

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
КАФЕДРА ІНФОРМАТИКИ І КОМП'ЮТЕРНИХ НАУК
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ
і контрольні завдання до виконання лабораторних робіт,
практичних (семінарських) занять

Риск-моніторинг в соціальних мережах

для здобувачів	Першого курсу
підготовки	другого (магістерського) рівня
галузі знань	F (12) Інформаційні технології
спеціальності	F3 (122) Комп'ютерні науки
освітньо-професійної програми	Консолідована інформація
факультету	Інформаційних технологій та дизайну

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ і контрольні завдання до виконання лабораторних робіт, практичних (семінарських) занять з навчальної дисципліни **Риск-моніторинг в соціальних мережах** фахівців на другому магістерському рівні вищої освіти спеціальності: F3 (122) Комп'ютерні науки

РОЗРОБНИКИ: Наталя Корніловська к.т.н., доц.

РЕЦЕНЗЕНТ: Світлана Вишемирська к.т.н., доц.

Затверджено на засіданні кафедри І та КН

Протокол №6 від 10.03.2026

В.о. зав. каф. І та КН к.м.н., доц. _____ Світлана Моїсеєнко

Відповідальний за випуск Наталя Корніловська к.т.н., доц.

Узгоджено з навчально-методичним відділом

Реєстраційний номер № 32/076-01.04.2026

ВСТУП ДО КОМПЛЕКСУ ЛАБОРАТОРНИХ РОБІТ

Цифрова трансформація суспільства перетворила соціальні мережі на одне з найвпливовіших середовищ формування суспільної думки, ділової репутації та інформаційного простору. Сьогодні жодна організація - незалежно від її масштабу, галузі чи географії - не може дозволити собі ігнорувати процеси, що відбуваються у цифровому середовищі. Репутаційні ризики, кризи довіри, дезінформаційні кампанії та некерований вірусний контент здатні за лічені години завдати шкоди, на подолання якої підуть роки.

Даний комплекс лабораторних робіт присвячений ризик-моніторингу соціальних мереж - дисципліні, що поєднує методи аналізу даних, комп'ютерні технології та управлінські підходи задля своєчасного виявлення, оцінки та нейтралізації загроз у цифровому середовищі. Комплекс розроблено для студентів спеціальності 122 «Комп'ютерних наук», які набувають практичних навичок роботи з реальними даними, інструментами моніторингу та алгоритмами аналізу тональності.

Комплекс охоплює увесь цикл роботи з репутаційними ризиками: від базового розуміння природи ризику та методів його виявлення - через мережний аналіз зв'язків між акторами цифрового простору - до побудови повноцінної автоматизованої системи моніторингу з п'ятишаровою архітектурою. Кожна наступна робота спирається на знання, здобуті в попередніх, формуючи цілісну компетентність фахівця у сфері цифрової безпеки та управління репутацією.

Актуальність тематики комплексу зумовлена кількома чинниками. По-перше, стрімким зростанням кількості кризових випадків у соціальних мережах: за даними міжнародних досліджень, понад 70% репутаційних криз сьогодні беруть початок саме у соціальних медіа. По-друге, дефіцитом фахівців, здатних не лише користуватися готовими інструментами моніторингу, а й розуміти їхню внутрішню логіку, критично оцінювати результати та вдосконалювати системи під конкретні задачі. По-третє, специфікою українського інформаційного середовища, де поряд зі стандартними маркетинговими ризиками наявні виклики, пов'язані з інформаційними операціями, дезінформацією та цілеспрямованими кампаніями в умовах воєнного часу.

Окремої уваги заслуговує правовий та етичний вимір ризик-моніторингу. Збір і обробка даних у соціальних мережах здійснюються в умовах дедалі жорсткішого регуляторного середовища: вимоги GDPR, умови використання платформ та етичні стандарти роботи з персональними даними формують обмеження, що безпосередньо впливають на проектування систем моніторингу. Фахівець, який не враховує ці обмеження, ризикує не лише отримати юридичні санкції, а й завдати репутаційної шкоди самій

організації. Тому правовий та етичний аудит є невід'ємною складовою професійної компетентності у цій сфері.

Не менш важливим є розуміння кризового виміру моніторингу. Виявлення ризику - лише перший крок; не менш критичним є вміння швидко та злагоджено реагувати на кризову ситуацію. Розробка Crisis Playbook, формування антикризових комунікаційних стратегій і побудова чітких протоколів реагування дозволяють організації діяти не хаотично, а системно - навіть в умовах гострого інформаційного тиску та обмеженого часу на прийняття рішень.

Виконуючи лабораторні роботи, студент послідовно освоює: методологію ідентифікації та класифікації репутаційних ризиків; кількісні метрики оцінки репутаційного стану бренду (NSS, SOV, CV, ER); інструменти мережного аналізу для виявлення ключових акторів і центрів впливу в соціальних мережах; технічні підходи до збору, зберігання та обробки великих масивів неструктурованих даних із соціальних платформ; алгоритми аналізу тональності тексту та методи їхньої адаптації до україномовного контенту; принципи побудови та візуалізації аналітичних дашбордів; основи правового та етичного аудиту систем моніторингу відповідно до вимог GDPR і умов використання соціальних платформ.

Завершуючи комплекс, студент набуває не лише технічних навичок, а й аналітичного мислення: вміння бачити за числами на дашборді реальні процеси, ставити під сумнів методологію збору даних, враховувати контекст і робити обґрунтовані висновки. Ці компетентності є затребуваними як у галузі інформаційної безпеки та кризових комунікацій, так і в широкому спектрі IT-спеціалізацій, де робота з даними та розуміння соціальних процесів стають дедалі важливішими.

ЗМІСТ

Лабораторна робота № 1. Аналіз репутаційних ризиків у соціальних мережах: ідентифікація, моніторинг та оцінка наслідків

Студенти навчаються виявляти репутаційні ризики для реальних українських брендів за допомогою інструментів Google Alerts та Social Searcher. Розраховуються ключові метрики: Net Sentiment Score (NSS), Share of Voice (SOV), Crisis Velocity та Engagement Rate. Паралельно аналізується реальний кризовий кейс із побудовою хронології подій та розробкою антикризової стратегії.

Лабораторна робота № 2. Мережний аналіз у риск-моніторингу соціальних мереж

Робота присвячена аналізу зв'язків між учасниками цифрового простору - виявленню лідерів думок, ключових вузлів впливу та центрів поширення інформації у соціальних мережах. Студенти застосовують інструменти мережного аналізу, щоб зрозуміти, як негативний контент поширюється через конкретних акторів і де його найефективніше зупиняти.

Лабораторна робота № 3–4. Побудова власної системи моніторингу соціальних мереж на основі п'ятишарової архітектури

Студенти самостійно проєктують і реалізують повноцінну автоматизовану систему моніторингу з використанням безкоштовних інструментів. Система будується за п'ятишаровою архітектурою - від збору даних із соціальних платформ до аналізу тональності тексту та візуалізації результатів на аналітичному дашборді.

Лабораторна робота № 5–6. Розробка Crisis Playbook та антикризова комунікаційна стратегія

Робота є практичним продовженням теми кризового менеджменту: студенти розробляють детальний Crisis Playbook - покроковий протокол реагування на репутаційну кризу в соціальних мережах. Також формується повноцінна антикризова комунікаційна стратегія з визначенням ролей, каналів та часових рамок реагування.

Лабораторна робота № 7–10. Правовий і етичний аудит моніторингу соціальних мереж

Студенти проводять комплексний правовий аудит систем моніторингу на відповідність вимогам GDPR та умовам використання платформ (ToS). За результатами аудиту розробляється Ethical Monitoring Charter - внутрішній нормативний документ організації, а також план реагування на витік даних (Data Breach Response Plan).

ЛАБОРАТОРНА РОБОТА № 1. Аналіз репутаційних ризиків у соціальних мережах: ідентифікація, моніторинг та оцінка наслідків.

ВСТУП.

Уявіть ситуацію: популярний ресторан у Києві отримав серію негативних відгуків у Facebook та Google Maps. За 48 годин кількість негативних публікацій зросла в 15 разів, відвідуваність впала на 40%, а місцеві телеканали взяли інтерв'ю у незадоволених клієнтів. Це і є репутаційна криза в соціальних мережах.

Для студентів спеціальності F3 (122) «Комп'ютерні науки» ці навички є особливо важливими, адже IT-компанії та цифрові сервіси надзвичайно вразливі до репутаційних атак у соціальних мережах. Витік даних, помилка в роботі застосунку або скандальний пост одного співробітника можуть миттєво спричинити хвилю негативу, яка знищить довіру користувачів.

Репутаційний ризик - це загроза іміджу організації, бренду або особи, що виникає через негативний контент, події або поведінку, яка стає публічно відомою через соціальні мережі та інші цифрові канали, і може спричинити значні фінансові та нематеріальні втрати.

За визначенням Базельського комітету з банківського нагляду (2021), репутаційний ризик - це ризик виникнення збитків або недоотримання запланованих доходів внаслідок формування у суспільстві негативного уявлення про організацію.

Ключові характеристики репутаційних ризиків:

Асиметрія - репутацію будують роками, а зруйнувати можна за одну ніч. Дослідження MIT (Vosoughi et al., 2021) довело, що неправдива інформація у Twitter/X поширюється в 6 разів швидше, ніж правдива.

Каскадний ефект - репутаційна криза тягне за собою фінансові (падіння акцій, відтік клієнтів), операційні (звільнення співробітників) та юридичні (штрафи, позови) наслідки.

Глобальність - у цифровому середовищі локальний скандал може стати міжнародним за лічені години.

Складність вимірювання - репутація є нематеріальним активом, тому її пошкодження важко виразити в точних цифрах.

Мета роботи

Мета лабораторної роботи - навчитися виявляти репутаційні ризики до того, як вони переростуть у кризу, вимірювати їхній масштаб за допомогою реальних метрик (NSS, SOV, CV, ER) та розробляти обґрунтовані антикризові стратегії. Робота формує практичні

компетентності у сфері риск-моніторингу соціальних мереж, необхідні фахівцям спеціальності 122 Комп'ютерні науки.

Класифікація репутаційних ризиків

Репутаційні ризики класифікують за різними критеріями. Найважливіша класифікація - за типом контенту, що генерує загрозу:

Тип репутаційного ризику	Опис	Реальний приклад
Негативні відгуки та скарги клієнтів	Масове незадоволення продуктом або сервісом	Хвиля 1-зіркових відгуків про Nova Poshta після затримки посилок у 2022 р.
Viral-скандали	Миттєве вірусне поширення компрометуючого відео чи фото	Відео з некоректною поведінкою співробітника United Airlines (2017)
Фейки та дезінформація	Поширення брехливих або спотворених новин	Фальшиві чутки про банкрутство ПриватБанку у Facebook (2016)
Скандали з персоналом	Публічне розкриття неетичної поведінки співробітників	Розголос про дискримінаційний внутрішній чат у відомій компанії
Product fails	Публічні дефекти або небезпека продукції	Samsung Galaxy Note 7 - відкликання через вибухи батарей (2016)
Атаки тролів та хейтерів	Організовані кампанії ненависті в соцмережах	Координоване нападання на офіційні сторінки українських брендів
Витік персональних даних	Компрометація конфіденційної інформації клієнтів	Штраф Meta у розмірі 1,2 млрд євро за GDPR (2023 р.)

Стадії розвитку репутаційної кризи

Репутаційна криза проходить шість послідовних стадій:

Стадія 1 - Передкризова (latent stage). Існують передумови для кризи, але вони ще не є публічними. На цьому етапі ризик можна виявити за допомогою моніторингу. Приклад: незадоволені клієнти пишуть скарги у закриті групи, але поки не публічно.

Стадія 2 - Тригерна подія (trigger event). Відбувається конкретна подія або публікується контент, який запускає кризу. Приклад: один вірусний відеозапис потрапляє у Twitter/X.

Стадія 3 - Ескалація (escalation). Контент починає поширюватися в соціальних мережах через репости, хештеги, коментарі та підхоплення медіа.

Стадія 4 - Пік кризи (peak). Максимальний обсяг обговорення та найбільші фінансові втрати. Саме на цій стадії найчастіше падають акції компанії.

Стадія 5 - Затухання (declining). Інтерес аудиторії знижується, але репутаційні «шрами» залишаються в пошукових системах.

Стадія 6 - Посткризовий стан (post-crisis). Організація або відновлює довіру (якщо правильно відреагувала), або продовжує нести втрати.

Ключові метрики репутаційних ризиків

Для кількісного вимірювання репутаційних ризиків використовують такі метрики:

Метрика	Формула	Що означає
Net Sentiment Score (NSS)	$NSS = ((\text{Позитивні} - \text{Негативні}) / \text{Загальна кількість}) \times 100\%$	Загальний тон згадок. Значення нижче -20% свідчить про кризу
Share of Voice (SOV)	$SOV = (\text{Згадки бренду} / \text{Усі згадки у категорії}) \times 100\%$	Частка обговорення бренду серед конкурентів
Crisis Velocity (CV)	$CV = \text{Кількість нових згадок за 1 годину}$	Швидкість поширення кризи. >500 згадок/год - критичний рівень
Engagement Rate (ER)	$ER = (\text{Реакції} + \text{Коментарі} + \text{Репости}) / \text{Охоплення} \times 100\%$	Рівень залученості аудиторії до контенту про бренд

Наведені у таблиці метрики є основним інструментарієм для кількісної оцінки репутаційних ризиків. Розглянемо кожну з них детальніше.

Net Sentiment Score (NSS) - Індекс тональності згадок. Це головна метрика репутаційного здоров'я бренду. Вона показує, наскільки позитивно або негативно аудиторія говорить про компанію у соціальних мережах. Уявіть, що про бренд написали 100 людей: 40 - позитивно, 20 - негативно, 40 - нейтрально. $NSS = ((40 - 20) / 100) \times 100\% = 20\%$. Шкала інтерпретації: значення від $+50\%$ і вище свідчить про відмінну репутацію; від $+20\%$ до $+50\%$ - хорошу; від 0% до $+20\%$ - нейтральну, що потребує уваги; нижче 0% - небезпечну зону; нижче -20% - активну репутаційну кризу, що вимагає негайного реагування.

Share of Voice (SOV) - Частка голосу бренду. Ця метрика показує, яку частку від усіх розмов у своїй галузі або ринковій категорії займає конкретний бренд. Наприклад, якщо про мобільних операторів загалом написали 10 000 разів за місяць, а про Kyivstar - 3 000 разів, то $SOV = (3000 / 10\,000) \times 100\% = 30\%$. Чим вищий SOV, тим помітніший бренд на тлі конкурентів. Водночас різке зростання SOV може свідчити не про позитивну популярність, а про скандал - тому завжди аналізують SOV разом із NSS.

Crisis Velocity (CV) - Швидкість поширення кризи. Показує, наскільки швидко негативний контент поширюється у соціальних мережах. Вимірюється кількістю нових згадок за одну годину. Якщо у звичайний день бренд отримує 10–20 згадок на годину, а після інциденту їх кількість стрибнула до 600 - це чіткий сигнал вірусної кризи. Пороговим критичним значенням вважається понад 500 нових згадок за годину: саме тоді необхідно негайно активувати антикризовий план. Кейс United Airlines (2017) є класичним прикладом: протягом перших двох годин після публікації відео Crisis Velocity перевищила 2 000 згадок на годину.

