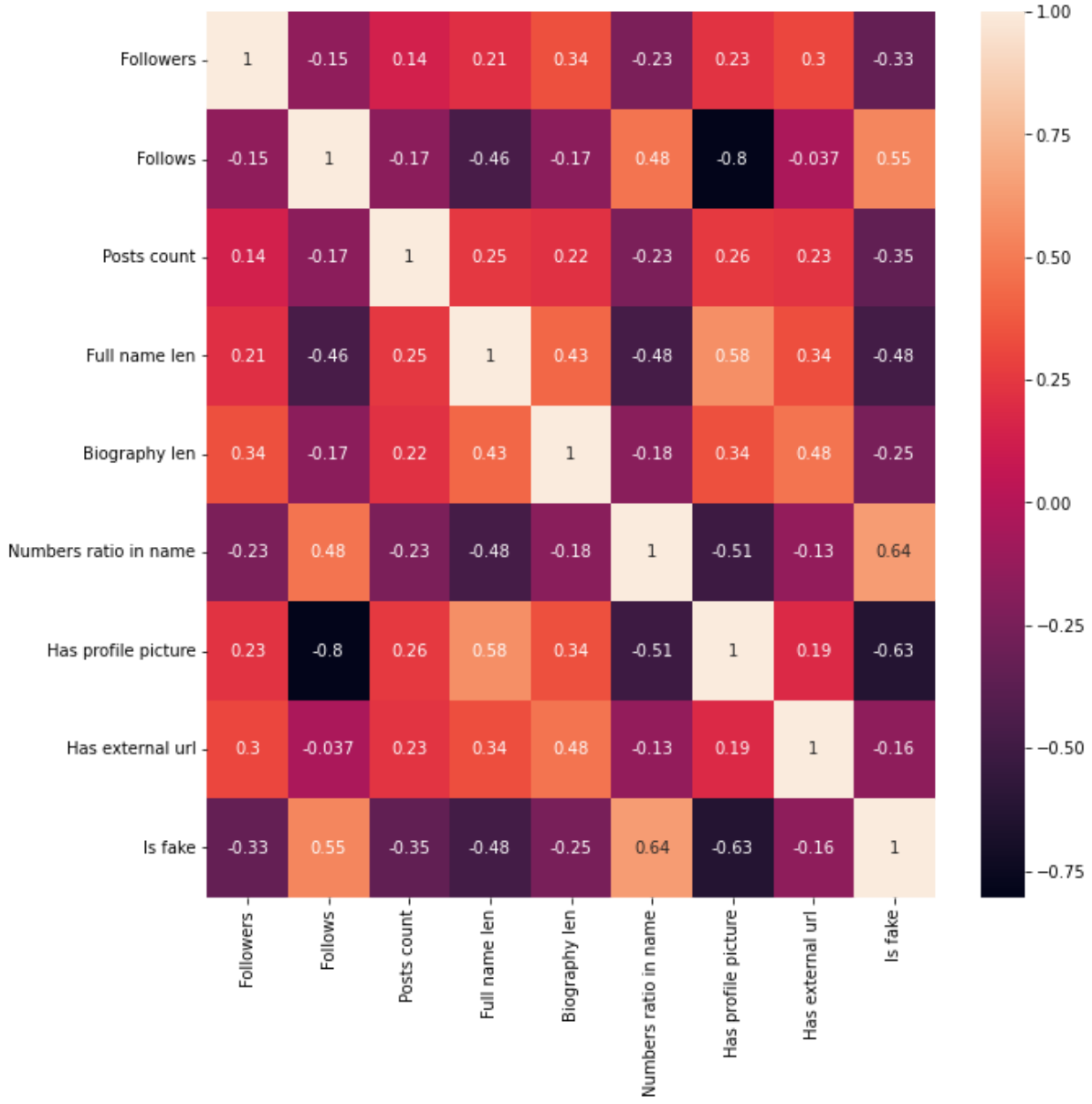

Рисунок 3.10 - Кореляційна матриця датасету

Дана матриця підтверджує те, що:

- Ознака фейкової сторінки є наявність великої кількості цифр у імені користувача;
- Наявність аватарки може свідчити про те, що сторінка є правдивою;

3.4 Побудова моделі

Для побудови моделі було обрано 6 методів машинного навчання, які найкраще підходять для задачі бінарної класифікації:

- Naive bytes;
- K-nn;
- Linear regression;
- Multi-layer Perceptron;
- Support Vector Classification;
- Decision tree;

Отримані метрики точностей побудованих моделей наведені у таблиці 3.1:

Model	Precision	Recall	f1-score
Naive bytes	1	1	1
KNN	0.94	0.94	0.94
LR	1	1	1
MLP	1	0.91	0.95
SVC	1	0.94	0.97
Decision Tree	1	1	1

Таблиця 3.1 - Метрики точностей отриманих моделей

На рисунку 3.11 наведено матриці невідповідностей для побудованих моделей:

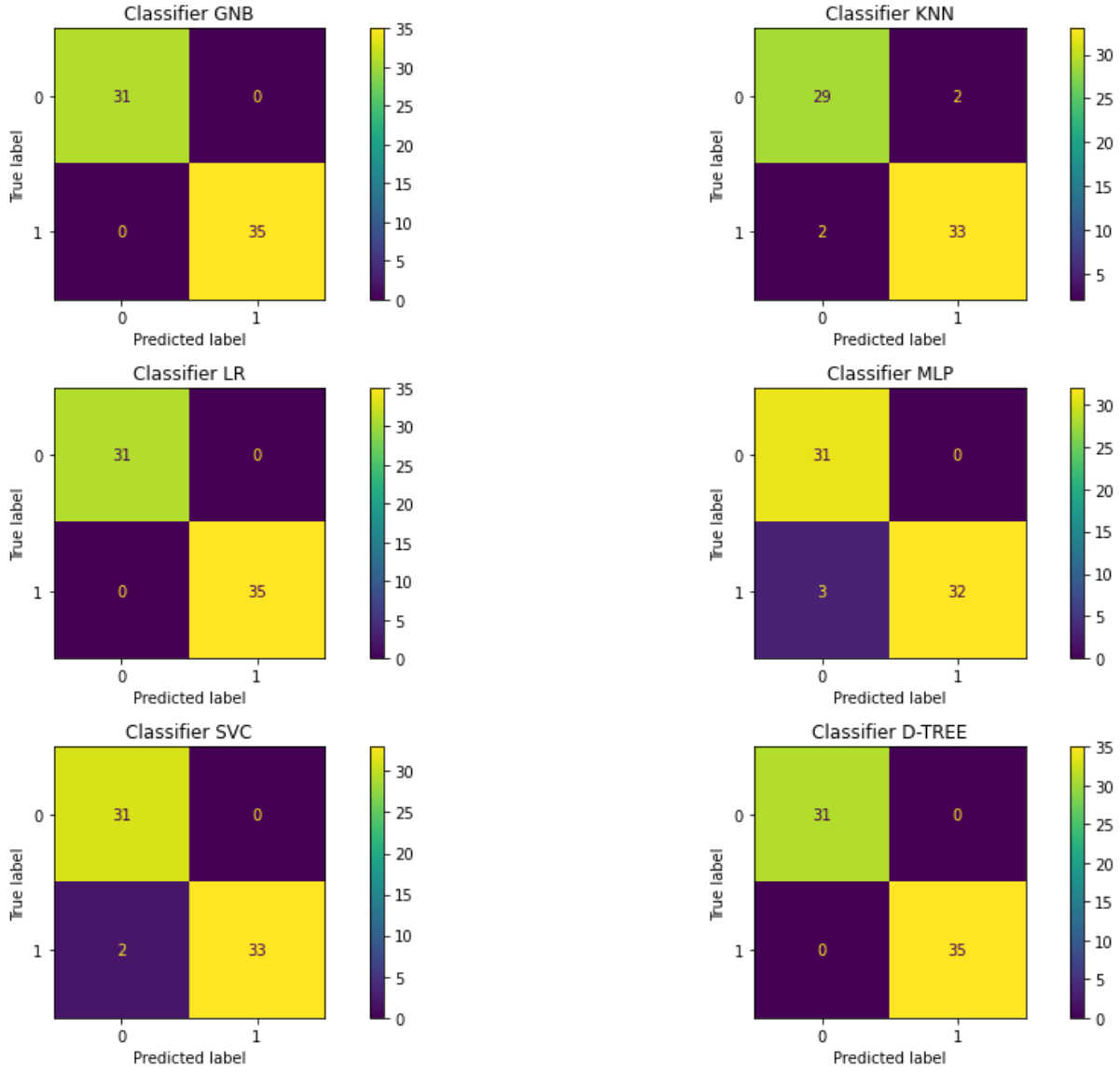

Рис 3.11 - Матриці невідповідностей побудованих моделей

З цього можна зробити висновки, що всі моделі мають високі значення точності, а деякі з них, а саме:

- Naive bytes;
- Linear regression;
- Decision tree;

показали 100% показник точності на обраному наборі даних. Модель з такою точністю на навчальних даних може бути хорошим знаком, але це не обов'язково означає, що модель досконала або буде добре працювати на непередбачуваних даних. Ось кілька моментів, на які мені слід звернути увагу у майбутньому при доопрацюванні мого дослідження для більш досконалої мети:

- Надмірне припасування: Модель, яка досягає 100% точності на навчальних даних, означає, що вона занадто добре вивчила навчальні дані і не може добре узагальнювати нові, невідомі дані. Перенавчання відбувається, коли модель фіксує шум або випадкові коливання в навчальних даних замість того, щоб вивчати основні закономірності.

- Продуктивність тестового набору: Дуже важливо оцінити продуктивність моделі на окремому тестовому наборі, який не використовувався під час навчання. Якщо модель досягає високої точності і на тестовому наборі, це свідчить про те, що модель працює добре і може узагальнювати нові дані.

- Якість даних та упередженість: Ефективність моделі сильно залежить від якості навчальних даних. Якщо навчальні дані є упередженими, неповними або не репрезентативними щодо реальних даних, висока точність моделі може виявитися ненадійною або непридатною для цільової популяції.

- Міркування щодо предметної області: Визначення "хорошої" продуктивності може відрізнятися залежно від предметної області та конкретної проблеми. Деякі області вимагають вищої точності, ніж

інші, і наслідки хибно позитивних або хибно негативних результатів можуть відрізнятися. Важливо враховувати конкретний контекст і вимоги при визначенні того, чи є ефективність моделі хорошою.

3.5 Можливі способи використання моделі

Вважаю, що побудована модель має багато корисних способів для використання як для звичайного користувача, так і для адміністраторів великих сторінок Instagram, які мають велику користувацьку активність протягом дня:

- Часто зловмисники можуть робити бот атаки на профіль - залишати під накручувати підписників. Тим самим мережа може заблокувати профіль, вважаючи його підозріло активни. Так, застосувавши дану модель, як етап перевірки, користувача ми можемо заблокувати його на етапі перших активностей на сторінці.
- Очистка коментарів від ботів. Боти дуже розповсюджений механізм для накрутки коментарів на сторінках. Так, вони можуть використовуватися для поширення фейків чи нагнітання обстановки серед населення. Застосувавши дану модель, ми можемо робити перевірки на те, чи справжній аккаунт та за потреби блокувати його разом з видаленням коментаря.
- Оцінка якості підписників: програма може оцінити якість підписників користувача, аналізуючи їхні профілі, активність залучення. Так ми можемо ідентифікувати облікові записи з високим відсотком неактивних або підозрілих підписників, що вказує на потенційних фальшивих підписників.
- Виявлення надзвичайної активності: програму можна вдосконалити, щоб вона могла відстежувати активність користувачів, наприклад раптове збільшення кількості підписників, нерегулярні шаблони

публікацій або аномальний рівень залучення, щоб ідентифікувати облікові записи, які демонструють підозрілу поведінку, зазвичай пов’язану з підробленими профілями чи діяльністю ботів.