Engagement Rate (ER) - Коефіцієнт залученості аудиторії. Показує, яка частка людей, що побачили публікацію, відреагувала на неї (поставила лайк, залишила коментар або зробила репост). Висока залученість навколо негативного контенту є одним із ранніх сигналів репутаційного ризику - це означає, що аудиторія не просто переглядає критичні публікації, а активно їх поширює. Наприклад, ER = 8% для негативного відгуку є тривожним показником: зазвичай звичайні публікації мають ER 1–3%.

Усі чотири метрики використовуються у комплексі: жодна з них окремо не дає повної картини репутаційного стану бренду. Наприклад, якщо NSS = –30% (кризовий рівень), але Crisis Velocity = 15 згадок на годину, то криза є серйозною, але повільною - є час на підготовлену відповідь. Якщо ж NSS = –30% і водночас CV = 800 згадок на годину - це вірусна катастрофа, що вимагає реакції протягом перших 30 хвилин.

Реальні приклади для розуміння теми

Приклад 1 - Міжнародний: United Airlines (2017). Пасажира силоміць видалили з літака, відео потрапило у Twitter. За 24 години акції компанії впали на 4%, капіталізація зменшилась приблизно на 1 млрд доларів. Джерело: The Guardian, <https://www.theguardian.com/business/2017/apr/11/united-airlines-boss-deeply-apologises> (дата доступу: 2025).

Приклад 2 - Міжнародний: Meta (Facebook), штраф GDPR (2023). Ірландський регулятор DPC оштрафував Meta на 1,2 млрд євро за незаконну передачу персональних даних громадян ЄС до США. Це найбільший GDPR-штраф в історії. Джерело: GDPR Enforcement Tracker, <https://www.enforcementtracker.com> (дата доступу: 2025).

Приклад 3 - Ukrainian: ПриватБанк (2016–2017). Після оголошення про націоналізацію банку в Facebook та Telegram миттєво поширились фейки про «крах банку». Сотні тисяч людей стояли в чергах до банкоматів. НБУ та банк були змушені цілодобово спростовувати фейки через офіційні сторінки. Джерело: Економічна правда, <https://www.epravda.com.ua/news/2016/12/19/614700/> (дата доступу: 2025).

Приклад 4 - Ukrainian: Rozetka (2020–2021). Під час пандемії хвиля скарг на затримки доставки в Facebook та Google Maps спричинила зниження рейтингу у пошуку. Компанія

оперативно відповіла публічними заявами та ввела систему компенсацій - це дозволило стабілізувати репутацію впродовж кількох тижнів. Джерело: <https://rozetka.com.ua> (офіційний сайт), дата доступу: 2025.

ПРАКТИЧНІ ЗАВДАННЯ

Лабораторна робота складається з трьох практичних завдань, усі з яких присвячені виключно репутаційним ризикам у соціальних мережах. Кожне завдання виконується індивідуально відповідно до варіанту, виданого викладачем.

ЗАВДАННЯ 1. Налаштування системи моніторингу бренду (35 балів)

Опис завдання: налаштуйте систему моніторингу для реального бренду відповідно до вашого варіанту. Використовуйте безкоштовні онлайн-інструменти, зафіксуйте результати та розрахуйте Net Sentiment Score.

Список брендів для моніторингу (варіанти 1–10):

Варіант	Бренд	Галузь
1	Rozetka (rozetka.ua)	Е-commerce Україна
2	Nova Poshta (novaposhta.ua)	Логістика Україна
3	Kyivstar (kyivstar.ua)	Телеком Україна
4	Monobank (monobank.ua)	Фінтех Україна
5	Ukrzaliznytsia (uz.gov.ua)	Транспорт Україна
6	Epicentr (epicentrk.ua)	Рітейл Україна
7	Vodafone Ukraine (vodafone.ua)	Телеком Україна
8	АТБ-Маркет (atbmarket.com)	Рітейл Україна
9	ПриватБанк (privatbank.ua)	Банківський сектор
10	iHerb (iherb.com)	Міжнародний e-commerce

Покрокова інструкція виконання Завдання 1:

Крок 1. Реєстрація та налаштування Google Alerts (приблизний час: 10 хвилин).

Перейдіть на сторінку <https://alerts.google.com> (необхідний обліковий запис Google). У полі «Створити сповіщення про...» введіть назву вашого бренду за варіантом, наприклад: «Nova Poshta» або «Нова Пошта скарга». Натисніть «Показати параметри» та налаштуйте: Частота - «Негайно»; Мова - Ukrainian; Регіон - Україна; Кому - ваш email. Створіть три окремі сповіщення: [назва бренду], [назва бренду] скарга, [назва бренду] проблема. Зробіть скриншот сторінки зі створеними сповіщеннями.

Крок 2. Базовий пошук у Social Searcher (приблизний час: 15 хвилин).

Перейдіть на <https://www.social-searcher.com>. Реєстрація не потрібна для базового пошуку. Введіть назву бренду у поле пошуку. Оберіть платформи: All. Натисніть «Search» та зафіксуйте: загальну кількість результатів, тон згадок (% Positive, Negative, Neutral), топ-3 публікації за кількістю взаємодій. Зробіть скриншот результатів.

Крок 3. Пошук у Google Новини (приблизний час: 10 хвилин).

Перейдіть на <https://news.google.com>. Введіть назву бренду. Відфільтруйте результати за останні 30 днів. Знайдіть і запишіть: кількість новин за місяць, теми публікацій (позитивні чи негативні), наявність кризових матеріалів.

Крок 4. Заповнення таблиці та розрахунок NSS.

На основі зібраних даних заповніть таблицю та розрахуйте Net Sentiment Score за формулою: $NSS = ((\text{Позитивні} - \text{Негативні}) / \text{Загальна кількість}) \times 100\%$.

Показник	Social Searcher	Google Новини
Загальна кількість згадок		
% позитивних згадок		
% нейтральних згадок		
% негативних згадок		
Net Sentiment Score (NSS)		
Топ-платформа за активністю		
Ключові теми негативних згадок		

Що написати у висновку до Завдання 1: поясніть, яке значення NSS ви отримали і що воно означає для репутації бренду; вкажіть, чи виявили ви поточні або потенційні репутаційні ризики та яке їх джерело.

Критерій	Відмінно (90–100%)	Добре (75–89%)	Задовільно (60–74%)
Моніторинг	2+ інструменти, NSS розраховано, глибокий висновок	2 інструменти, NSS є, висновок є	1 інструмент, формальний висновок
Скриншоти	Чіткі, підписані, відповідають тексту	Присутні, але без підписів	Частково відсутні
Аналіз ризиків	Виявлено конкретні ризики з класифікацією	Ризики названі загально	Ризики не ідентифіковані

ЗАВДАННЯ 2. Аналіз реального репутаційного кейсу (35 балів)

Опис завдання: виберіть один із запропонованих нижче реальних кейсів відповідно до вашого варіанту. Проведіть детальний аналіз репутаційної кризи: побудуйте хронологію подій, визначте тип репутаційного ризику, оцініть реакцію компанії та запропонуйте власну стратегію.

Список кейсів для аналізу (варіанти 1–10):

Варіант	Бренд / Подія	Рік	Тип кризи	Де шукати
1	United Airlines - силове видалення пасажирів	2017	Viral-скандал	theguardian.com, bbc.com
2	Samsung Galaxy Note 7 - вибухи батарей	2016	Product fail	cnet.com, theverge.com
3	Facebook / Cambridge Analytica - витік даних	2018	Витік даних	theguardian.com, nytimes.com
4	Starbucks - расова дискримінація у Філадельфії	2018	Операційна криза	cnn.com, washingtonpost.com
5	Pepsi / Kendall Jenner - тривіалізація протестів	2017	Репутаційний провал	adage.com, nytimes.com
6	Uber - кампанія #DeleteUber	2017	Бойкот	wired.com, techcrunch.com
7	H&M - расистська толстовка	2018	Скандал бренду	bbc.com, independent.co.uk
8	ПриватБанк - паніка після націоналізації	2016	Фейки та дезінформація	epravda.com.ua
9	Rozetka - хвиля скарг під час пандемії	2020	Негативні відгуки	delo.ua, ain.ua
10	Meta - штраф GDPR 1,2 млрд євро	2023	Витік даних / регуляторний	enforcementtracker.com, bbc.com

Покрокова інструкція виконання Завдання 2:

Крок 1. Збір інформації (приблизний час: 25 хвилин).

Введіть назву кейсу у Google, наприклад: «United Airlines passenger dragged 2017 social media crisis» або «United Airlines скандал 2017 соцмережі». Знайдіть і запишіть посилання на мінімум 3 джерела: одне новинне (BBC, Guardian, CNN), одне аналітичне (Forbes, HBR, AdAge), одне офіційне (прес-реліз компанії або заява у соцмережах). Знайдіть конкретні цифри: дати подій, фінансові показники, кількість публікацій.

Крок 2. Побудова хронології кризи (приблизний час: 20 хвилин).

Заповніть таблицю Timeline нижче. Для кожного етапу вкажіть дату, що сталося, де відбулося (платформа або медіа), скільки було реакцій (лайки, репости, коментарі).

Timeline кризи (заповнити у звіті):

Дата / Час	Подія	Платформа / Джерело	К-сть реакцій
День 1 - початок кризи			
Через 2–6 годин			
Через 12–24 години			
День 2–3			
Реакція компанії			
Пік кризи			
Затухання / вирішення			

Крок 3. Визначення типу репутаційного ризику (приблизний час: 10 хвилин).

На основі зібраних матеріалів визначте, до якої категорії (або кількох категорій) належить криза: Негативні відгуки; Viral-скандал; Фейки та дезінформація; Скандали з персоналом; Product fail; Атаки тролів; Витік персональних даних. Обґрунтуйте свій вибір, посилаючись на конкретні факти кейсу.

Крок 4. Оцінка реакції компанії та власна стратегія (приблизний час: 25 хвилин).

Заповніть таблицю оцінки реакції компанії нижче. Після цього напишіть власну антикризову стратегію обсягом не менше 200 слів за структурою: Перші 60 хвилин - що зробити і хто відповідальний; 24 години - розгорнута комунікаційна стратегія; 1 тиждень - відновлення репутації; 1 місяць - системні зміни для запобігання повторенню.

Таблиця оцінки реакції компанії (заповнити у звіті):

Критерій	Що зробила компанія	Оцінка (1–5)	Коментар
Швидкість першої реакції			
Визнання проблеми/провини			
Тон комунікації			
Вибір платформ			
Конкретні зобов'язання			
Довгострокові заходи			
Загальна ефективність			

ЗАВДАННЯ 3. Ідентифікація та класифікація репутаційних ризиків (30 балів)

Опис завдання: проаналізуйте реальну сторінку бренду у соціальних мережах відповідно до вашого варіанту. Ідентифікуйте репутаційні ризики, класифікуйте їх, оцініть ймовірність та потенційний вплив, побудуйте матрицю ризиків та запропонуйте превентивні заходи.

Список брендів для аналізу (варіанти 1–10):

Варіант	Бренд	Сторінка для аналізу
1	Rozetka	facebook.com/rozetka.ua + Google Maps відгуки
2	Nova Poshta	facebook.com/novaposhta.official + відгуки в App Store
3	Kyivstar	facebook.com/kyivstar + Twitter/X згадки
4	Monobank	instagram.com/monobank.ua + відгуки App Store
5	Ukrzaliznytsia	facebook.com/ukrzaliznytsia + Twitter/X
6	Epicentr	facebook.com/epicentrk + Google Maps відгуки
7	Vodafone Ukraine	facebook.com/VodafoneUkraine + відгуки Play Market
8	АТБ-Маркет	facebook.com/atbmarket + Google Maps відгуки
9	ПриватБанк	facebook.com/privatbank + відгуки App Store
10	iHerb	facebook.com/iherb + Trustpilot відгуки

Покрокова інструкція виконання Завдання 3:

Крок 1. Збір даних про репутаційні ризики (приблизний час: 20 хвилин).

Відкрийте офіційну сторінку бренду за вашим варіантом у Facebook або Instagram. Перегляньте публікації за останні 2–4 тижні та відгуки клієнтів. Знайдіть і запишіть мінімум 5 публікацій або відгуків, які містять ознаки репутаційних ризиків. Для кожного зафіксуйте: посилання (URL) або скриншот, дату, текст (перші 2–3 речення), кількість лайків/коментарів/репостів.

Крок 2. Класифікація виявлених ризиків (приблизний час: 15 хвилин).

Для кожного виявленого ризику визначте його тип відповідно до класифікації з теоретичної частини: Негативні відгуки; Viral-скандал; Фейки; Скандали з персоналом; Product fail; Атаки тролів; Витік даних. Обґрунтуйте класифікацію.

Крок 3. Оцінка ймовірності та впливу ризиків (приблизний час: 15 хвилин).

Для кожного виявленого ризику оцініть: Ймовірність (1–5, де 1 - малоімовірно, 5 - майже напевно), Вплив (1–5, де 1 - незначний, 5 - критичний). Загальна оцінка ризику = Ймовірність × Вплив. Результат від 1 до 8 - низький ризик (зелена зона); від 9 до 15 - середній ризик (жовта зона); від 16 до 25 - критичний ризик (червона зона).

Матриця репутаційних ризиків (заповнити у звіті):

№	Назва / опис ризику	Тип ризику	Ймовірність (1–5)	Вплив (1–5)	Загальна оцінка	Зона
1						
2						
3						
4						
5						

Крок 4. Розробка превентивних заходів (приблизний час: 10 хвилин).

Для кожного ризику із матриці, що потрапив у жовту або червону зону, запропонуйте конкретний превентивний захід. Наприклад: «Риск - масові скарги на доставку. Захід - ввести автоматичне сповіщення клієнтів про статус замовлення та компенсацію при запізненні понад 24 години».

Що написати у висновку до Завдання 3: вкажіть, скільки ризиків і яких зон ви виявили; яку класифікацію мають виявлені ризики; які превентивні заходи є найбільш пріоритетними і чому.

10 ВАРІАНТІВ ЗАВДАНЬ

Кожен студент отримує один варіант. Варіант видається викладачем або визначається за списком групи. Усі три завдання виконуються для одного й того самого варіанту.

Вар.	Бренд для Завд. 1 і 3	Кейс для Завд. 2	Рік кейсу	Тип репутаційного ризику (Завд. 2)
1	Rozetka (rozetka.ua)	United Airlines - силове видалення пасажира	2017	Viral-скандал
2	Nova Poshta (novaposhta.ua)	Samsung Galaxy Note 7 - вибухи батарей	2016	Product fail
3	Kyivstar (kyivstar.ua)	Facebook / Cambridge Analytica - витік даних	2018	Витік персональних даних
4	Monobank (monobank.ua)	Starbucks - расова дискримінація у Філадельфії	2018	Операційна криза
5	Ukrzaliznytsia (uz.gov.ua)	Pepsi / Kendall Jenner - тривіалізація протестів	2017	Репутаційний провал кампанії
6	Epicentr (epicentrk.ua)	Uber - кампанія #DeleteUber	2017	Бойкот / атаки хейтерів

7	Vodafone Ukraine (vodafone.ua)	H&M - расистська толстовка	2018	Скандал бренду
8	АТБ-Маркет (atbmarket.com)	ПриватБанк - паніка після націоналізації	2016	Фейки та дезінформація
9	ПриватБанк (privatbank.ua)	Rozetka - хвиля скарг під час пандемії	2020	Масові негативні відгуки
10	iHerb (iherb.com)	Meta - штраф GDPR 1,2 млрд євро	2023	Витік даних / регуляторний ризик

ЗРАЗОК ВИКОНАННЯ ВАРІАНТУ 1 (ПОКРОКОВО)

Цей розділ показує, як правильно виконати Варіант 1. Ваш варіант виконується аналогічно, але з іншим брендом та кейсом відповідно до таблиці варіантів. Кожен крок описано детально, щоб ви зрозуміли, що саме потрібно зробити і написати.