Наприклад, зайшовши на сторінку ministry_of_defense_ua (https://www.instagram.com/ministry_of_defense_ua/) я бачу під одним з постом коментарі, які не містять жодного змісту та інформативного характеру. Після перевірки їх користувачів на справжність я отримав, що два користувачі є фейками (рис. 3.12 та рис. 3.13) і їх коментарі містять провокативний характер, а один з них бажає зробити крадіжку грошей.
Даний експеримент було проведено на багатьох дописах, і модель показала високу точність виявлення фейкових сторінок. Повний програмний код можна переглянути у додатку Г - файл main.py

```
/Users/andrii.p/PycharmProjects/insta/venv/bin/python /Users/andrii.p/PycharmProjects/insta/test.py
Model mas created
Loaded session from /Users/andrii.p/.config/instaloader/session-andrii.prykhodko.
User vetalfreeman26 seems to be FAKE!
User ameliamacdonald76620 seems to be FAKE!


Process finished with exit code 0
```

Рисунок 3.12 - приклад роботи програми

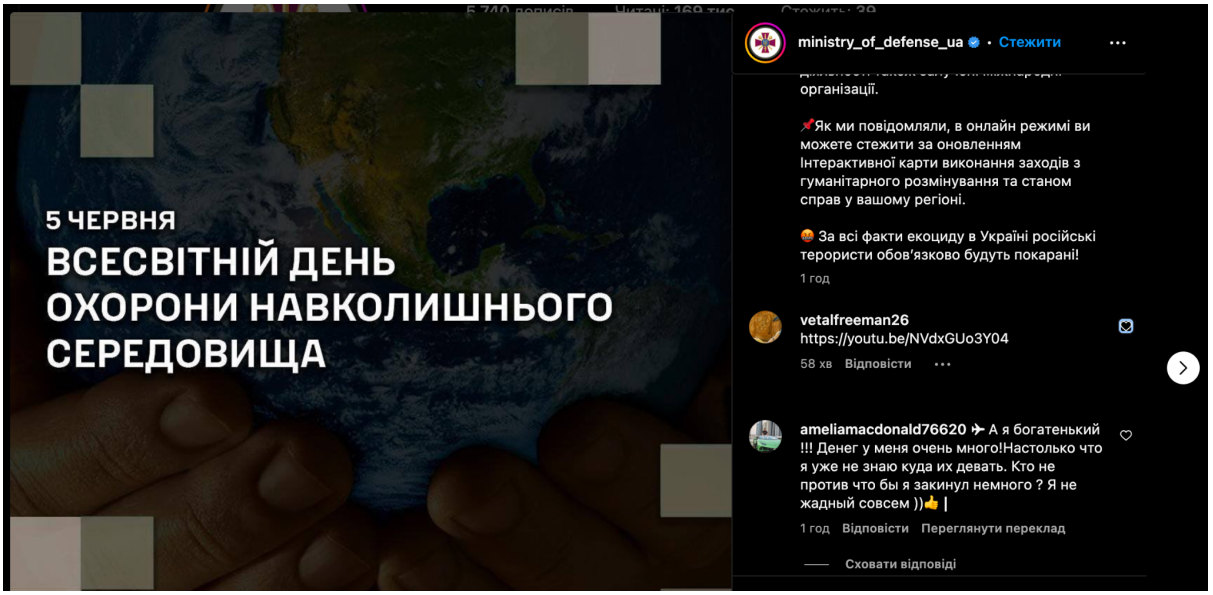

Рисунок 3.13 - Приклад допису, який проходив перевірку

Підсумовуючи, можна сказати, модель показує доволі високу точність і може з легкістю відфільтровувати ботів у соціальних мережах.

Висновки до розділу 3

В даному розділі було теоретично оглянуто можливі інструменти для вирішення поставленої задачі дипломної роботи. Було описано принцип роботи обраного алгоритму, згенеровано навчальний набір даних на основі результатів дослідження у розділі під номером 2. Аналіз 6 побудованих моделей показав, що на даному наборі даних вони всі мають напрочуд високу точність. Було вказано про недоліки, які можуть бути присутні у моделі, зважаючи на 100% точність деяких з них. Було наведено та продемонстровано приклад можливого юзкейсу даної програми. Наведено скріншоти, що підтверджують точність виявлення фейкових сторінок.

ВИСНОВКИ

На сьогоднішній день соціальні мережі стали невід’ємною складовою життя майже кожної людини. В свою чергу, соціальна мережа Instagram, безсумнівно, стала важливою частиною нашого життя, впливаючи на те, як ми спілкуємося, ділимося досвідом і взаємодіємо з навколишнім світом.

Аналіз мережі Інтернет та літературних джерел дав мені змогу навести відомість про природу фейкових сторінок, найчастіші типи атак та наслідки для як для одного окремого користувача, так і для суспільства в цілому, які пов'язані з використанням фейкових сторінок.

На основі опрацьованої мною інформацією, а також власного аналізу соціальної мережі Instagram, в другому розділі дипломної роботи було мною були виділені головні ознаки, за якими можна визначати те, чи є сторінка справжньою. Ці ознаки охоплюють різні частини профілю людини - від кількості її підписників до формату за яким створене її ім’я та дозволять в сукупності зробити припущення про справжність сторінки.

За результатами другого розділу, мною була створена програма, яка може робити прогноз чи є аналізована сторінка фейком. Використання методів машинного навчання зробило можливим реалізацію поставлених переді мною завдань. Аналіз роботи програми показує, що він показує високу точність на реальних прикладах фейкових сторінок та може бути вдосконаленим та опрацьованим мною у подальшому.

Реалізована програмна реалізація повністю відповідає поставленим переді мною завданням і має багато прикладів для використання у реальному житті, наприклад, адміністраторам популярних сторінок - таким чином вони можуть захистити себе від спаму ботів в коментарях чи атак по накрутці підписників. Дана програма може підтримувати на рівні

інформаційну безпеку в соціальних мережах, адже вона дозволяє очищати коментарі від ботів, які можуть розповсюджувати фейкові новини.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Алгоритм виявлення фейкових сторінок фейкових сторінок соціальної мережі “Instagram” / А. Р. Приходько, С. А. Смирнов // XXI Всеукраїнська Науково-практична Конференція Студентів, Аспірантів Та Молодих Вчених , 11-12 травня 2023 р., м. Київ. – 2023. – С. 174-177.
2. Bylestone D. Instagram: What It Is, Its History, and How the Popular App Works. — 2022. — URL: https://www.investopedia.com/articles/investing/102615/story-instagram-rise-1-photo0sharing-app.asp
3. Муджирі Є. Якими соцмережами користуються українці під час війни: статистика. — 2023. — URL: https://speka.media/yakimi-socmerezami-koristuyutsya-ukrayinci-pid-cas-viini-doslidzennya-p22nyp
4. Pelish J. 10 Different Types of Fake Facebook Accounts. — 2014. - URL: https://clickwhisperer.com/2014/04/the-10-types-of-fake-facebook-accounts/
5. Wegerer L. Top Instagram Scams of 2023 and How to Avoid Them. - 2023. - URL: https:vpnoverview.com/privacy/social-media/instagram-scams/
6. Newberry C. Instagram Analytics Explained (Plus 5 Tools for 2023). — 2022. — URL: https://blog.hootsuite.com/instagram-analytics-tools-business/
7. High quality social networks promotion — URL: https://instamer.com/en
8. Demeku A. The Ultimate Guide to Instagram Analytics in 2023. — 2023. — URL: https://later.com/blog/instagram-analytics/

9. Parisi M. 3 Signs That an Instagram Account Is Fake (and How to Stay Safe). — 2022. — URL: https://www.makeuseof.com/signs-of-fake-instagram-accounts/
10. IBM. What is machine learning? — 2022. — URL: https://www.ibm.com/topics/machine-learning
11. Harrison O. Machine Learning Basics with the K-Nearest Neighbors Algorithm. — 2018. — URL:https://towardsdatascience.com/machine-learning-basics-with-the-k-nearest-neighbors-algorithm-6a6e71d01761
12. https://instaloader.github.io/
13. Garwal N. What is EDA? — 2023. — URL: https://www.geeksforgeeks.org/what-is-exploratory-data-analysis/
14. What is a Correlation Matrix? — 2022. — URL: https://www.displayr.com/what-is-a-correlation-matrix/
15. Nguyen X. Understanding the Mean Squared Error. — 2020. — URL: https://medium.com/nothingaholic/understanding-the-mean-squared-error-df41e2c87958
16. Classification: ROC Curve and AUC https://developers.google.com/machine-learning/crash-course/classification/roc-and-auc

ДОДАТОК А

generate_data.py

```
import csv
import instaloader

DEFAULT_PIC =
"44884218_345707102882519_2446069589734326272_n.jpg"



def generate_data():
    # Create an Instaloader instance
    L = instaloader.Instaloader()
    L.load_session_from_file("andrii.prykhodko")




    # Store column headers in a list
    headers = ['Username',
               'Followers',
               'Follows',
               'Posts count',
               'Full name len',
               'Biography len',
               'Numbers ratio in name',
               'Has profile picture',
               'Has external url',
               'Is fake'
               ]
```

```
    # Open a CSV file in write mode
    with open('data_back.csv', mode='w', newline='') as file:
        # Create a CSV writer object
        writer = csv.writer(file)
        # Write the headers to the CSV file
        writer.writerow(headers)
        counter = 0
        # Open a text file containing usernames in read mode
        with open('profiles.txt', 'r') as users:
            # Loop through each username in the text file
            for user in users:
                # Load a profile by its username
                profile = instaloader.Profile.from_username(L.context, user.strip())

                # Check if the profile has a default profile picture or not
                has_profile_pic = 0 if DEFAULT_PIC in profile.profile_pic_url else 1
                # Write the profile data to the CSV file
                writer.writerow([profile.username,
                                 int(profile.followers),
                                 int(profile.followees),
                                 int(profile.mediacount),
                                 len(profile.full_name),
                                 len(profile.biography),
                                 round(len([int(x) for x in profile.username if x.isdigit()]) /
len(profile.username),
                                       2),
                                 has_profile_pic,
                                 0 if profile.external_url is None else 1,
```

```
                    1 if counter < 50 else 0
                    ])
            print('User number {0} was added to CSV file - {1}'.format(counter +
1, user))
            counter += 1

    # Print a message indicating that data has been added to the CSV file
successfully
    print("Data added to CSV file successfully!")



def single_profile(username):
    L = instaloader.Instaloader()
    L.load_session_from_file("andrii.prykhodko")

    profile = instaloader.Profile.from_username(L.context, username.strip())
    has_profile_pic = 0 if DEFAULT_PIC in profile.profile_pic_url else 1

    return [int(profile.followers),
            int(profile.followees),
            int(profile.mediacount),
            len(profile.full_name),
            len(profile.biography),
            round(len([int(x) for x in profile.username if x.isdigit()]) /
len(profile.username), 2),
            has_profile_pic,
            0 if profile.external_url is None else 1,
            ]
```

ДОДАТОК Б

'gumnam3524', 'chay.ma7867', 'wtfrony2023', 'parfullanarzary',
'sonamroy2156', 'gupta2112deepak', 'ashoksin553', 'swyn__416.719',
'ritabariha6', 'aslam_4091', 'test_user_ipt',
'richardgonzalez2042927', 'johnjohnson3224185', 'markgreen0513146',
'margaretbailey9848486', 'emmaunderwood544sxf',
'wandagraham591rc2', 'amy9008whitfhx', 'beking4625439',
'ameliajohnston317oh4', 'andrealee2768ss', 'janeberry7483cw',
'michellemackay285bsy', 'jennifer5829baileyzy',
'irenesanderson54jxq', 'mollypeters42108a', 'fionabower537z9p',
'andreapayne478nct', 'joannebutler973vpk', 'zoeadams618ryw',
'amy5601hernande3716', 'thomasroberts6157419',
'patriciaevansuwmcxhtjpy', 'deborahparkerntpvmzmxqv',
'donaldhillsfptlpcltc', 'maryscottrtosivkfip', 'nuriiaermolaeva20',
'traptrap759', 'mwansahpauline', 'christopherclarkaffoetpkle',
'georgewilliamsvydpzsxbcd', '1farangiz.1', 'kushaneyhern',
'melanie8__riley_', 'karenthomastpfmvcdcre', 'lisasmithawytlmzkbp',
'itzabhishek129', 'forever.anuelxyailin', 'lisapullman9948601',
'amanda9369jonecoe', 'andrii.prykhodko', 'pashtoss', 'cordies_di',
'li.antonenko', 'kateshakhova_', 'tanialisovaia', 'krukovamakeup',
'olesik_antonenko', 'oomelchenko1', 'nekit_pap', 'lomelp_l',
'beiba_pulia', 'mariya500', 'tankeyzz', 'nadiia__kyrylova',
'alina.sk.v', 'lavrenkokate', '_makenzi_', 'l_s_kate',
'antohnys_s', 'may_may1.6', 'allinaa.k', 'oleheida', 'v.solo666',
'milterrr', 'kyzovko', 'dudnikviktoria', 'zelenskayya',
'heavyhipe', 'ddarinka', 'serhii.kuzub', 'vicktorinad',
'mouse_plt', 'kriven_n', 'sosnyuschka', 'dwa.kolory', 'uljana3156',
'pozitiv_22', 'babyannts', 'liliiadovganiuk', 'stovba.vlad',