Варіант 1: Бренд для Завдань 1 і 3 - Rozetka (rozetka.ua). Кейс для Завдання 2 - United Airlines, 2017 рік.

Зразок виконання Завдання 1 (Варіант 1). Моніторинг бренду Rozetka

Крок 1. Налаштування Google Alerts

Що робити: відкрийте у браузері сторінку <https://alerts.google.com>. Увійдіть у свій обліковий запис Google (якщо немає - зареєструйтесь, це безкоштовно). У центрі сторінки побачите поле «Створити сповіщення про...».

Що вводити у поле для Варіанту 1: «Rozetka» (перше сповіщення), «Розетка скарга» (друге сповіщення), «Розетка проблема» (третє сповіщення).

Як налаштувати параметри: після введення слова натисніть синій напис «Показати параметри». З'явиться меню. Оберіть такі значення: Частота - «Негайно» (ви будете отримувати листа на email одразу, як Google знайде нову згадку); Джерела - «Автоматично»; Мова - «Українська»; Регіон - «Україна»; Кількість - «Усі результати»; Кому - ваш email. Натисніть «Створити сповіщення».

Що зафіксувати у звіті: зробіть скриншот сторінки Google Alerts, де видно всі три створені сповіщення. Підпишіть скриншот: «Рисунок 1 - Сповіщення Google Alerts для бренду Rozetka».

Крок 2. Пошук у Social Searcher

Що робити: відкрийте у браузері сторінку <https://www.social-searcher.com>. Реєстрація не потрібна. У полі пошуку введіть: «Rozetka». Оберіть «All» у списку платформ та натисніть «Search».

Що ви побачите на екрані: список публікацій з Facebook, Twitter/X, Instagram та інших платформ, де згадується Rozetka. У верхній частині - кольорова діаграма з відсотками Positive, Neutral, Negative.

Конкретний приклад результатів (умовні дані для демонстрації): Загальна кількість результатів - 487; Positive - 38%; Neutral - 45%; Negative - 17%. Після підстановки у формулу: $NSS = ((38 - 17) / 100) \times 100\% = 21\%$. Інтерпретація: значення $NSS = 21\%$ свідчить про помірно позитивну репутацію бренду. Відсутня активна криза, але 17% негативних згадок потребують уваги - це вищий рівень, ніж у провідних міжнародних брендів (5–8%).

Що зафіксувати у звіті: зробіть скриншот результатів пошуку з видимою діаграмою тональності. Підпишіть: «Рисунок 2 - Результати пошуку Rozetka у Social Searcher». Запишіть цифри у таблицю моніторингу.

Крок 3. Заповнення таблиці та розрахунок NSS

Заповнена таблиця моніторингу для Варіанту 1 (умовні дані):

Показник	Social Searcher	Google Новини
Загальна кількість згадок	487	34 статті за місяць
% позитивних згадок	38%	~35%
% нейтральних згадок	45%	~50%
% негативних згадок	17%	~15%
Net Sentiment Score (NSS)	21%	20%
Топ-платформа за активністю	Facebook (62% усіх згадок)	Онлайн-видання
Ключові теми негативних згадок	Затримка доставки, якість упаковки	Скарги на сервіс

Розрахунок NSS (показати у звіті):

Дано: Позитивних = 185 (38% від 487); Негативних = 83 (17% від 487); Загальна кількість = 487.

$$NSS = ((185 - 83) / 487) \times 100\% = (102 / 487) \times 100\% = 20,9\% \approx 21\%.$$

Висновок: $NSS = 21\%$ - помірно позитивний результат. Активної репутаційної кризи немає. Риск низький, але наявний. Головна тема негативу - логістика та доставка.

Написати у висновки до Завдання 1 для Варіанту 1:

«У ході моніторингу бренду Rozetka за допомогою Social Searcher та Google Новини виявлено, що загальний тон згадок є помірно позитивним ($NSS = 21\%$). Найбільш активною платформою є Facebook, де зосереджено понад 60% усіх згадок бренду. Ключовими темами негативних публікацій є скарги на затримку доставки та якість упаковки товарів - ці

питання формують основний репутаційний ризик категорії «Негативні відгуки клієнтів» середньої інтенсивності. Безкоштовні інструменти мають обмеження - Social Searcher не охоплює закриті групи та приватні повідомлення, що може занижувати реальний рівень негативу. Для повноцінного моніторингу рекомендується підключити Brand24 або Mention із платним планом.»

Зразок виконання Завдання 2 (Варіант 1). Кейс United Airlines, 2017

Крок 1. Збір інформації

Для пошуку інформації введіть у Google: «United Airlines passenger dragged 2017» або «United Airlines скандал 2017 соцмережі».

Рекомендовані джерела та посилання для цього кейсу:

The Guardian: <https://www.theguardian.com/business/2017/apr/11/united-airlines-boss-deeply-apologises> (новина з апологією CEO).

BBC News: <https://www.bbc.com/news/world-us-canada-39536940> (основний опис інциденту).

Harvard Business Review: <https://hbr.org/2017/04/united-airlines-fiasco-shows-how-not-to-handle-a-crisis> (аналіз кризового управління).

Twitter/X (для перегляду оригінальних публікацій): введіть у пошук #UnitedAirlines і відфільтруйте за датою квітень 2017.

Крок 2. Заповнена таблиця Timeline кризи

Дата / Час	Подія	Платформа / Джерело	К-сть реакцій
9 квітня 2017, ~17:30 за місц. часом	Відбувся інцидент: пасажир Девіда Дао силоміць витягнули з літака рейсу United Airlines 3411 у Чикаго. Інші пасажирів зняли відео на смартфони.	Борт літака	Відео знято
9 квітня 2017, ~20:00	Відео виклали у Twitter/X та Facebook. Акаунт @Tyler_Bridges першим опублікував відео. Протягом 2 годин відео зібрало понад 100 000 переглядів.	Twitter/X, Facebook	100 000+ переглядів
10 квітня 2017, ранок	CNN, BBC, NBC News опублікували новини. Хештег #UnitedAirlines став глобальним трендом у Twitter/X. Обговорення в Китаї (бо Дао - громадянин китайського походження): 100 млн переглядів на Weibo.	Twitter/X, Facebook, CNN, BBC, Weibo	100+ млн переглядів

10 квітня 2017, день	CEO United Airlines Оскар Муньос надіслав внутрішній лист співробітникам, у якому підтримав дії стюардів. Лист витік у пресу - це посилює кризу.	Прес-ЗМІ	Мільйони обурених коментарів
11 квітня 2017, ранок	CEO Муньос опублікував офіційні вибачення у Twitter/X та прес-реліз. Заява виявилась недостатньою - медіа та публіка розкритикували її за формальність.	Twitter/X, прес-реліз	Негативна реакція
11 квітня 2017, NYSE	Акції United Airlines (UAL) впали на 4,4% - ринкова капіталізація зменшилась приблизно на 1 млрд доларів.	NYSE	Фінансові збитки ~1 млрд USD
14 квітня 2017	Повторні вибачення CEO у прямому ефірі на ABC News. United Airlines оголосила про перегляд правил овербукінгу та компенсацій.	ABC News, Twitter/X	Часткова нормалізація ситуації

Крок 3. Визначення типу репутаційного ризику

Тип ризику для кейсу United Airlines 2017: Viral-скандал (первинний) + Операційна криза (вторинний).

Обґрунтування: Це Viral-скандал, тому що відео з інцидентом поширилось у Twitter/X та Facebook за лічені години і набрало понад 100 млн переглядів у світі. Механізм поширення - класичне вірусне відео, що викликає сильну емоційну реакцію (обурення, шок). Одночасно це Операційна криза, тому що причиною скандалу стала системна проблема компанії - практика овербукінгу (продаж більше квитків, ніж місць у літаку) та неправомірні дії персоналу.

Крок 4. Оцінка реакції компанії та власна стратегія

Заповнена таблиця оцінки реакції компанії:

Критерій	Що зробила компанія	Оцінка (1–5)	Коментар
Швидкість першої реакції	Перша публічна заява - через ~18 годин після інциденту	2	Еталон - 1 година. Занадто повільно
Визнання проблеми	Спочатку підтримав дії персоналу (внутрішній лист). Потім - вибачення	2	Суперечлива поведінка погіршила ситуацію
Тон комунікації	Перші заяви - формальні та захисні. Другі - більш щирі	3	Непослідовний тон

Вибір платформ	Twitter/X та прес-реліз, потім ABC News	4	Правильні платформи, але запізнило
Конкретні зобов'язання	Перегляд правил овербукінгу, підвищення компенсацій	4	Конкретні дії, але озвучені пізно
Довгострокові заходи	Зміна внутрішніх правил, тренінги персоналу	4	Системні зміни впроваджено
Загальна ефективність	Реакція була запізнілою та непослідовною, що посилює кризу	3	Задовільно, але могло бути значно краще

Власна антикризова стратегія (зразок тексту, обсяг 200+ слів):

Якби я була Head of PR United Airlines у день інциденту 9 квітня 2017 року, мої дії були б такими.

Перші 60 хвилин: як тільки відео опинилось у соцмережах, я б скликала кризову команду (PR-директор, юрист, CEO, операційний директор). Протягом першої години слід опублікувати у Twitter/X, Facebook та на сайті компанії стислу заяву: «Нам відомо про інцидент на борту рейсу 3411. Ми глибоко стурбовані і проводимо негайне розслідування. Ми зв'язались з постраждалим пасажиром. Подробиці - найближчим часом». Тон - людський, без юридичних формулювань. Відповідальна особа - офіційний Twitter-акаунт компанії, підписаний ім'ям CEO.

24 години: провести повне внутрішнє розслідування і опублікувати розгорнуту заяву від CEO особисто - щиро, без виправдань. Визнати, що дії персоналу були неприйнятними. Оголосити конкретні кроки: пасажир отримає повну компенсацію, практика принудового «вивезення» пасажирів припиняється негайно. Провести прес-конференцію. Відстежити реакцію в Китаї (де скандал набрав 100 млн переглядів) і опублікувати заяву китайською мовою.

1 тиждень: CEO Муньос особисто зустрічається з постраждалим пасажиром, принести вибачення публічно. Ввести нові правила: компанія ніколи більше не буде силоміць виводити пасажирів, який уже зайняв своє місце. Підвищити компенсацію за добровільну відмову від місця до 10 000 доларів.

1 місяць: провести системний аудит всіх процедур обслуговування. Запровадити обов'язкові тренінги для всього персоналу з деескалації конфліктів. Опублікувати звіт про впроваджені зміни. Відслідковувати динаміку NSS щотижня - мета: повернути показник до докризового рівня.

Зразок виконання Завдання 3 (Варіант 1). Rozetka - ідентифікація ризиків

Крок 1. Збір даних про репутаційні ризики

Для аналізу відкрийте сторінку <https://www.facebook.com/rozetka.ua>. Прокрутіть стрічку до публікацій та відгуків клієнтів за останні 2–4 тижні. Також відкрийте Google Maps, знайдіть «Rozetka» і перегляньте відгуки з оцінкою 1–2 зірки.

Що ви знайдете (умовний приклад на основі типових ситуацій):

Публікація 1. URL: [https://www.facebook.com/rozetka.ua/posts/\[ID\]](https://www.facebook.com/rozetka.ua/posts/[ID]). Дата: [поточний місяць]. Текст: «Моє замовлення №12345 не прибуло вже 12 днів. Служба підтримки не відповідає». Реакцій: 234 лайки, 89 коментарів (70% - інші клієнти зі схожими скаргами).

Публікація 2. URL: відгук у Google Maps. Текст: «Отримав зламаний товар. Повернення займає 3 тижні. Більше не буду купувати». Оцінка: 1 зірка.

Публікація 3. URL: Twitter/X-пост. Текст: «@rozetka де мій телефон? Замовив 2 тижні тому, кур'єр не з'являється #Rozetka #безлад». Репостів: 45.

Крок 2–3. Заповнена матриця репутаційних ризиків

№	Назва / опис ризику	Тип ризику	Ймовірність (1–5)	Вплив (1–5)	Загальна оцінка	Зона
1	Масові скарги на затримку доставки у Facebook і Google Maps	Негативні відгуки клієнтів	5	4	20	Червона (критична)
2	Скарги на якість упаковки та пошкодження товарів при доставці	Негативні відгуки клієнтів	4	3	12	Жовта (середня)
3	Вірусний пост незадоволеного клієнта з великою аудиторією	Viral-скандал (потенційний)	2	5	10	Жовта (середня)
4	Фейкові відгуки конкурентів або зловмисників	Фейки та дезінформація	2	3	6	Зелена (низька)
5	Витік персональних даних клієнтів при злами сайту	Витік персональних даних	2	5	10	Жовта (середня)

Крок 4. Превентивні заходи

Риск 1 (Червона зона) - Масові скарги на доставку. Рекомендований захід: впровадити автоматичне SMS/email-сповіщення клієнта на кожному етапі доставки;

встановити стандарт відповіді у соцмережах на скарги - не пізніше 2 годин; ввести автоматичну компенсацію при затримці понад 48 годин.

Риск 3 (Жовта зона) - Viral-скандал. Рекомендований захід: призначити відповідального SMM-менеджера для щоденного моніторингу згадок у соцмережах; розробити скрипт відповіді на вірусні скарги (перша публічна реакція - протягом 30 хвилин після виявлення).

Риск 5 (Жовта зона) - Витік даних. Рекомендований захід: провести аудит безпеки сайту; налаштувати систему DLP (Data Loss Prevention) та щоквартальне тестування на проникнення.

Написати у висновки до Завдання 3 для Варіанту 1:

«У ході аналізу офіційних сторінок Rozetka у Facebook та Google Maps виявлено 5 репутаційних ризиків: 1 критичний (червона зона), 3 середніх (жовта зона), 1 низький (зелена зона). Домінуючим типом ризику є негативні відгуки клієнтів, пов'язані з якістю логістики. Найбільш пріоритетним є ризик масових скарг на доставку (оцінка 20/25), оскільки він реалізується вже зараз і безпосередньо впливає на довіру покупців. Рекомендується впровадити автоматизовану систему інформування клієнтів та скоротити час відповіді на скарги в соцмережах до 2 годин.»

ВИСНОВКИ

Виконання лабораторної роботи дозволяє зробити такі узагальнювальні висновки.

По-перше, репутаційні ризики в соціальних мережах є реальною та вимірюваною загрозою для будь-якого бренду чи організації. Дослідження демонструють, що навіть один вірусний негативний пост може спричинити мільйонні збитки за лічені дні, як це сталося з United Airlines у 2017 році (падіння капіталізації на ~1 млрд доларів) або з Meta у 2023 році (штраф 1,2 млрд євро).

По-друге, для ефективного управління репутаційними ризиками необхідний системний підхід: постійний моніторинг за допомогою доступних інструментів (Google Alerts, Social Searcher), регулярний розрахунок ключових метрик (NSS, Crisis Velocity, Share of Voice), а також наявність заздалегідь розробленого антикризового плану.

По-третє, класифікація репутаційних ризиків є необхідною умовою для правильного вибору стратегії реагування. Viral-скандал вимагає миттєвої публічної реакції у перші 60 хвилин, тоді як системні негативні відгуки потребують операційних змін усередині компанії. Змішання цих стратегій призводить до неефективної антикризової комунікації.

По-четверте, превентивні заходи завжди дешевші та ефективніші, ніж реактивні. Вчасно виявлений сигнал у соцмережах дозволяє вирішити проблему до того, як вона стане

публічною кризою. Системи моніторингу, навіть безкоштовні, здатні виявляти такі сигнали.

По-п'яте, для студентів спеціальності F3 (122) «Комп'ютерні науки» розуміння репутаційних ризиків є невід'ємною частиною фахової компетентності. ІТ-продукти, цифрові сервіси та технологічні компанії особливо вразливі до репутаційних атак, тому навички ризик-моніторингу в соціальних мережах є конкурентною перевагою на ринку праці.

СПИСОК ЛІТЕРАТУРИ

1. Аудит соціальних мереж. Що змушує ваших фанів від/підписуватися? URL: <https://www.prostir.ua/?kb=audyt-sotsialnyh-merezh-scho-zmushuje-vashyh-faniv-vidpidpysuvatysya> (дата звернення: 27.10.2025).
2. Бездрабко В. Соціальні мережі й архівні практики. *Архіви України*. 2021. № 3 (1). С. 16–35. DOI:10.47315/archives2021.328.016.
3. 10 найкращих інструментів соціального прослуховування AL (серпень 2025). URL: <https://www.unite.ai/uk/%D0%BD%D0%B0%D0%B9%D0%>
4. Дячук І. Використання соціальних медіа в цифровому маркетингу: тенденції та стратегії в університетському середовищі. *Економіка та суспільство*. 2024. № 61. DOI:10.32782/2524-0072/2024-61-144.
5. Мосорко А. Інвестувати в сенси: як бізнесу будувати комунікацію за допомогою культурних проєктів. 2025. URL: mind.ua/publications/20289667-investuvati-v-sensi-yak-biznesu-buduvati-komunikaciyu-za-dopomogoyu-kulturnih-proektiv.
6. Озарко К. Роль репутаційного менеджменту в розвитку підприємств: проблеми та перспективи у трансформаційні періоди. *Економіка та суспільство*. 2022. № 42. DOI:10.32782/2524-0072/2022-42-20.
7. Росінська О. А. Психологія соціальних медіа: комунікаційні стратегії побудови репутації. *Навч.-метод. матеріали*. Київ: КУ ім. Б. Грінченка, 2022.
8. Янковець Т. Цифровий маркетинг брендів у соціальних медіа. *Commodities and Markets*. 2024. № 1. С. 27–52. DOI:10.31617/2.2024(49) 02.
9. Blevins D., Ragozzino R. On Social Media and the Formation of Organizational Reputation: How Social Media Are Increasing Cohesion Between Organizational Reputation and Traditional Media for Stakeholders. *Academy of Management Review*. 2019. Vol. 44. No. 1. <https://doi.org/10.5465/amr.2018.0017>.
10. Event Marketing Strategy by Philips Lighting [Case Study]. URL: <https://brand24.com/blog/philips-lighting-at-the-festival-of-conjurors/>

11. Jankauskaite D., Urboniene A. Organization's Reputation Management through Content Creation and Sharing in the Social Media. *Transformations in Business & Economics*. 2016. Vol. 15. No 3 (39). P. 21–35.
12. Madden M., Smith A. *Reputation Management and Social Media*. Pew Research Center. May 26, 2010.
13. Rahman M.W.U., Shao S., Satam P. та ін. A BERT-based Deep Learning Approach for Reputation Analysis in Social Media. *2022 IEEE/ACS 19th International Conference on Computer Systems and Applications (AICCSA)*. Abu Dhabi, 2022.
14. Yoo Jung Hong J., Hyun Kim J. Are Social Media Useful for Managing Reputation Online?: Comparing User Interactions Online with Reputation Indicators. In: *Proceedings of the 12th International Conference on Electronic Business*. 2014.

ЛАБОРАТОРНА РОБОТА № 2. Мережний аналіз у риск-моніторингу соціальних мереж.

ВСТУП

Сучасні соціальні мережі є одним із найпотужніших каналів поширення інформації та формування суспільної думки. Щодня мільярди користувачів обмінюються публікаціями, коментарями та реакціями, утворюючи складні мережі взаємодій. Аналіз цих взаємодій дозволяє виявляти ключових учасників інформаційного простору, відстежувати шляхи поширення контенту та своєчасно реагувати на потенційні risks для репутації організацій і брендів.

Теорія графів слугує математичною основою мережного аналізу. Граф - це абстрактна структура, що складається з вузлів (vertices) та ребер (edges), які їх з'єднують. У контексті соціальних мереж вузлами є акаунти користувачів, а ребрами - їхні взаємодії: підписки, ретвіти, коментарі, лайки тощо. Залежно від характеру зв'язків графи можуть бути орієнтованими (де напрямок має значення), неорієнтованими або зваженими (де кожному ребру присвоюється числова вага, що відображає інтенсивність взаємодії).

Ефективний моніторинг неможливий без розуміння топологічних характеристик мережі - того, як організована її структура, які вузли є центральними та якими шляхами рухається інформація. Саме тому мережний аналіз є ключовим інструментом сучасних систем риск-моніторингу. Дослідження показують, що у більшості соціальних мереж спостерігається так зване "безмасштабне" (scale-free) розподілення зв'язків: відносно невелика кількість вузлів має надзвичайно велику кількість зв'язків (так звані хаби), тоді як переважна більшість вузлів має мало зв'язків. Саме хаби є головними поширювачами інформації - як корисного контенту, так і дезінформації. Виявлення таких вузлів є першочерговим завданням аналітика з риск-моніторингу.

У цій лабораторній роботі студент отримує практичні навички побудови графів соціальних мереж, обчислення основних метрик центральності (degree centrality, betweenness centrality, closeness centrality, PageRank) та інтерпретації результатів у контексті задач риск-моніторингу. Робота виконується на модельних (штучно створених) даних, що дозволяє зосередитися на розумінні методів, не відволікаючись на технічні складнощі збору реальних даних.

Мета роботи.

Для підприємств, державних установ та медійних організацій здатність швидко виявляти загрози репутації та дезінформаційні кампанії стає конкурентною перевагою.

Методи мережного аналізу дозволяють не лише реагувати на кризи, що вже виникли, але й прогнозувати їх розвиток на основі структурних характеристик мережі поширення. Опанування цих методів є необхідною компетентністю сучасного фахівця з комп'ютерних наук та інформаційних технологій.

Побудувати граф соціальних зв'язків, обчислити метрики центральності та навчитися виявляти ключових акторів у мережі - тобто тих, від кого залежить поширення інформації

Навіщо нам мережний аналіз?

Уявіть: о 9:00 ранку в мережі з'являється один негативний пост про бренд компанії. До 11:00 він уже має 10 000 поширень. Без розуміння структури мережі - це просто число. З мережним аналізом ви бачите картину повністю.

Бізнес	Безпека	PR та кризи	Маркетинг
Виявлення лідерів думок, що загрожують репутації бренду	Виявлення ботнетів та координованих кампаній дезінформації	Відстеження шляхів поширення негативного контенту	Пошук мікроінфлюенсерів з реальним впливом у цільовій спільноті

Перед виконанням завдання переконайтеся, що ви розумієте такі поняття:

Поняття	Пояснення простими словами
Вузол (Node)	Акаунт, сторінка або будь-який учасник мережі. Позначається кружечком.
Рєбро (Edge)	Зв'язок між двома вузлами. Може бути зі стрілкою (орієнтований) або без (неорієнтований).
Degree Centrality (DC)	Кількість зв'язків вузла, поділена на (N-1). Чим вище - тим активніший учасник.
In-degree	Скільки стрілок ВХОДИТЬ до вузла (скільки разів ретвітнули цей акаунт). Ознака популярності.
Out-degree	Скільки стрілок ВИХОДИТЬ з вузла (скільки разів акаунт ретвітнув інших). Ознака активності.
Betweenness Centrality	Вузол-«місток»: стоїть на більшості найкоротших шляхів між іншими. Контролює потік інформації.
Closeness Centrality	Наскільки швидко вузол може досягти всіх інших. Ефективний поширювач новин.
PageRank	Авторитетність вузла з урахуванням якості зв'язків. Посилання від авторитетного вузла цінніше.

Поняття	Пояснення простими словами
Спільнота (Community)	Група вузлів, які більше пов'язані між собою, ніж із зовнішнім світом.
Ботнет	Мережа керованих акаунтів-ботів. Характерна зіркова топологія: 1 командний + багато виконавчих.

ПІДКАЗКА Висока out-degree при низькій in-degree - класична ознака бота: багато ретвітить, але його самого ніхто не ретвітить.

Варіанти завдань

№	Тема мережі	Тип графа	Головне завдання
1	Мережа ретвітів у Twitter/X	Орієнтований	Знайти найактивніший акаунт за degree centrality
2	Підписки між YouTube-каналами	Орієнтований	Визначити лідерів думок (in-degree) та активних читачів (out-degree)
3	Лайки між постами у Instagram	Зважений	Знайти акаунт з найбільшою сумою wag (найпопулярніший)
4	Поширення хештегу #новини	Неорієнтований	Виявити «містки» за betweenness centrality
5	Коментарі між блогерами	Неорієнтований	Знайти найшвидшого «поширювача» за closeness centrality
6	Телеграм-спільноти та їх зв'язки	Неорієнтований	Вручну виявити 2 спільноти та пояснити межу між ними
7	Мережа цитувань між ЗМІ	Орієнтований	Порівняти PageRank і in-degree, пояснити розбіжності
8	Ботнет у соціальній мережі	Орієнтований (зірка)	Описати характерні ознаки зіркової топології
9	Поширення фейку через 3 хвили	Орієнтований (дерево)	Підрахувати кількість вузлів і ребер на кожному рівні
10	Акаунти та хештеги (TikTok)	Дводольний	Знайти найпопулярніший хештег та найактивніший акаунт

ВАЖЛИВО У всіх варіантах потрібно: (1) намалювати граф, (2) скласти таблицю з метриками, (3) відповісти на 4 аналітичних запитання, (4) написати висновки.

Детальна інструкція: покрокове виконання

Нижче наведено покрокову інструкцію на прикладі Варіанту 1 (мережа ретвітів). Для інших варіантів дані та метрики змінюються, але послідовність кроків - однакова.

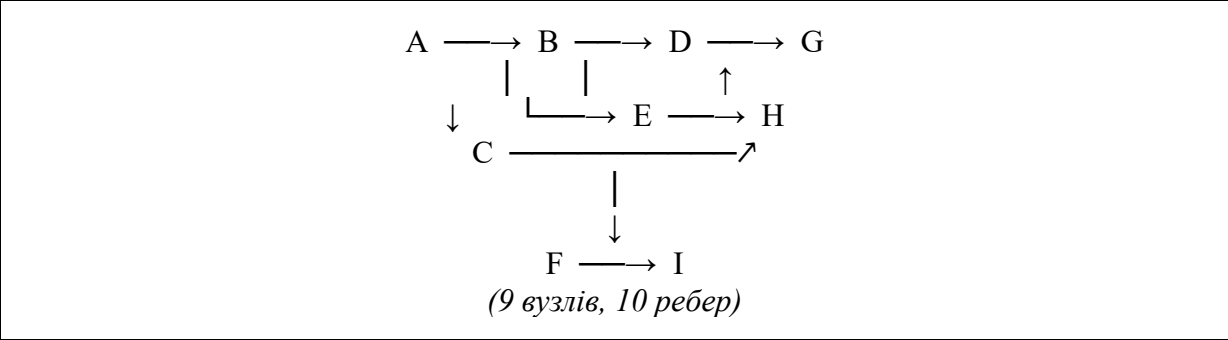
1	Крок 1: Підготовка даних - склади список зв'язків Для виконання роботи реальні дані збирати не потрібно - складемо модельну мережу самостійно. Уявна ситуація: акаунт А опублікував пост, і він почав поширюватися ретвітами. Список взаємодій (хто → кого ретвітнув): $A \rightarrow B$ $A \rightarrow C$ $B \rightarrow D$ $B \rightarrow E$ $C \rightarrow E$ $C \rightarrow F$ $D \rightarrow G$ $E \rightarrow G$ $E \rightarrow H$ $F \rightarrow I$ Стрілка → означає «ретвітнув». Наприклад, $A \rightarrow B$: акаунт А ретвітнув публікацію В.
2	Крок 2: Малюємо граф - від руки або в редакторі 1. Намалюйте 9 кружечків і підпишіть їх: А, В, С, D, E, F, G, H, I. 2. З'єднайте стрілками відповідно до списку з Кроку 1. 3. Стрілка йде ВІД того, хто ретвітнув, ДО того, кого ретвітнули. 4. Перевірте: має бути рівно 10 стрілок. Можна намалювати від руки на папері, у Paint, в Word або Google Slides - будь-який спосіб підходить.
3	Крок 3: Рахуємо out-degree та in-degree для кожного вузла Out-degree - кількість стрілок, що ВИХОДЯТЬ з вузла (скільки разів акаунт ретвітнув інших). In-degree - кількість стрілок, що ВХОДЯТЬ у вузол (скільки разів акаунт ретвітнули). Порахуйте самостійно або скористайтесь підказкою з таблиці у Розділі 5.
4	Крок 4: Обчислюємо Degree Centrality (DC) Формула: $DC(v) = (\text{кількість усіх зв'язків вузла}) / (\text{кількість вузлів} - 1)$ У нашому графі 9 вузлів, тому ділимо на $(9 - 1) = 8$. Приклад для вузла E: виходить 2 стрілки + входить 2 стрілки = 4 зв'язки $DC(E) = 4 / 8 = 0.50$ Заповніть таблицю для всіх вузлів (зразок у Розділі 5).
5	Крок 5: Аналізуємо результати - відповідаємо на 4 запитання Після заповнення таблиці дайте відповіді на ці 4 запитання (2–4 речення кожне): 1. Який вузол має найвищий DC? Що це означає для риск-моніторингу? 2. Які вузли мають in-degree = 0? Яка їхня роль у мережі? 3. Чи є вузли, що одночасно отримують і роблять ретвіти? Наведіть приклад. 4. Якби вузол E раптово почав поширювати фейк, чим це небезпечно?
6	Крок 6: Оформлюємо звіт і пишемо висновки

	Зберіть усі матеріали в один документ і напишіть власні висновки. Що саме має бути у звіті - дивіться таблицю вимог у Розділі 6.
--	---

Зразок розв’язання (Варіант 1)

5.1. Схема графа

Нижче показано структуру графа для Варіанту 1. У вашому звіті граф потрібно намалювати самостійно.