'vkycno.art', 'vlad_petrash', 'st.files', 'era.1v', 'april_monro',
'gooncharenko', 'polina_rkv', 'andrewtodos', 'slavik_shovak',
'n_zav8', 'olya.nota', 'brat_qk', 'ice_miracle', 'totalikspice',
'aya.kut', 'loofyver', 'littlsun', 'kostya_bay', 'n0m0repain_',
'olexander_y', 'ms.sugar', 'tm_meme_queen', 'lavrenkokate',
'zhurav_natali_', 'criiztz', 'stovba.a', 'sashkohrabar',
'rubalkoi', 'prosto.slogno', 'ann.aheieva', 'elenavedmedenko',
'alina.sk.v', 'lomelp_l', 'a.l.e.s.i.a_iv', 'karlovaska',
'arh1_t1m', 'denismityachkin', 'lu.nnyysvet', 'ilonarss',
'vanyakozyr', 'elenagranko', 'michaelsomko', 'valerysikt',
's_fes17', 'e.v.j.e.n.i.y.a', 'solo_way_v', 'olef.ira',
'natdzhakeli', 'kirpichik_vira', 'ivankarybitskaia', 'olya_mzs',
'roma_polonskiy', 'brewer.maks_', 'svitlana_baidan',
'liliialapteva', 'yaa.m_', 'albert_ponomarenko', 'alefan_03',
'na_ta_lisova', 'julia_kriukova', 'nicolachurchill7tuz',
'oliviapeters653p3p', 'eltu.rner805xq8', 'carolinelyman81fbp',
'melaniemackenzie9045sh', 'lindabond545osk', 'rebeccawatson881kqr',
'juliapaige528avl', 'traceypaterson624edo', 'yvonnetucker504c7g',
'clairemitchell408hvs', 'felicitygraham3096905',
'virginiaarnold30exq', 'lilywhite462lci', 'wendywalsh184uny',
'olivianorth363phm', 'wendymacdonald177gvt', 'emilymorrison101jid',
'suenewman268gs', 'audr.eylambert882okm',
'm_r_wanted_the_rohan_nishad___', 'kushvahaprempal749',
'asl___ake', 'farh.ankhan2042', 'joangonzalez73ydw',
'anna.chapman149jer', 'sallygraham6695866', 'beha.rris741061',
'carolinelewis349mze', 'dorothyallan5441756', 'nancymills4449521',
'muhammadsaqib8148', 'eyyupozdolanbay', 'lasfashionb',
'justin_losxx', 'michellemurray8191280', 'jenniferoliver8914352',
'alisonhardacre5742143', 'lindamathis107sp4', 'ruthmarshall118ud9',

'oliv.iagonzalez54h6v', 'leah.turner513rih', 'play.beats.co', 'ballon.uz', 'dj_samir_officle', 'leoraktdz5220', 'amy5363whitewz', 'victoriahoward2742ck', 'diana7675garciflo', 'sueslater907gr6', 'graceoliver275boq', 'felicitynorth1772be', 'jenn.iferdavies820ozy', 'bettyhardacre792hvn', 'alexandragill3676c', 'virg.iniapeake5480bt', 'wand.aquinn827pjv', 'laurajohnston681yxb', 'vanessarandall9028ih', 'soph.iealsop655tn', 'danny__force', 'dmytro.danilin', 'nik_tishkov', 'maschreider', 'kavovashe', 'nekit_pap', 'ta_shcho_vidaye', 'sieedykh', 'dziub_anet'profiles.txt

ДОДАТОК В

data.csv

Username,Followers,Follows,Posts count,Full name len,Biography len,Numbers ratio in name,Has profile picture,Has external url,Is fake