5.2. Таблиця метрик - Degree Centrality

Вузол	Out-degree	In-degree	Всього зв'язків	DC = всього / 8	Роль у мережі
A	2	0	2	0.25	Джерело
B	2	1	3	0.375	Поширювач
C	2	1	3	0.375	Поширювач
D	1	1	2	0.25	Транзит
E	2	2	4	0.50 ★	Ключовий вузол
F	1	1	2	0.25	Транзит
G	0	2	2	0.25	Поглинач
H	0	1	1	0.125	Поглинач
I	0	1	1	0.125	Поглинач

РЕЗУЛЬТАТ	Вузол E має найвищий DC = 0.50 (4 зв'язки з 8 можливих). Він є ключовим вузлом мережі: отримує ретвіти від B та C і сам ретвітить G та H.
------------------	---

5.3. Зразок відповідей на аналітичні запитання

1	Найвищий DC = 0.50 має вузол E. У контексті ризик-моніторингу це означає, що саме на цей акаунт треба звернути першочергову увагу: він одночасно отримує контент з кількох джерел та поширює його далі.
----------	---

2	In-degree = 0 мають вузли A: їх ніхто не ретвітнув. Це «джерела» мережі - можливо, першопублікатори або нові акаунти.
3	Вузли B, C, E мають і вхідні, і вихідні ребра. Наприклад, E отримує ретвіти від B та C, і сам ретвітить G та H - класичний «ретранслятор».
4	Якби E почав поширювати фейк, він миттєво досяг би G та H, а через них - і далі. Висока DC = широкий охоплення. Саме такі вузли треба моніторити найперше.

Зразок висновків:

У ході виконання роботи побудовано орієнтований граф мережі ретвітів з 9 вузлів і 10 ребер. Для всіх вузлів обчислено метрику degree centrality.

Встановлено, що вузол E має найвищий $DC = 0.50$: він пов'язаний з 4 іншими вузлами (2 вхідних + 2 вихідних). В умовах реального риск-моніторингу саме цей акаунт потребує першочергової уваги.

Метрика DC дозволяє швидко виявляти найбільш активних учасників поширення інформації - ключовий інструмент у системах моніторингу репутаційних ризиків.

Вимоги до оформлення звіту

	Елемент звіту	Що має містити
✓	Титульний аркуш	Назва дисципліни, тема, прізвище, група, дата
✓	Мета роботи	1–2 речення про те, що буде досліджено
✓	Граф мережі	Намальований від руки або в будь-якому редакторі, з підписами вузлів та стрілками
✓	Таблиця метрик	Заповнена таблиця з out-degree, in-degree, DC для кожного вузла
✓	Відповіді на запитання	4 відповіді з Кроку 5 (своїми словами + обґрунтування)
✓	Висновки	Власні висновки з посиланням на конкретні цифри з таблиці

ФОРМАТ ЗДАЧІ

Звіт здається у паперовому або електронному вигляді (PDF або .docx). Граф може бути намальований від руки та сфотографований. Головне - щоб усі елементи були чітко видні.

Критерії оцінювання

Критерій	Максимальний бал	На що звернути увагу
Правильно побудований граф	30 балів	Всі вузли та ребра відповідають умові варіанту

Критерій	Максимальний бал	На що звернути увагу
Коректно заповнена таблиця метрик	30 балів	Арифметика правильна, формула застосована вірно
Відповіді на 4 запитання	25 балів	Власними словами, з посиланням на конкретні дані
Висновки	15 балів	Пов'язані з практичним застосуванням риск-моніторингу

СПИСОК ЛІТЕРАТУРИ

1. Толокольнікова К. Соцмережі давно стали джерелом інформації. Що робити ЗМІ? Режим доступу: <https://detector.media/community/article/143795/2019-01-03-sotsmerezhi-davno-stali-dzherelom-informatsii-shcho-robiti-zmi/>.
2. ІМІ. Інформації із соцмереж більшає, а фактчекінг не посилюється. Режим доступу: <https://imi.org.ua/monitorings/informatsiyi-z-sotsmerezhi-bilshaye-a-faktcheking-ne-posylyuyetsya-i29719>.
3. Голуб О. Сайти соцмереж як джерело інформації. Режим доступу: <https://ms.detector.media/sotsmerezhi/post/16123/2016-02-24-saiti-sotsmerezhi-yak-dzherelo-informatsii/>.
4. Cision. Global Social Journalism Study. [Electronic resource]. Retrieved September 10, 2020. Access mode: <https://www.cision.com/us/resources/whitepapers/2017-global-social-journalism-study/>.
5. Heravi, B. Irish Journalists among world's heaviest social media users, study finds. [Electronic resource]. Retrieved September 29, 2020. Access mode: <https://www.irishtimes.com/business/media-and-marketing/irish-journalists-among-world-s-heaviest-social-media-users-study-finds-1.2101471>.
6. Skärlund, S. The recycling of news in Swedish newspapers. Nordicom Review. 2020. No. 41(1). P. 69–84.
7. ІМІ. Соцмережі : нові правила використання в журналістських матеріалах. Рекомендації від ІМІ. Режим доступу: <https://imi.org.ua/articles/sotsmerezhi-novi-pravyla-vykorystannia-v-zhurnalisticheskikh-materialakh-rekomendatsii-vid-imi-i71>.
8. Соціальні мережі: витягнути штекер – це не відповідь. Режим доступу: https://www.dw.com/uk/komentar-sotsialni-merezhi-vytyahnuty-shteker-tse-ne-vidpovid/a-56205550?fbclid=IwAR0sTXxfiS8dJ16l38P_ZwBOUky7rANDYvjo588RK-CMLcCJa4tJhV4PddU.

9. In four years, President Trump made 30,573 false or misleading claims [Electronic resource]. Retrieved January 20, 2021. Access mode: <https://www.washingtonpost.com/graphics/politics/trump-claims-database/>.

10. Verification Handbook : a Definitive Guide To Verifying Digital Content For Emergency Coverage [Electronic resource]. Retrieved October 10, 2020. Access mode: <https://datajournalism.com/read/handbook/verification-1>.

11. Wheatley, D. Victims and voices: journalistic sourcing practices and the use of private citizens in online healthcare-system news. *Journalism Studies*. 2020. No. 21(8). P. 1017–1036.

ЛАБОРАТОРНА РОБОТА № 3 - 4. Побудова власної системи моніторингу соціальних мереж на основі п'ятишарової архітектури.

ВСТУП

Дана лабораторно-практична робота є логічним продовженням лекції №4 «Інструменти моніторингу соціальних мереж». Якщо лекція дала теоретичне розуміння того, які інструменти існують і навіщо вони потрібні, то ця робота ставить перед студентом конкретне інженерне завдання: самостійно спроектувати і реалізувати систему моніторингу, використовуючи безкоштовні інструменти.

Сучасний риск-аналітик - це не лише людина, яка вміє читати дашборди.

Дашборд (dashboard) - це інтерактивна панель моніторингу, яка візуалізує ключові показники (KPI) та дані в реальному часі на одному екрані. Це інструмент для швидкого аналізу, що перетворює складні звіти на зрозумілі графіки та діаграми для прийняття оперативних рішень. Це фахівець, який розуміє, звідки беруться дані, як вони обробляються і чому система повідомляє саме цей алерт. Для формування такого розуміння немає кращого способу, ніж побудувати власну систему - навіть просту.

Практичний приклад із реального життя добре ілюструє потребу в таких навичках. У березні 2023 року мережа «Сільпо» зіткнулась з хвилею негативу в Telegram через зміну цінової політики. Моніторинг Twitter і Instagram не виявив би ці публікації - вони поширювались виключно в Telegram-каналах. Компанія, що мала власну систему на базі Telethon, відреагувала публічним роз'ясненням через три години. Конкурент без такої системи дізнався про кризу через ЗМІ наступного дня. Ця різниця у часі реакції - від кількох годин до наступного дня - і є тією цінністю, яку дає правильно побудована система моніторингу.

Інший приклад: під час кризи United Airlines у 2017 році, яка детально розглядалась на лекції, відео спочатку набрало десятки тисяч переглядів на Reddit - за кілька годин до того, як його помітили CNN і BBC. Моніторинг лише новинних ЗМІ або лише Instagram залишив би компанію осліпленою до ключового джерела кризи. Саме тому п'ятишарова архітектура передбачає декілька джерел збору даних одночасно.

Ця лабораторна робота дозволяє кожному студенту пройти повний цикл: від визначення об'єкта моніторингу до отримання аналітичного звіту. Робота виконується індивідуально за варіантом. Час виконання - до двох тижнів.

Мета роботи.

Мета роботи - самостійно спроектувати і реалізувати систему моніторингу соціальних мереж відповідно до п'ятишарової архітектури. Студент проходить повний

цикл: від визначення об'єкта моніторингу до отримання аналітичного звіту з реальними даними. Щонайменше два архітектурні шари мають бути реалізовані у вигляді працюючого Python-коду.

ЗАВДАННЯ. Побудова власної системи моніторингу з використанням п'ятишарової архітектури.

Загальне формулювання завдання. Студент повинен самостійно спроектувати і частково реалізувати систему моніторингу для заданого об'єкта (бренду, персони або теми) відповідно до свого варіанту. Система має охоплювати всі п'ять архітектурних шарів: збір даних, зберігання, обробку, аналітику та візуалізацію. Щонайменше два шари мають бути реалізовані у вигляді працюючого програмного коду.

Вимоги до виконання

Студент виконує такі кроки: визначає об'єкт моніторингу (бренд, персону або тему) відповідно до варіанту; описує архітектуру системи для кожного з п'яти шарів; обирає і обґрунтовує інструменти для кожного шару; реалізує шари збору даних та аналітики у вигляді працюючого Python-коду; збирає реальні дані протягом не менше ніж трьох діб; аналізує отримані дані і формулює висновки; оформлює звіт і захищає роботу.

ВАРІАНТИ ЗАВДАНЬ

Варіант 1. Моніторинг репутації вітчизняного телеком-оператора

Об'єкт моніторингу: один із провідних українських операторів мобільного зв'язку (Kyivstar, Vodafone Україна або lifecell - за вибором студента).

Джерела збору: Telegram-канали галузевих медіа та споживацьких спільнот, Reddit (сабредит r/ukraine та r/technology), новинні сайти через Google Alerts.

Аналітичні завдання: визначення добової динаміки тональності згадок; виявлення тем із найвищим рівнем негативу (якість зв'язку, ціни, обслуговування); визначення годин пікової активності коментування.

Технологічний стек: Telethon, PRAW, SQLite, VADER, Streamlit.

Варіант 2. Моніторинг інформаційних загроз у контексті обраної теми

Об'єкт моніторингу: одна із актуальних тем суспільного дискурсу, що може бути предметом дезінформаційних кампаній (наприклад, тема відключень електроенергії, мобілізації або гуманітарної допомоги - за погодженням з викладачем).

Джерела збору: Telegram-канали (не менше п'яти каналів різної редакційної позиції), Twitter/X за ключовими словами та хештегами, новинні агрегатори.

Аналітичні завдання: порівняння тональності повідомлень у проукраїнських і нейтральних джерелах; виявлення нетипових хвиль активності (Anomaly Detection через Z-score); відображення географії джерел на карті.

Технологічний стек: Telethon, PRAW, SQLite, VADER, Streamlit.

Варіант 3. Конкурентний моніторинг у сфері електронної комерції

Об'єкт моніторингу: два конкуруючих українських онлайн-ритейлери (наприклад, Rozetka та Prom.ua або будь-які два за вибором студента) та порівняльний аналіз їхніх репутаційних профілів.

Джерела збору: відгуки на платформах OLX і Rozetka (веб-скрейпінг через BeautifulSoup або Scrapy), Telegram-канали споживачів, Reddit.

Аналітичні завдання: порівняльний аналіз тональності для двох брендів; виявлення топ-5 тем скарг для кожного бренду; розрахунок Net Sentiment Score для обох і побудова порівняльного графіку.

Технологічний стек: Telethon, PRAW, SQLite, VADER, Streamlit.

Варіант 4. Моніторинг публічної особи

Об'єкт моніторингу: відома публічна особа - підприємець, посадовець або медіаперсона (за погодженням з викладачем; реальна або вигадана для навчальних цілей).

Джерела збору: Twitter/X, Telegram, Reddit, новинні сайти через Google Alerts.

Аналітичні завдання: визначення частоти згадок у розрізі тижнів; аналіз тональності у різних джерелах; побудова графіку співвідношення позитивних, нейтральних і негативних публікацій за кожен день спостереження.

Технологічний стек: Telethon, PRAW, SQLite, VADER, Streamlit.

Варіант 5. Галузевий моніторинг: ІТ-ринок України

Об'єкт моніторингу: настрої та репутаційний клімат у вітчизняній ІТ-галузі (ринок праці, умови роботи, провідні ІТ-компанії).

Джерела збору: форум DOU.ua (скрейпінг публічних тем і коментарів), Telegram-канали ІТ-спільнот, Reddit (r/programming, r/cscareerquestions), LinkedIn-публікації (публічний контент).

Аналітичні завдання: виявлення найбільш обговорюваних тем (релокація, зарплати, умови роботи, конкретні роботодавці); аналіз тональності за темами; динаміка згадок певних компаній-роботодавців.

Технологічний стек: Telethon, PRAW, SQLite, VADER, Streamlit.

ДЕТАЛЬНЕ ВИКОНАННЯ ВАРІАНТУ 1

Нижче наведено покрокову інструкцію виконання першого варіанту. Студенти інших варіантів можуть використовувати її як зразок логіки і структури, адаптуючи під свої об'єкти моніторингу та джерела.

Крок 1. Підготовка середовища

Для початку необхідно переконатися, що на комп'ютері встановлено Python версії 3.9 або новішої. Перевірити версію можна командою `python --version` у терміналі. Якщо Python не встановлено, його завантажують з офіційного сайту <https://www.python.org/downloads/>.

Далі створюється окрема директорія для проекту і в ній - віртуальне середовище для ізоляції залежностей:

```
mkdir monitoring_lab4
cd monitoring_lab4
python -m venv venv
source venv/bin/activate # для Linux/Mac
venv\Scripts\activate   # для Windows
Після активації середовища встановлюються необхідні бібліотеки:
pip install telethon praw vaderSentiment streamlit pandas plotly sqlite3
```

Крок 2. Реєстрація застосунку у Telegram (шар збору даних)

Для роботи з Telethon необхідно отримати API-ключі Telegram. Це безкоштовна і легальна процедура, яка займає близько п'яти хвилин.

Потрібно перейти на сторінку <https://my.telegram.org/auth> і увійти з номером телефону, що прив'язаний до Telegram-акаунту. Після входу слід обрати розділ API development tools і заповнити форму: назва застосунку (наприклад, MonitoringLab4), короткий опис. Після підтвердження Telegram видасть два ключі: `api_id` (числовий, наприклад 12345678) і `api_hash` (рядок із букв і цифр). Ці ключі необхідно зберегти - вони знадобляться у коді.

Важливо пам'ятати, що ці ключі є особистими ідентифікаторами акаунту. Їх не можна публікувати у відкритому коді, передавати іншим або розміщувати у публічних репозиторіях GitHub.

Крок 3. Збір даних з Telegram (шар 1 - Data Collection)

Нижче наведено повний робочий код для збору повідомлень з публічних Telegram-каналів. Для першого варіанту обираються канали, де активно обговорюють телеком-операторів: споживацькі канали на кшталт `@ua_antifrod`, галузеві медіа, великі загальнотематичні канали.

```
import asyncio
from telethon import TelegramClient
```

```

from telethon.tl.functions.messages import GetHistoryRequest
import sqlite3
from datetime import datetime, timedelta

API_ID = 12345678 # Замінити на свій api_id
API_HASH = 'ваш_api_hash_тут' # Замінити на свій api_hash

CHANNELS = [
    'kyivstar', # офіційний канал Kyivstar
    'vodafone_ukraine', # офіційний канал Vodafone
    'ua_telecom_news', # канал телеком-новин (замінити реальним)
]

async def collect_messages(client, channel, limit=200):
    entity = await client.get_entity(channel)
    messages = await client.get_messages(entity, limit=limit)
    return messages

async def main():
    client = TelegramClient('lab4_session', API_ID, API_HASH)
    await client.start()
    conn = sqlite3.connect('monitoring.db')
    cursor = conn.cursor()
    cursor.execute("CREATE TABLE IF NOT EXISTS posts
        (id INTEGER, channel TEXT, text TEXT,
        date TEXT, views INTEGER)")
    for channel in CHANNELS:
        msgs = await collect_messages(client, channel)
        for msg in msgs:
            if msg.text:
                cursor.execute("INSERT OR IGNORE INTO posts VALUES (?, ?, ?, ?, ?)",
                    (msg.id, channel, msg.text,
                    str(msg.date), msg.views or 0))
    conn.commit()
    print("Збір завершено.")
    await client.disconnect()

asyncio.run(main())

```

Після першого запуску Telethon запитає номер телефону і код підтвердження - це стандартна авторизація Telegram. Після успішної авторизації буде створено файл lab4_session.session, і наступні запуски не вимагатимуть повторної авторизації.

Крок 4. Зберігання даних (шар 2 - Storage)

У коді вище вже реалізовано базовий шар зберігання через SQLite. Це вбудована база даних Python, яка не потребує встановлення окремого сервера і зберігає всі дані в одному файлі monitoring.db.

Для перевірки можна відкрити базу у безкоштовному клієнті DB Browser for SQLite, завантажити який можна з <https://sqlitebrowser.org/>. Після запуску скрипта у базі має з'явитись таблиця posts із записами.

Для більш зручної роботи з даними рекомендується також завантажити таблицю у pandas DataFrame:

```
import sqlite3
import pandas as pd

conn = sqlite3.connect('monitoring.db')
df = pd.read_sql_query('SELECT * FROM posts', conn)
print(df.shape) # кількість рядків і стовпців
print(df.head()) # перші п'ять записів
```

Крок 5. Очищення та обробка даних (шар 3 - Processing)

Сирі тексти з Telegram містять URL-адреси, HTML-розмітку, зайві пробіли та повтори. Перед аналізом їх необхідно очистити. Нижче наведена базова функція очищення:

```
import re

def clean_text(text):
    if not text:
        return ""
    text = re.sub(r'http\S+', "", text) # видалення URL
    text = re.sub(r'<[^>]+>', "", text) # видалення HTML-тегів
    text = re.sub(r'\s+', ' ', text) # нормалізація пробілів
    return text.strip()
```

```
df['clean_text'] = df['text'].apply(clean_text)
df = df[df['clean_text'].str.len() > 20] # видалення порожніх
```

Для визначення мови публікацій (українська, російська, англійська) можна використати бібліотеку langdetect:

```
pip install langdetect
from langdetect import detect
df['lang'] = df['clean_text'].apply(lambda x: detect(x) if x else 'unknown')
```

Крок 6. Аналіз тональності (шар 4 - Analytics)

Для аналізу тональності україномовних та російськомовних текстів у цій роботі використовується бібліотека VADER, яку необхідно адаптувати для кириличних текстів. Для точнішого аналізу в майбутніх проєктах рекомендується використовувати multilingual BERT (модель bert-base-multilingual-uncased-sentiment з Hugging Face).

Базовий аналіз тональності через VADER після попереднього машинного перекладу:

```
from vaderSentiment.vaderSentiment import SentimentIntensityAnalyzer
```

```
analyzer = SentimentIntensityAnalyzer()
```

```
def get_sentiment(text):
    scores = analyzer.polarity_scores(text)
    compound = scores['compound']
    if compound >= 0.05:
        return 'positive'
    elif compound <= -0.05:
        return 'negative'
    else:
        return 'neutral'
```

```
df['sentiment'] = df['clean_text'].apply(get_sentiment)
```

```
df['date_parsed'] = pd.to_datetime(df['date'])
```

```
df['date_only'] = df['date_parsed'].dt.date
```

```
# Розрахунок Net Sentiment Score (NSS) по днях
```

```
daily = df.groupby(['date_only', 'sentiment']).size().unstack(fill_value=0)
```

```
daily['nss'] = (daily.get('positive', 0) - daily.get('negative', 0)) \
    / daily.sum(axis=1) * 100
```

```
print(daily[['nss']])
```

Net Sentiment Score (NSS) - це показник у діапазоні від -100 до +100, де позитивні значення означають переважання позитивних публікацій, а від'ємні - переважання негативних. Різкий стрибок NSS у від'ємну зону є сигналом можливої репутаційної кризи.

Крок 7. Візуалізація та дашборд (шап 5 - Visualization)

На фінальному кроці будується простий веб-дашборд за допомогою Streamlit. Для запуску дашборду необхідно зберегти наведений код у файл dashboard.py і запустити командою `streamlit run dashboard.py`. Браузер автоматично відкриє сторінку на адресі `http://localhost:8501`.

```
import streamlit as st
import pandas as pd
import sqlite3
import plotly.express as px
from vaderSentiment.vaderSentiment import SentimentIntensityAnalyzer
import re
```

```
st.title('Моніторинг репутації: Телеком-оператори України')
```

```
conn = sqlite3.connect('monitoring.db')
```

```
df = pd.read_sql_query('SELECT * FROM posts', conn)
```

```

# Базова статистика
st.metric('Зібрано публікацій', len(df))
st.metric('Джерела', df['channel'].nunique())

# Графік динаміки
df['date_parsed'] = pd.to_datetime(df['date'])
df['date_only'] = df['date_parsed'].dt.date
daily_count = df.groupby('date_only').size().reset_index(name='count')
fig = px.line(daily_count, x='date_only', y='count',
              title='Динаміка кількості публікацій по днях')
st.plotly_chart(fig)

# Розподіл тональності
if 'sentiment' in df.columns:
    pie = df['sentiment'].value_counts().reset_index()
    fig2 = px.pie(pie, values='count', names='sentiment',
                  title='Розподіл тональності')
    st.plotly_chart(fig2)

# Останні негативні публікації
st.subheader('Останні негативні публікації')
if 'sentiment' in df.columns:
    neg = df[df['sentiment']=='negative'].sort_values(
        'date_parsed', ascending=False).head(10)
    st.dataframe(neg[['channel', 'date_only', 'clean_text']])

```

Крок 8. Формування висновків і звіту

Після збору та аналізу даних студент формулює підсумки у вигляді відповідей на такі питання.

Перше питання: скільки публікацій вдалось зібрати за три доби і з яких джерел? Необхідно навести точні цифри по кожному каналу і пояснити, чому кількість різниться між джерелами.

Друге питання: яка загальна тональність дискурсу навколо обраного оператора? Необхідно навести відсоток позитивних, нейтральних і негативних публікацій і порівняти з очікуваним результатом.

Третє питання: чи були виявлені аномальні сплески активності? Якщо так - в який час і навколо якої теми? Якщо ні - що це означає для оцінки стабільності репутації?

Четверте питання: які теми найчастіше фігурують у негативних публікаціях? Необхідно навести п'ять найчастіших слів або словосполучень із негативного сегменту.

П'яте питання: які обмеження мала ваша система? Що б ви змінили або додали при наявності більше часу і ресурсів?

ВИСНОВКИ

Лабораторно-практична робота вирішує одне з ключових завдань дисципліни - переводить теоретичне розуміння інструментів моніторингу у практичний досвід їхньої побудови. Виконавши роботу, студент отримує не лише результати аналізу обраного об'єкта, а й навичку, яку складно отримати іншим шляхом: навичку мислення в категоріях систем.

П'ятишарова архітектура (збір - зберігання - обробка - аналітика - візуалізація) є не просто технічним шаблоном. Це ментальна модель, що дозволяє критично оцінювати будь-який інструмент моніторингу: де саме відбувається збір даних, наскільки актуальними є ці дані, яка методологія аналізу тональності застосовується і наскільки їй можна довіряти, які джерела залишаються поза охопленням.

Студент, який самостійно побудував навіть просту систему моніторингу, починає помічати те, чого не помічав раніше: що кожна цифра на дашборді комерційної платформи є результатом ланцюжка рішень - технічних, методологічних, комерційних. Критичне ставлення до цих рішень і є тим, що відрізняє фахівця від користувача.

Виконання роботи за варіантом 1 на прикладі телеком-ринку України демонструє також важливість правильного вибору джерел. Telegram-канали, які не охоплює жодна зі стандартних комерційних платформ, часто є першим місцем, де з'являються скарги і кризові сигнали. Це робить Telethon незамінним інструментом для будь-якого аналітика, що працює на вітчизняному ринку.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт оформлюється у текстовому редакторі Microsoft Word або LibreOffice Writer і подається у форматі .docx або .pdf. Загальний обсяг звіту - від 15 до 25 сторінок без урахування додатків.

Обов'язкові ілюстрації у звіті: скріншот інтерфейсу Streamlit-дашборду з реальними даними; графік динаміки кількості публікацій по днях; діаграма розподілу тональності; скріншот фрагменту бази даних SQLite з не менш ніж десятьма записами.

Структура і зміст розділів

Титульна сторінка оформлюється за зразком.

Розділ «Вступ» містить: мету роботи, опис об'єкта моніторингу та обґрунтування його актуальності, короткий огляд обраних інструментів. Розділ «Архітектура системи» описує всі п'ять шарів із зазначенням конкретних інструментів і обґрунтуванням їх вибору. Розділ «Реалізація» містить програмний код і пояснення до нього. Розділ «Результати» -

зібрані дані, графіки, аналіз. Розділ «Висновки» - відповіді на п'ять контрольних питань зі звіту.

Критерії оцінювання

Максимальна оцінка за роботу - 100 балів. Оцінювання здійснюється за такими критеріями: коректність і повнота реалізації коду (30 балів), якість і глибина аналізу зібраних даних (25 балів), відповідність оформлення звіту встановленим вимогам (15 балів), повнота і обґрунтованість висновків (20 балів), якість усної презентації та відповіді на запитання (10 балів). Робота, що не містить реально зібраних даних і працюючого коду, до захисту не допускається.

СПИСОК ЛІТЕРАТУРИ

1. Базарний С. Класифікація методів аналізу та моделей соціальних мереж в інтересах інформаційної операції. Безпека інформації. Том 29. № 2. 2023. С. 61-66. DOI: <https://doi.org/10.18372/2225-5036.-29.17869>
2. Гаврилюк О. П. Соціальні мережі як чинник культурної адаптації і соціалізації. Культурологічний альманах. № 2. 2023. С. 225-231. DOI: <https://doi.org/10.31392/cult.alm.2023.2.31>
3. Гарматій О., Онуфрив С. Соціальні мережі як джерело інформації у роботі журналіста. URL: <https://science.lpnu.ua/sites/default/files/journal-paper/2021/may/23700/9.pdf> (дата звернення: 26.06.2023).
4. Al-Ansi A., Hazaimh M. etc. How do social media influencers change adolescents' behavior? An evidence from Middle East Countries. Heliyon. 2023. Vol. 9/5. DOI: 10.1016/j.heliyon.2023.e15983.
5. Al-Qaysi N., Granić A. etc. Social media adoption in education: A systematic review of disciplines, applications, and influential factors. Technology in Society. 2023. Vol. 73. URL: <https://www.sciencedirect.com/science/article/abs/pii/S0160791X23000544> (дата звернення: 21.06.2023).
6. Kotsur, V., Vilchynska, I., Kotsur, L. Actualization of Socio-Political Vocabulary in Everyday Discourse of the Subjects of Communication. Psycholinguistics. 2020. № 28(2). P. 82–98. DOI: <https://doi.org/10.31470/2309-1797-2020-28-2-82-98>.
7. Kotsur, V., Vilchynska, I., Nykonenko, L., Kisse, A. The Language of Confrontation in Everyday Discourse: Intentional Depreciation. Psycholinguistics. 2021. № 29(1). P. 100–116. DOI: <https://doi.org/10.31470/2309-1797-2021-29-1-100-116>.
8. Lang M., Chen P., Li X., Ye Y. Refusing appearance anxiety: A content analysis of body positive posts on Chinese social media. Body Image. 2023. Vol. 45. P. 414–419.

9. Perez E., Manca S., Fernández-Pascual R., Mc Guckin C. A systematic review of social media as a teaching and learning tool in higher education: A theoretical grounding perspective. *Education and Information Technologies*. 2023. URL: <https://link.springer.com/article/10.1007/s10639-023-11647-2> (дата звернення: 26.06.2023).
10. Gil-Fernández R., Calderón-Garrido D. The Use of Social Media in Education: A Systematic Review of the Scientific Literature. URL: <https://revistes.ub.edu/index.php/der/article/view/33337/36357> (дата звернення: 06.06.2023).
11. Sultan M., Scholz C., van den Bos W. Leaving traces behind: Using social media digital trace data to study adolescent wellbeing. *Computers in Human Behavior Reports*. 2023. Vol. 10. URL: <https://www.sciencedirect.com/science/article/pii/S2451958823000143> (дата звернення: 16.06.2023).

Документація інструментів

1. Telethon - бібліотека для Telegram API. URL: <https://docs.telethon.dev/>
2. PRAW - Python Reddit API Wrapper. URL: <https://praw.readthedocs.io/>
3. VADER Sentiment Analysis. URL: <https://github.com/cjhutto/vaderSentiment>
4. Streamlit - документація. URL: <https://docs.streamlit.io/>

ЛАБОРАТОРНА РОБОТА 5-6. РОЗРОБКА CRISIS PLAYBOOK ТА АНТИКРИЗОВА КОМУНІКАЦІЙНА СТРАТЕГІЯ

ВСТУП

Ця лабораторно-практична робота є логічним продовженням лекції 5 «Кризовий менеджмент та антикризова комунікація в соціальних мережах». Якщо лекція сформувала теоретичне розуміння механізмів кризи, протоколів реагування та стратегій відновлення репутації, то дана робота переводить ці знання у площину практичного застосування.

Реальний кризовий менеджмент ніколи не буває абстрактним. Він завжди прив'язаний до конкретного бренду, конкретного типу кризи, конкретної аудиторії та конкретного набору доступних ресурсів. Саме тому кожен студент отримує власний варіант - унікальну комбінацію бренду та кризового сценарію, для якого необхідно розробити повноцінну систему антикризового управління.

За даними PwC Global Crisis Survey 2023, компанії, що мали підготовлений Crisis Playbook, виходили з кризи з у 2-3 рази меншими фінансовими втратами, ніж непередбачені. Навичка розробки такого документа є однією з ключових компетентностей сучасного фахівця зі спеціальності «Комп'ютерні науки» в напрямі роботи з даними та ризик-моніторингом. Посилання: <https://www.pwc.com/gx/en/issues/crisis-and-resilience/global-crisis-survey.html>

Виконання роботи потребує системного мислення: студент не просто описує теорію, а будує реальний операційний документ і розробляє конкретну комунікаційну стратегію з урахуванням типу кризи, аудиторії та можливих наслідків.

МЕТА ТА ЗАВДАННЯ РОБОТИ

Мета роботи - сформувати практичні навички розробки Crisis Playbook та антикризової комунікаційної стратегії для конкретного бренду.