gumnam3524,51,6,1,0,0,0.4,1,0,1

chay.ma7867,13,2,0,0,0,0.36,1,0,1

wtfrony2023,54,88,3,17,97,0.36,1,0,1

parfullanarzary,15,2,4,16,0,0.0,1,0,1

sonamroy2156,56,55,1,9,0,0.33,1,0,1

gupta2112deepak,31,8,0,16,0,0.27,1,0,1

ashoksin553,0,0,0,9,0,0.27,1,0,1

swyn__416.719,22,8,0,9,36,0.46,1,0,1

ritabariha6,0,4,0,11,0,0.09,1,0,1

aslam_4091,46,22,0,12,0,0.4,1,0,1

test_user_ipt,0,0,1,0,0,0.0,0,0,1

richardgonzalez2042927,0,550,13,0,0,0.32,1,0,1

johnjohnson3224185,0,550,13,0,0,0.39,1,0,1

markgreen0513146,0,155,13,0,0,0.44,1,0,1

margaretbailey9848486,9,3584,0,0,0,0.33,0,0,1

emmaunderwood544sxf,6,3620,0,0,0,0.16,0,0,1

wandagraham591rc2,7,3487,0,0,0,0.24,0,0,1

amy9008whitfhx,3,3732,0,0,0,0.29,0,0,1

beking4625439,3,1569,0,0,0,0.54,0,0,1

ameliajohnston317oh4,10,3820,0,0,0,0.2,0,0,1

andrealee2768ss,11,3742,0,0,0,0.27,0,0,1

janeberry7483cw,15,3587,0,0,0,0.27,0,0,1

michellemackay285bsy,5,3607,0,0,0,0.15,0,0,1

jennifer5829baileyzy,7,1187,0,0,0,0.2,0,0,1

irenesanderson54jxq,1,1422,0,0,0,0.11,0,0,1
mollypeters42108a,3,3455,0,0,0,0.29,0,0,1
fionabower537z9p,3,3599,0,0,0,0.25,0,0,1
andreapayne478nct,4,3624,0,0,0,0.18,0,0,1
joannebutler973vpk,2,3214,0,0,0,0.17,0,0,1
zoeadams618ryw,1,1567,0,0,0,0.21,0,0,1
amy5601hernande3716,4,1863,0,0,0,0.42,0,0,1
thomasroberts6157419,0,548,13,0,0,0.35,1,0,1
patriciaevansuwmcxhtjpy,8,0,0,8,0,0.0,1,0,1
deborahparkerntpvmzmxqv,7,0,0,7,0,0.0,1,0,1
donaldhillsfptlpcltc,8,0,0,6,0,0.0,1,0,1
maryscottrtosivkfip,8,0,0,4,0,0.0,1,0,1
nuriiaermolaeva20,1,0,0,16,0,0.12,1,0,1
traptrap759,4,0,0,0,0,0.27,1,0,1
mwansahpauline,11,84,4,16,0,0.0,1,0,1
christopherclarkaffoetpkle,7,0,0,11,0,0.0,1,0,1
georgewilliamsvydpzsxbcd,5,0,0,6,0,0.0,1,0,1
1farangiz.1,49,6,3,2,0,0.18,1,0,1
kushaneyhern,52,4,3,13,0,0.0,1,0,1
melanie8__riley_,9,0,0,0,0,0.06,1,0,1
karenthomastpfmvcdcre,8,0,0,5,0,0.0,1,0,1
lisasmithawytlmzkbp,0,0,0,4,0,0.0,1,0,1
itzabhishek129,50,4,0,13,0,0.21,1,0,1
forever.anuelxyailin,4,4,3,14,58,0.0,1,0,1
lisapullman9948601,25,7400,0,0,0,0.39,0,0,1
amanda9369jonecoe,1,3209,0,0,0,0.24,0,0,1
andrii.prykhodko,217,407,60,16,28,0.0,1,0,0
pashtoss,111,114,5,5,0,0.0,0,0,0
cordies_di,113,102,2,18,0,0.0,1,0,0

li.antonenko,1077,1022,172,5,39,0.0,1,0,0
kateshakhova_,390,353,1,13,7,0.0,1,0,0
tanialisovaia,655,372,198,12,57,0.0,1,0,0
krukovamakeup,1311,866,145,29,132,0.0,1,1,0
olesik_antonenko,405,228,96,18,0,0.0,1,0,0
oomelchenko1,108,364,25,6,37,0.08,1,0,0
nekit_pap,684,592,15,10,89,0.0,1,0,0
lomelp_l,635,314,33,8,88,0.0,1,0,0
beiba_pulia,1308,2136,116,14,45,0.0,1,1,0
mariya500,178,199,52,6,0,0.33,1,0,0
tankeyzz,861,186,222,0,9,0.0,1,0,0
nadiia__kyrylova,184,56,16,15,0,0.0,1,0,0
alina.sk.v,333,160,35,17,1,0.0,1,0,0
lavrenkokate,1532,649,41,7,123,0.0,1,0,0
makenzi,15,1,0,16,65,0.0,0,0,0
l_s_kate,412,437,9,13,8,0.0,1,0,0
antohnys_s,295,382,2,5,23,0.0,1,0,0
may_may1.6,195,355,12,10,0,0.2,1,0,0
allinaa.k,1180,302,57,41,48,0.0,1,0,0
oleheida,193,299,2,12,0,0.0,1,0,0
v.solo666,2287,37,9,16,17,0.33,1,0,0
milterrr,86,134,9,0,25,0.0,1,0,0
kyzovko,600,459,3,17,0,0.0,1,0,0
dudnikviktoria,425,1091,25,16,0,0.0,1,0,0
zelenskayya,290,118,0,5,17,0.0,1,0,0
heavyhipe,234,111,40,17,0,0.0,1,0,0
ddarinka,139,39,578,16,17,0.0,1,0,0
serhii.kuzub,140,77,0,12,0,0.0,1,0,0
vicktorinad,493,971,357,8,54,0.0,1,0,0

mouse_plt,777,458,18,10,80,0.0,1,0,0
kriven_n,2177,7422,159,17,101,0.0,1,1,0
sosnyuschka,168,73,11,11,6,0.0,1,0,0
dwa.kolory,289,346,63,60,149,0.0,1,0,0
uljana3156,59,1303,10,6,140,0.4,1,0,0
pozitiv_22,625,416,3,2,0,0.2,1,0,0
babyannts,1131,869,11,7,29,0.0,1,0,0
liliiadovganiuk,471,500,35,14,0,0.0,1,0,0
stovba.vlad,397,129,4,11,0,0.0,1,0,0
vkycno.art,11263,508,64,21,132,0.0,1,1,0
vlad_petrash,529,395,5,11,20,0.0,1,0,0
st.files,358,581,80,33,27,0.0,1,1,0
era.1v,552,143,0,6,0,0.17,1,0,0
april_monro,378,565,229,11,20,0.0,1,1,0
gooncharenko,450,144,15,16,11,0.0,1,0,0
polina_rkv,960,592,88,7,48,0.0,1,0,0
andrewtodos,1309,743,33,13,58,0.0,1,1,0
slavik_shovak,95,90,41,13,15,0.0,1,0,0
n_zav8,121,141,72,0,0,0.17,1,0,0
olya.nota,274,313,45,4,48,0.0,1,0,0
brat_qk,118,133,2,7,1,0.0,1,0,0
ice_miracle,95,92,409,15,0,0.0,1,0,0
totalikspice,966,650,38,11,0,0.0,1,0,0
aya.kut,139,640,47,12,54,0.0,1,0,0
loofyver,184,417,89,15,0,0.0,1,0,0
littlsun,254,255,124,15,0,0.0,1,0,0
kostya_bay,1161,550,38,10,49,0.0,1,0,0
n0m0repain_,129,97,2,7,0,0.18,1,0,0
olexander_y,22,15,0,9,3,0.0,1,0,0