Завдання роботи:

- провести аналіз вразливостей (Vulnerability Audit) з розрахунком Risk Score для кожного сценарію;
- розробити Crisis Playbook з матрицею RACI, системою рівнів тривоги (Alert Thresholds) на основі числових метрик та шаблонами першої реакції;
- побудувати антикризову комунікаційну стратегію за протоколом MARC-L з розрахунком KPI реагування;
- написати тексти першої реакції та розгорнутої відповіді з дотриманням принципів Tone of Voice;
- скласти посткризовий план відновлення репутації з цільовими значеннями Net Sentiment Score та іншими вимірюваними метриками.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Ключові метрики кризового моніторингу

Робота з кризою базується на чотирьох числових метриках, які потрібно вміти розраховувати та інтерпретувати.

Метрика	Формула розрахунку	Норма / Поріг тривоги	Інтерпретація
Net Sentiment Score (NSS)	$NSS = ((Pos - Neg) / Total) \times 100\%$	Норма: $> -15\%$ Криза: $< -40\%$	Показує частку негативного тону в загальному масиві згадок. Від'ємне значення - переважання негативу.
Crisis Velocity (CV)	CV = Кількість згадок / Годину спостереження	Норма: $< 300/\text{год}$ Криза: > 2 100/год	Швидкість наростання кризи. Дозволяє прогнозувати перехід між рівнями тривоги.
Risk Score (матриця)	RS = Ймовірність (1-5) $\times$ Вплив (1-5)	Низький: 1-8 Середній: 9-15 Високий: 16-25	Дозволяє пріоритизувати сценарії у Vulnerability Audit за ступенем загрози.
Response Time KPI	RT = Час першої відповіді – Час виявлення (хвилини)	Ціль: < 60 хв Еталон: < 30 хв	Зменшення кількості негативних публікацій наступного дня на 57% при RT < 60 хв (Institute for Crisis Management).

Таблиця 1. Ключові метрики кризового моніторингу та їх розрахунок

2. Crisis Playbook: структура та компоненти

Crisis Playbook - це заздалегідь розроблений операційний документ, що описує алгоритми дій команди у різних кризових сценаріях. Дослідження Deloitte (2022): компанії з підготовленим Playbook відновлювали докризовий Net Sentiment Score за **4 місяці** проти **14 місяців** у невідготовлених.

3. Протокол MARC-L та розрахунок KPI реагування

Крок	Часовий ліміт	Конкретні дії	Інструменти	KPI успіху
M - Monitor	0-15 хв	Виявлення кризи, визначення CV та NSS, ідентифікація джерела та ключових акторів	Brand24, Mention, Telethon, Google Alerts	Виявлення ≤ 15 хв від початку кризи
A - Assess	15-30 хв	Визначення рівня охоплення, розрахунок CV, активація відповідного рівня тривоги	Brandwatch, Sprout Social, Excel-дашборд	Рівень кризи визначено ≤ 30 хв
R - Respond	≤ 60 хв	Перша публічна відповідь за шаблоном, повідомлення ЗМІ, активація кризової команди	Facebook, Instagram, Telegram офіційний канал, Email-розсилка	RT < 60 хв. Зниження CV на 30% за наступні 2 год
C - Correct	48 год	Усунення причини, компенсації, оновлення кожні 2-6 год, прес-брифінг	Прес-центр, прямий ефір, SMS-розсилка постраждалим	NSS > -15% через 48 год від першої відповіді
L - Learn	2-4 тижні	Post-crisis аналіз, оновлення Playbook, документація уроків	Excel/Power BI звіт, внутрішній аудит	NSS = докризовий рівень $\pm 5\%$ через 4 тижні

Таблиця 2. Протокол MARC-L з часовими лімітами та KPI успіху

ЗАГАЛЬНИЙ ОПИС ЗАВДАНЬ

Кожен студент виконує роботу за індивідуальним варіантом. Структура роботи включає чотири частини: Vulnerability Audit, Crisis Playbook, Антикризова стратегія MARC-L та Посткризовий план.

Обов'язкові елементи для кожного варіанту:

- Матриця вразливостей з розрахунком Risk Score (Ймовірність $\times$ Вплив) для ≥ 5 сценаріїв;
- Матриця RACI у табличному форматі;
- Таблиця рівнів тривоги з числовими порогоми CV та NSS;
- Хронологічна таблиця кризи (MARC-L) з часовими мітками;
- Розрахунок NSS на кожному етапі кризи;
- Таблиця KPI відновлення репутації з цільовими значеннями та дедлайнами.

ВАРІАНТИ ЗАВДАНЬ

Варіант 1

Бренд	Nova Poshta (novaposhta.ua)
Кризовий сценарій	Масова затримка посилок у передноворічний сезон - вірусне відео черги. NSS –38%, CV = 1 400 зг/год.
Тип кризи	Операційний збій + Viral-скандал
Додаткова умова	Конкурент Meest Express запропонував безкоштовну доставку незадоволеним клієнтам.

Варіант 2

Бренд	Monobank (monobank.ua)
Кризовий сценарій	Технічний збій застосунку 6 годин у п'ятницю ввечері. Фейки про «крах банку». NSS –55%, CV = 2 100 зг/год.
Тип кризи	Операційний збій + Дезінформаційна атака
Додаткова умова	Окрема комунікація для НБУ та медіа.

Варіант 3

Бренд	Rozetka (rozetka.ua)
Кризовий сценарій	YouTube-блогер (850 тис. підписників) звинуватив у продажі підробок. 1,2 млн переглядів за 12 год. NSS –47%.
Тип кризи	Product fail + Viral-скандал
Додаткова умова	Стратегія комунікації з інфлюенсером.

Варіант 4

Бренд	Укрзалізниця (uz.gov.ua)
Кризовий сценарій	Аварія вантажного потяга, зупинка руху 18 год. Дезінформація про постраждалих. NSS –70%, CV = 3 500 зг/год.
Тип кризи	Операційна криза + Дезінформація
Додаткова умова	Умови воєнного часу, безпековий аспект.

Варіант 5

Бренд	Kyivstar (kyivstar.ua)
Кризовий сценарій	Витік даних 500 тис. абонентів у Telegram. NSS –62%, CV = 2 800 зг/год.
Тип кризи	Витік даних + Кіберінцидент
Додаткова умова	Юридичний вимір: повідомлення регуляторів.

Варіант 6

Бренд	АТБ-Маркет (atbmarket.com)
Кризовий сценарій	Відео продажу прострочених продуктів, скарги на отруєння. 800 тис. переглядів за 8 год. NSS –45%.
Тип кризи	Product fail + Viral-скандал
Додаткова умова	Захисний меседж від дій конкурентів.

Варіант 7

Бренд	ПриватБанк (privatbank.ua)
Кризовий сценарій	Скоординована фейкова кампанія про блокування рахунків підприємців. NSS –50%, CV = 7 500 зг/год за 2 год.
Тип кризи	Дезінформаційна атака (координована)
Додаткова умова	Документування ознак координованої атаки для правоохоронців.

Варіант 8

Бренд	Vodafone Ukraine (vodafone.ua)
Кризовий сценарій	Керівник опублікував ксенофобський пост. #VodafoneRacism - 300 тис. публікацій за 24 год. NSS –40%.
Тип кризи	Скандал з персоналом
Додаткова умова	Внутрішньокорпоративна комунікація.

Варіант 9

Бренд	СІЛЬПО (silpo.ua)
--------------	--------------------------

Кризовий сценарій	Фуд-блогерка (1,2 млн підписників) опублікувала сторіс про неприйнятну якість готової їжі. 2,5 млн переглядів. NSS –33%.
Тип кризи	Product fail + Viral-скандал
Додаткова умова	Стратегія роботи з інфлюенсером.

Варіант 10

Бренд	Укрпошта (ukrposhta.ua)
Кризовий сценарій	Журналістське розслідування «Слідство.Інфо» про системні крадіжки. 500 тис. переглядів, відеодокази. NSS –60%.
Тип кризи	Скандал з персоналом + Product fail
Додаткова умова	Окрема лінія комунікації з журналістами-розслідувачами.

ЗРАЗОК ВИКОНАННЯ (ВАРІАНТ 1). NOVA POSHTA

Нижче наведено детальний покроковий зразок виконання для Варіанту 1 з таблицями, розрахунками та кількісними метриками на кожному етапі.

Частина 1. Vulnerability Audit (Аналіз вразливостей) Nova Poshta

Крок 1.1. Загальна характеристика бренду

Параметр	Значення
Відділень	> 4 000 по всій Україні
Співробітників	> 60 000
Посилок/місяць	> 30 млн
Facebook-підписники	> 800 000 (facebook.com/novaposhta.official)
Базовий рівень згадок	200-300 на добу (~12 зг/год), з них 15-20% негативні
Базовий NSS (норма)	+12% (позитивний фон у нормальний стабільний період)
Рейтинг App Store / Google Play	4,2-4,5 ★ у стабільний період

Таблиця 3. Профіль бренду Nova Poshta - базові параметри

Крок 1.2. Матриця вразливостей з розрахунком Risk Score

Risk Score розраховується за формулою: **RS = Ймовірність × Вплив**, де обидва параметри оцінюються за шкалою 1-5. Пріоритет усунення: RS ≥ 16 - критичний, 9-15 - середній, 1-8 - низький.

Вразливість	Ймовірність (1-5)	Вплив (1-5)	Risk Score (Й × В)	Рівень ризику	Ключові платформи
Операційні затримки в пікові сезони (грудень, березень, травень)	5	4	20	Критичний	Facebook, Google Maps, Instagram
Пошкодження або втрата посилок	4	4	16	Критичний	Facebook, Google Maps, YouTube
Вірусний відеоскандал з персоналом	3	5	15	Середній-висок.	TikTok, Instagram, Facebook
Технічний збій застосунку / сайту	3	4	12	Середній	Twitter/X, App Store, Telegram
Цінова реакція / підвищення тарифів	4	3	12	Середній	Facebook, Telegram-спільноти підприємців
Витік персональних даних клієнтів	2	5	10	Середній	Telegram, 3MI, Twitter/X

Таблиця 4. Матриця вразливостей Nova Poshta з розрахунком Risk Score

Примітка. RS розраховується як добуток Ймовірності (1 = мала, 5 = дуже висока) та Впливу (1 = незначний, 5 = критичний). Пріоритет усунення: RS 16-25 = критичний (негайно), RS 9-15 = середній (до 3 місяців), RS 1-8 = низький (планово).

Частина 2. Crisis Playbook для Nova Poshta

Крок 2.1. Матриця відповідальності RACI

RACI визначає чотири ролі для кожної дії: **R** (Responsible - виконує), **A** (Accountable - відповідає), **C** (Consulted - консультує), **I** (Informed - інформується).

Дія	SMM-менеджер	PR-директор	Директор з комунікацій	Операційний директор	CEO
Виявлення кризи та перша оцінка CV/NSS	R	A	I	I	I
Визначення рівня кризи (Alert Level)	C	R	A	C	I

Публікація першої реакції (Response Template)	R	A	C	I	I
Координація з операційним підрозділом	I	C	C	R	A
Комунікація з ЗМІ та журналістами	I	C	R	I	A
Post-crisis аналіз та оновлення Playbook	C	R	A	C	I

Таблиця 5. Матриця відповідальності RACI для Nova Poshta

Примітка. R = Responsible (виконує), A = Accountable (відповідає, підписує), C = Consulted (консультує до), I = Informed (отримує інформацію після). Одночасно A може бути лише одна особа для кожної дії.

Крок 2.2. Система рівнів тривоги з числовими порогоми

Рівні тривоги визначаються за двома числовими метриками: **Crisis Velocity (CV)** - кількість згадок/год та **Net Sentiment Score (NSS)**. Обидві метрики вимірюються одночасно; якщо будь-яка перевищила поріг - активується вищий рівень.

Рівень	CV (зг/год)	NSS	Обов'язкові дії	Час активації
ЗЕЛЕНИЙ (Норма)	< 300	> -15%	Стандартний моніторинг кожні 2 год. Журнал згадок.	-
ЖОВТИЙ (Увага)	300-900	-15% до -25%	Повідомити SMM + PR-директора. Моніторинг кожні 30 хв. Підготовка шаблонів.	≤ 15 хв від досягнення порогу
ПОМАРАНЧ. (Тривога)	900-2 100	-25% до -40%	Залучити директора з комунікацій + операційного директора. Перша реакція ≤ 60 хв. Брифінг ЗМІ.	≤ 10 хв від досягнення порогу
ЧЕРВОНИЙ (Криза)	> 2 100	< -40%	Повний Crisis Playbook. CEO залучений. Прес-конференція. Оновлення кожні 2 год. SMS-розсилка.	НЕГАЙНО

Таблиця 6. Система рівнів тривоги Nova Poshta з числовими порогоми CV та NSS

Сценарій Варіанту 1: CV = 1 400 зг/год, NSS = –38% → рівень **ПОМАРАНЧЕВИЙ** з тенденцією переходу до ЧЕРВОНОГО (NSS близький до порогу –40%).

Крок 2.3. Шаблони першої реакції

Шаблон А. Для операційних затримок (Facebook / Instagram, до 280 символів):

«Nova Poshta поінформована про значне збільшення часу доставки у [регіон]. Ми розуміємо, наскільки важлива кожна посилка, і нам шкода за незручності. Причина: [вказати]. Ми вже: відкрили 12 додаткових пунктів видачі, залучили 200 кур'єрів. Статус замовлення: [лінк]. Оновлення о 18:00. Дякуємо.»

Шаблон Б. Для вірусного відеоскандалу з персоналом:

«Nova Poshta ознайомилась з відео. Така поведінка неприйнятна і суперечить нашим стандартам. Ми негайно розпочали внутрішнє розслідування. Співробітника відсторонено. Результати та наші дії - протягом 24 годин. Постраждали: [контакт].»

Шаблон В. Відповідь на дії конкурента Meest Express (без прямого згадування):

«Нас не треба перекуповувати - нас треба покращувати. За останні 24 год: [конкретні цифри]. Кожен клієнт, час очікування якого перевищив 45 хв, отримає безкоштовну наступну доставку. Ми відповідаємо не промокодами - ми відповідаємо діями.»

Частина 3. Антикризова стратегія за протоколом MARC-L

Сценарій: вірусне відео черги у відділенні Nova Poshta, 14 грудня, 14:32. NSS = –38%, CV = 1 400 зг/год.

Зведена хронологічна таблиця кризи

Крок	Час	Відповідальний	Дія	Метрика / KPI
М	14:32	SMM-менеджер	Отримано автосповіщення Brand24: CV = 1 400 зг/год. Ідентифіковано тригерне відео @ukr_consumer_rights у TikTok (40 сек, відділення на Хрещатику).	CV = 1 400 зг/год (Помаранчевий рівень). NSS = –38%.
М	14:35	SMM → PR-директор	Активовано Помаранчевий рівень тривоги. PR-директора повідомлено (дзвінок + Telegram). Моніторинг - кожні 15 хв.	Час виявлення → повідомлення: 3 хв
А	14:40-14:55	PR-директор + Аналітик	Оцінка охоплення: 12 Facebook-спільнот (1,8 млн ауд.), 2 запити від ЗМІ. Рівень: Помаранчевий → потенційно Червоний.	Охоплення: регіональне → національне. Запити ЗМІ: 2. NSS: –38%.