ms.sugar,376,1884,94,0,55,0.0,1,0,0
tm_meme_queen,571,590,13,5,0,0.0,1,0,0
lavrenkokate,1544,661,42,7,123,0.0,1,0,0
zhurav_natali_,1009,359,86,0,36,0.0,1,0,0
criiztz,151,202,18,9,8,0.0,1,0,0
stovba.a,1514,998,42,12,0,0.0,1,0,0
sashkohrabar,609,491,20,0,2,0.0,0,0,0
rubalkoi,336,666,5,8,0,0.0,1,0,0
prosto.slogno,226,333,6,8,0,0.0,1,0,0
ann.aheieva,922,798,368,22,74,0.0,1,1,0
elenavedmedenko,323,409,59,16,0,0.0,1,0,0
alina.sk.v,339,157,36,17,1,0.0,1,0,0
lomelp_l,638,334,36,8,88,0.0,1,0,0
a.l.e.s.i.a_iv,172,83,4,6,0,0.0,1,0,0
karlovaska,380,305,28,8,6,0.0,1,0,0
arh1_t1m,90,188,0,3,0,0.25,1,0,0
denismityachkin,440,366,8,8,10,0.0,1,0,0
lu.nnyysvet,811,781,3,5,0,0.0,1,0,0
ilonarss,270,123,1,5,0,0.0,1,0,0
vanyakozyr,762,1050,3,2,0,0.0,1,0,0
elenagranko,201,293,127,13,0,0.0,1,0,0
michaelsomko,8418,164,28,5,40,0.0,1,0,0
valerysikt,279,268,7,5,0,0.0,1,0,0
s_fes17,322,495,47,8,81,0.29,1,0,0
e.v.j.e.n.i.y.a,236,103,0,0,0,0.0,1,0,0
solo_way_v,496,522,7,12,0,0.0,1,0,0
olef.ira,1346,956,15,5,66,0.0,1,0,0
natdzhakeli,767,439,81,16,19,0.0,1,0,0
kirpichik_vira,433,307,118,17,111,0.0,1,1,0

ivankarybitskaia,962,230,79,8,2,0.0,1,0,0
olya_mzs,997,806,949,13,53,0.0,1,0,0
roma_polonskiy,296,260,4,16,2,0.0,1,0,0
brewer.maks_,329,370,6,7,10,0.0,1,0,0
svitlana_baidan,248,206,106,15,0,0.0,1,0,0
liliialapteva,335,481,10,13,0,0.0,1,0,0
yaa.m_,246,69,2,0,0,0.0,1,0,0
albert_ponomarenko,264,212,65,19,13,0.0,1,1,0
alefan_03,205,296,478,0,0,0.22,1,0,0
na_ta_lisova,344,333,155,14,0,0.0,1,0,0
olesik_antonenko,405,228,96,18,0,0.0,1,0,0
julia_kriukova,496,445,166,14,25,0.0,1,1,0
nicolachurchill7tuz,13,3911,0,0,0,0.05,0,0,1
oliviapeters653p3p,13,3839,0,0,0,0.22,0,0,1
eltu.rner805xq8,14,2703,0,0,0,0.27,0,0,1
carolinelyman81fbp,11,4102,0,0,0,0.11,0,0,1
melaniemackenzie9045sh,5,3872,0,0,0,0.18,0,0,1
lindabond545osk,1,2669,0,0,0,0.2,0,0,1
rebeccawatson881kqr,7,5244,0,0,0,0.16,0,0,1
juliapaige528avl,2,5423,0,0,0,0.19,0,0,1
traceypaterson624edo,5,5535,0,0,0,0.15,0,0,1
yvonnetucker504c7g,8,5614,0,0,0,0.22,0,0,1
clairemitchell408hvs,3,6387,0,0,0,0.15,0,0,1
felicitygraham3096905,2,3695,0,0,0,0.33,0,0,1
virginiaarnold30exq,3,5208,0,0,0,0.11,0,0,1
lilywhite462lci,11,5740,0,0,0,0.2,0,0,1
wendywalsh184uny,11,4119,0,0,0,0.19,0,0,1
olivianorth363phm,12,3915,0,0,0,0.18,0,0,1
wendymacdonald177gvt,15,4129,0,0,0,0.15,0,0,1

emilymorrison101jid,4,5398,0,0,0,0.16,0,0,1

suenewman268gs,1,5509,0,0,0,0.21,0,0,1

audr.eylambert882okm,0,5341,0,0,0,0.15,0,0,1

m_r_wanted_the_rohan_nishad___,57,1534,2,33,150,0.0,1,1,1

kushvahaprempal749,92,2972,5,16,39,0.17,1,0,1

asl___ake,5,684,6,5,0,0.0,1,0,1

farh.ankhan2042,21,1047,37,12,18,0.27,1,0,1

joangonzalez73ydw,3,4985,0,0,0,0.12,0,0,1

anna.chapman149jer,6,2266,0,0,0,0.17,0,0,1

sallygraham6695866,11,7024,0,0,0,0.39,0,0,1

beha.rris741061,12,7233,0,0,0,0.4,0,0,1

carolinelewis349mze,1,2241,0,0,0,0.16,0,0,1

dorothyallan5441756,8,7543,0,0,0,0.37,0,0,1

nancymills4449521,5,4796,0,0,0,0.41,0,0,1

muhammadsaqib8148,9,3052,50,14,103,0.24,1,0,1

eyyupozdolanbay,16,369,0,16,0,0.0,1,0,1

lasfashionb,151,783,12,20,52,0.0,1,0,1

justin_losxx111,7,71,1,0,13,0.2,1,0,1

michellemurray8191280,2,3098,0,0,0,0.33,0,0,1

jenniferoliver8914352,11,7511,0,0,0,0.33,0,0,1

alisonhardacre5742143,11,7616,0,0,0,0.33,0,0,1

lindamathis107sp4,5,5869,0,0,0,0.24,0,0,1

ruthmarshall118ud9,15,7677,0,0,0,0.22,0,0,1

oliv.iagonzalez54h6v,8,3550,0,0,0,0.15,0,0,1

leah.turner513rih,14,3489,0,0,0,0.18,0,0,1

play.beats.co,10,595,15,11,83,0.0,1,0,1

ballon.uz12345,8,3474,78,9,150,0.35,1,1,1

dj_samir_officle,50,229,20,0,149,0.0,1,0,1

leoraktdz5220,10,70,0,0,109,0.31,1,1,1

amy5363whitewz,13,5325,0,0,0,0.29,0,0,1
victoriahoward2742ck,23,4768,0,0,0,0.2,0,0,1
diana7675garciflo,25,2901,0,0,0,0.24,0,0,1
sueslater907gr6,26,3229,0,0,0,0.27,0,0,1
graceoliver275boq,36,3299,0,0,0,0.18,0,0,1
felicitynorth1772be,53,3671,0,0,0,0.21,0,0,1
jenn.iferdavies820ozy,29,5343,0,0,0,0.14,0,0,1
bettyhardacre792hvn,45,3182,0,0,0,0.16,0,0,1
alexandragill3676c,15,5025,0,0,0,0.22,0,0,1
virg.iniapeake5480bt,38,3025,0,0,0,0.2,0,0,1
wand.aquinn827pjv,5,7857,0,0,0,0.18,0,0,1
laurajohnston681yxb,15,8024,0,0,0,0.16,0,0,1
vanessarandall9028ih,11,8015,0,0,0,0.2,0,0,1
soph.iealsop655tn,5,8015,0,0,0,0.18,0,0,1
danny__force,123,243,16,13,0,0.0,1,0,0
dmytro.danilin,344,287,10,14,2,0.0,1,0,0
nik_tishkov,60,273,0,14,0,0.0,1,0,0
maschreider,95,132,0,0,0,0.0,1,0,0
kavovashe,281,232,5,4,2,0.0,1,0,0
nekit_pap,683,607,15,10,89,0.0,1,0,0
ta_shcho_vidaye,356,345,92,18,111,0.0,1,0,0
sieedykh,419,356,108,13,51,0.0,1,0,0
dziub_anet,1913,1025,205,11,102,0.0,1,1,0

ДОДАТОК Г

main.py

```
import matplotlib.pyplot as plt
import pandas as pd
import seaborn as sns
from sklearn.model_selection import train_test_split
from sklearn.neighbors import KNeighborsClassifier
from sklearn.metrics import confusion_matrix, accuracy_score,
mean_squared_error
from generate_dataset import single_profile
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import plot_confusion_matrix
from sklearn.pipeline import make_pipeline
from sklearn.preprocessing import StandardScaler
from sklearn.neural_network import MLPClassifier
from sklearn.svm import SVC
from sklearn.linear_model import LogisticRegression
from sklearn.naive_bayes import GaussianNB



def dataset_info(data):
    df = pd.read_csv(data)
    print(df.info())
    print(df.head())

print("/*********************************************************/"
)
```

```
def visualize_data(data, features):
    df = pd.read_csv(data)
    fig, axes = plt.subplots(4, 2, figsize=(10, 12))

    axes = axes.flatten()

    for i, fea in enumerate(features):
        ax = axes[i]
        sns.histplot(x=fea, data=df, ax=ax)
        ax.set_title(fea)

    plt.tight_layout()

    plt.savefig("visualize.jpg")
    print("Please check result in visualize.jpg")

print("/*******************************************************/"
)



def split_features(data):
    df = pd.read_csv(data)
    df = df.drop('Username', axis=1)  # not necessary
    X = df.drop('Is fake', axis=1)
    y = df['Is fake'].values
    print("Features were chose")
    return X, y
```

```
def heatmap(data):
    plt.figure(figsize=(10, 10))
    cm = data.corr()
    ax = plt.subplot()
    sns.heatmap(cm, annot=True, ax=ax)
    plt.savefig("heatmap.jpg")
    print("Please check result in heatmap.jpg")

print("/*******************************************************/"
)


def split_test_train(X, y):
    print("Dataset was split into test and train")
    return train_test_split(X, y, test_size=0.3, random_state=0)


def create_model(X_train, y_train):
    classifier = KNeighborsClassifier(n_neighbors=9)
    print("Model mas created")
    return classifier.fit(X_train, y_train)


def make_prediction(classifier, X_test):
    return classifier.predict(X_test)


def conf_matr(y_test, y_pred):
```

```
    print("Confusion matrix is:")

    # Assuming you have already defined y_test and y_pred
    cm = confusion_matrix(y_test, y_pred)
    print(cm)


def calculate_accur(y_test, y_pred):
    print("Model accuracy score = {0}; "
          "Model MSE = {1}".format(accuracy_score(y_test, y_pred)*100,
mean_squared_error(y_test, y_pred)))


def make_prediction_for_account(classifier, account):
    data = single_profile(account)
    pred = classifier.predict([data])
    if pred == [0]:
        print("User {0} seems to be REAL!".format(account))
    else:
        print("User {0} seems to be FAKE!".format(account))


def build_models():
    classifier_knn = KNeighborsClassifier(n_neighbors=5)
    classifier_knn.fit(X_train, y_train)

    classifier_lr = LogisticRegression(random_state=0,
max_iter=500).fit(X_train, y_train)
    y_pred_lr = classifier_lr.predict(X_test)
```

```
    classifier_mlp = MLPClassifier(random_state=1, max_iter=300).fit(X_train,
y_train)
    y_pred_mlp = classifier_mlp.predict(X_test)

    classifier_gnb = GaussianNB().fit(X_train, y_train)
    y_pred_gnb = classifier_gnb.predict(X_test)

    classifier_tree = DecisionTreeClassifier(random_state=0).fit(X_train, y_train)
    y_pred_tree = classifier_tree.predict(X_test, check_input=True)

    classifier_svc = make_pipeline(StandardScaler(),
SVC(gamma='auto')).fit(X_train, y_train)
    y_pred_svc = classifier_svc.predict(X_test)

    return [classifier_gnb, classifier_knn, classifier_lr, classifier_mlp,
classifier_svc, classifier_tree]



def matrix():
    # Create a figure with subplots
    fig, axes = plt.subplots(nrows=3, ncols=2, figsize=(15, 10))
    classifiers_list = build_models()
    classifiers_names = ["GNB", "KNN", "LR", "MLP", "SVC", "D-TREE"]

    ax = axes[0, 0]
    plot_confusion_matrix(classifiers_list[0], X_test, y_test, ax=ax)
    ax.set_title('Classifier GNB')
    ax.set_xlabel('Predicted label')
```

```
    ax.set_ylabel('True label')


    for i in range(1, 6):

        row = i // 2
        col = i % 2


        ax = axes[row, col]
        plot_confusion_matrix(classifiers_list[i], X_test, y_test, ax=ax)
        ax.set_title(f'Classifier {classifiers_names[i]}')
        ax.set_xlabel('Predicted label')
        ax.set_ylabel('True label')


    plt.tight_layout()

    plt.show()


if __name__ == '__main__':
    dataset = "/Users/andrii.p/PycharmProjects/insta/data.csv"

    dataset_info(dataset)

    visualize_data(dataset, [
        'Followers',
        'Posts count',
```

```
    'Full name len',
    'Biography len',
    'Has profile picture',
    'Has external url'])

X, y = split_features(dataset)

heatmap(X)

X_train, X_test, y_train, y_test = split_test_train(X, y)

models = build_models()
matrix()

make_prediction_for_account(models[1], 'aevozovski')
```