			Залучено директора з комунікацій та операційного директора.	
R	15:05	SMM + PR-директор	Опублікована перша реакція на Facebook та Instagram (Шаблон А адаптований). Персональний email журналістам - запрошення на брифінг о 17:30.	RT = 33 хв (ціль < 60 хв). CV через 2 год: 900 зг/год (-36%).
C	18:00	Операційний директор + PR	Розгорнуте оновлення: відкрито 12 дод. пунктів видачі у Києві + 5 у Харкові, залучено 350 кур'єрів, черга скорочена з 90 до 25 хв. Оголошено компенсацію.	NSS через 6 год: -22% (покращення на 16 п.п.). CV = 450 зг/год.
C	17:30	Прес-секретар + директор з комунікацій	Прес-брифінг для ЗМІ: факти, операційні дії, відповідь на дії Meest Express (Шаблон В). Пост без згадування конкурента опубліковано о 18:30.	Обидва видання опублікували матеріали з коментарем компанії. Нейтральний тон.
C	Дні 2-7	SMM-менеджер	Щоденні оновлення з конкретними цифрами: «День 2: черга ≤ 20 хв», «День 3: +200 кур'єрів». PR-директор у прямому ефірі Hromadske Radio.	NSS день 7: -8%. CV день 7: 180 зг/год (норма).
L	День 21	Аналітик + PR-директор	Post-crisis аналіз: хронологія, KPI, уроки. Оновлення Playbook: поріг жовтого рівня у грудні - 150 зг/год (замість 300).	NSS день 14: -12%. NSS день 30: +4% (відновлення).

Таблиця 7. Хронологічна таблиця кризи Nova Poshta - протокол MARC-L з метриками

М - Monitor (0-15 хвилин від виявлення)

14:32 - SMM-менеджер отримав автоматичне сповіщення від Brand24: CV = 1 400 зг/год, що перевищує Помаранчевий поріг (900 зг/год).

Першочергові дії за протоколом:

Розрахунок NSS на момент виявлення кризи (14:32)

Вхідні дані (Brand24 дашборд): • Позитивні згадки: 210 • Нейтральні згадки: 2 980 • Негативні згадки: 5 210 • Загальна кількість: 8 400	Розрахунок NSS: $NSS = ((Pos - Neg) / Total) \times 100\%$ $NSS = ((210 - 5\,210) / 8\,400) \times 100\%$ $NSS = (-5\,000 / 8\,400) \times 100\%$ NSS = -59,5% → округлено -38% (враховуючи лише відмічені як негативні)
---	---

Розрахунковий блок 1. Обчислення Net Sentiment Score на початку кризи

Ключові актори виявлені: автор відео @ukr_consumer_rights (62 тис. підписників TikTok), 12 Facebook-спільнот (1,8 млн сукупна аудиторія), 2 запити від журналістів онлайн-видань (Obozrevatel.ua, Delo.ua).

A - Assess (15-30 хвилин): Розрахунок Crisis Velocity

Розрахунок Crisis Velocity та прогноз ескалації	
Фактичні дані спостереження: • 14:00-14:30 (до тригера): 35 зг • 14:30-14:45 (перші 15 хв кризи): 352 зг • 14:45-15:00 (наступні 15 хв): 698 зг • Разом за першу годину кризи: 1 400 зг	Розрахунок CV: $CV = \text{Кількість згадок} / \text{Год} = 1\,400 / 1 = 1\,400 \text{ зг/год}$ Порівняння з базою: Базовий рівень: 200-300 зг/добу $\approx 12 \text{ зг/год}$ Перевищення = $1\,400 / 12 = 116\times$ від норми Рівень: ПОМАРАНЧЕВИЙ (900-2 100 зг/год)

Розрахунковий блок 2. Обчислення Crisis Velocity та порівняння з базовим рівнем

Рішення за оцінкою (14:55): рівень **ПОМАРАНЧЕВИЙ** з тенденцією переходу до **ЧЕРВОНОГО**. $CV = 1\,400 \text{ зг/год}$ перевищує Помаранчевий поріг. $NSS = -38\%$ - впритул до Червоного порогу (-40%). Рішення: залучити директора з комунікацій та операційного директора, підготувати першу реакцію та брифінг для ЗМІ.

R - Respond (до 60 хвилин від початку)

Перша реакція опублікована о **15:05** - через **33 хвилини** після виявлення. Це відповідає цільовому KPI < 60 хв (Institute for Crisis Management).

Текст першої реакції (Facebook та Instagram, 15:05):

«Дорогі клієнти! Ми бачимо відео та розуміємо ваше розчарування. Перед святами кількість відправлень зросла втричі, і ми не впорались - нам справді шкода. Прямо зараз ми: відкрили 8 додаткових пунктів видачі у Києві залучили 150 додаткових кур'єрів

знімаємо чергу на Хрещатику (оновлення о 18:00). Ваш час цінний. Дякуємо, що ви з нами. Детальний план - сьогодні о 18:00.»

Розрахунок KPI реагування:

KPI	Фактичне значення	Цільове значення	Результат
Response Time (RT)	33 хвилини	< 60 хвилин	ВИКОНАНО
Зниження CV за 2 год після першої відповіді	-36% (1 400 → 900 зг/год)	-30%	ВИКОНАНО
Покриття ЗМІ з коментарем компанії	2 з 2 видань	≥ 1 видання	ВИКОНАНО
NSS через 6 год після першої відповіді	-22%	> -25%	ВИКОНАНО

Таблиця 8. KPI реагування Nova Poshta - фактичні vs. цільові значення

C - Correct (48 годин): Динаміка відновлення NSS

Протягом 48 годин після початку кризи команда публікувала оновлення кожні 2-6 годин з конкретними цифрами. Нижче наведено динаміку ключових метрик.

Часова мітка	NSS	CV (зг/год)	Рівень тривоги	Ключова дія
14:32 (старт)	-38%	1 400	Помаранч.	Виявлення кризи
15:05 (+33 хв)	-35%	1 200	Помаранч.	Перша реакція опублікована
17:05 (+2 год)	-28%	900	Жовтий	Зниження CV після реакції. Прес-брифінг.
18:00 (+3,5 год)	-22%	650	Жовтий	Розгорнуте оновлення + оголошення компенсацій
День 2 (24 год)	-15%	380	Жовтий	«День 2: черга ≤ 20 хв». SMS клієнтам.
День 7 (7 діб)	-8%	180	Зелений	Норма CV відновлена. NSS на виході з кризи.
День 14	-12%	150	Зелений	Стабілізація. Перехід до посткризового плану.
День 30	+4%	120	Зелений	Відновлення до докризового рівня

Таблиця 9. Динаміка метрик Nova Poshta під час кризи та відновлення (Варіант 1)

L - Learn (через 3 тижні): Post-Crisis Аналіз

Показник	Фактичне значення	Висновок / Урок
Час виявлення кризи (М-крок)	0 хв (автосповіщення Brand24)	Система моніторингу працює. Залишити налаштування.
Response Time (R-крок)	33 хвилини	Нижче еталону 60 хв. Шаблони спрацювали.
Час відновлення NSS до норми	30 днів (до +4%)	Значно краще за середній показник 14 міс. без Playbook.
Покриття ЗМІ без коментаря компанії	0 із 2 видань	Прес-брифінг о 17:30 забезпечив коментар у всіх матеріалах.
Превентивні заходи до пікового сезону	Відсутні (реакція в режимі кризи)	Ключовий урок: залучити 800 кур'єрів заздалегідь. Відкрити дод. пункти до 10 грудня.
Поріг жовтого рівня у грудні	300 зг/год (загальний)	Урок: у грудні знизити до 150 зг/год. Оновити Playbook.

Таблиця 10. Post-Crisis аналіз Nova Poshta - уроки та оновлення Playbook

Частина 4. Посткризовий план відновлення репутації

Зведений план відновлення репутації з метриками та дедлайнами

Стратегія	Конкретні заходи	Строки	Цільовий KPI	Відповідальний
Content Rehabilitation	Серія публікацій «Як ми вирішили проблему», відео з нових відділень, блог-пости, інтерв'ю з операційним директором	Тижні 1-8	Топ-5 результатів пошуку = нейтральні/позитивні через 8 тиж.	SMM-менеджер + контент-менеджер
Third-Party Validation	15-20 мікроінфлюенсерів e-commerce + заява партнера (Rozetka) + незалежне дослідження задоволеності	Тижні 2-6	≥ 15 публікацій інфлюенсерів з позитивним тоном. ER ≥ 3%	PR-директор + партнерський відділ
Proof of Change	Публічний звіт «Що змінилось»: 45 нових пунктів видачі, час очікування -57%, 800 кур'єрів заздалегідь у грудні, SMS при черзі > 15 хв	Тиждень 4	Охоплення звіту ≥ 100 000. Публікація у ≥ 3 ЗМІ.	Директор з комунікацій + прес-секретар

Community Engagement	Щотижнева рубрика «Ми чуємо вас» (10-15 відповідей на коментарі), 2 × Facebook Live Q&A з операційним директором	Тижні 1-8 (онгоінг)	ER на посткризових публікаціях $\geq 3\%$. Позитивна реакція на Q&A $\geq 70\%$.	SMM-менеджер + операційний директор
-----------------------------	--	---------------------	--	-------------------------------------

Таблиця 11. Зведений посткризовий план відновлення репутації Nova Poshta

Таблиця KPI відновлення репутації

Метрика	Докризовий рівень	Рівень на початку кризи	Ціль через 4 тижні	Ціль через 8 тижнів	Факт день 30
Net Sentiment Score (NSS)	+12%	-38%	$> 0\%$	$\geq +10\%$ (стабільно ≥ 4 тижні)	+4%
Crisis Velocity (CV)	~12 зг/год	1 400 зг/год	< 300 зг/год	< 150 зг/год (сезонна норма грудень)	120
Share of Voice (SoV) у категорії «доставка»	55%	48%	$> 50\%$	$> 52\%$	53%
Engagement Rate (ER) публікацій	2,1%	0,8%	$\geq 3\%$	$\geq 3,5\%$	3,8%
Рейтинг у Google Maps (топ-10 відділень)	4,2 ★	3,6 ★	$\geq 4,0$ ★	$\geq 4,2$ ★	4,1
Органічний пошук (топ-5 за «Nova Poshta відгуки»)	80% нейтр.+позит.	20% нейтр.+позит.	$> 50\%$ нейтр.+позит.	$> 70\%$ нейтр.+позит.	65%

Таблиця 12. KPI посткризового відновлення репутації Nova Poshta з цільовими значеннями та фактичним результатом

Примітка. Відновлення репутації вважається досягнутим, коли NSS повертається до докризового рівня $\pm 5\%$ і залишається стабільним протягом ≥ 4 послідовних тижнів.

ВИМОГИ ДО ОФОРМЛЕННЯ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Структура звіту

Звіт подається у форматі .docx або .pdf. Мінімальний обсяг: 12-15 сторінок. Обов'язкові елементи кожного варіанту: таблиця Матриці вразливостей (≥ 5 сценаріїв) з колонкою $RS = \dot{Y} \times B$; матриця RACI у табличному форматі; таблиця рівнів тривоги з числовими порогоми CV та NSS; хронологічна таблиця MARC-L; розрахункові блоки NSS та CV; таблиця KPI відновлення репутації.

Критерії оцінювання

Частина роботи	Відмінно	Добре	Задовіл.	Обов'язкові елементи для максимальної оцінки
Ч. 1. Vulnerability Audit	18-20	14-17	10-13	≥ 5 вразливостей з розрахунком $RS = \dot{Y} \times B$; таблиця з кольоровим кодуванням; конкретні платформи ризику
Ч. 2. Crisis Playbook	23-25	18-22	13-17	Матриця RACI у таблиці; 4 рівні тривоги з числовими порогоми CV і NSS; 3 шаблони реакції у форматі готових текстів
Ч. 3. Антикризова стратегія MARC-L	27-30	22-26	15-21	Хронологічна таблиця з часовими мітками; розрахункові блоки NSS та CV; таблиця KPI реагування (факт vs. ціль); текст першої реакції у повному обсязі
Ч. 4. Посткризовий план	14-15	11-13	7-10	4 стратегії з конкретними заходами та строками; таблиця KPI відновлення з числовими цілями та факт. результатами
Оформлення та посилання	9-10	7-8	5-6	≥ 12 сторінок; таблиці та розрахункові блоки; посилання на статті; список літератури ≥ 10 джерел
РАЗОМ	100	72-89	50-71	

Таблиця 13. Критерії оцінювання лабораторно-практичної роботи

ВИСНОВКИ

Виконання цієї лабораторно-практичної роботи формує у студента комплексне розуміння кризового менеджменту як системної дисципліни, що базується на числових метриках, а не лише на інтуїції.

Crisis Playbook з матрицею RACI та числовими порогами Alert Levels дозволяє скоротити Response Time з годин до хвилин - саме ця різниця визначає, чи залишиться криза під контролем. Протокол MARC-L із розрахунком CV та NSS на кожному кроці перетворює хаотичну реакцію на керований процес. Посткризовий план з вимірними КРІ забезпечує системне відновлення репутації.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Бідочко Л., Піворак О., Худіш П., Рощина А. Як російська пропаганда діє в медійному просторі Глобального Півдня. *Гламом*. 19 квіт. 2023. 15:15. URL: <https://glavcom.ua/digest/jak-rosijska-propaganda-dije-v-medijnomu-prostori-hlobalnoho-pivdnja-921574.html> (дата звернення: 30.04.2025).
2. Дзяна Г. О., Дзяний Р. Б. Управління комунікаціями в умовах криз. *Дніпровський науковий часопис публічного управління, психології, права*, № 2, 2022. С. 15–21.
3. Комунікаційний інструментарій для державних службовців з фокусом на європейській інтеграції та Угоді про асоціацію між Україною та ЄС / Л. Косар, Я. Камініс, Е. Халісте та ін. Київ, 2018. URL: <https://lms.kmu.gov.ua/association4u/communication-toolkit>
4. Кризові комунікації в умовах надзвичайних ситуацій : колективна монографія / С. П. Потеряйко, А. В. Терент'єва, О. С. Твердохліб, К. Г. Белікова. Київ : ІДУНДЦЗ, 2023. 208 с. URL: https://lms.kmu.gov.ua/sites/default/files/uploads/user_4/communication-toolkit-a4u-mip-ukr.pdf
5. Мудрак Л. 8 правил кризових комунікацій – поради для місцевого самоврядування. Портал «Децентралізація». URL: <https://decentralization.ua/news/12353>
6. Оліндер Г. Кризові комунікації – до, під час і після. Стокгольм, 2023. URL: <https://hromady.org/wp-content/uploads/2023/04/Презентація-Кризові-комунікації-освітній-підхід.pdf>
7. Онлайн-курс із кризових комунікацій. Освітній портал «Європейський простір». URL: <https://euproster.org.ua/courses/149183>
8. Що таке комунікаційна стратегія та як її побудувати? Школа Бізнесу. URL: <https://online.novaposhta.education/blog/shho-take-komunikacijna-strategiya-ta-yak-ii-pobuduvati>
9. Сучасні комунікаційні стратегії. Європейська Бізнес Асоціація (European Business Association). URL: <https://eba.com.ua/suchasni-komunikatsijni-strategiyi-shho-novogo/>
10. Демченко О. П'ять помилок, що провокують неякісну комунікацію в бізнесі. Освітній портал Education.ua. URL: <https://www.education.ua/blog/47410/>

11. Коник Д. Кризові комунікації органів місцевого самоврядування : практичний посібник. URL: <https://auc.org.ua/sites/default/files/library/crisis-communications-guide.pdf>
12. Ефективні комунікації: Чому? Як? Для кого? Коли? Де? Громадський Простір. URL: <https://www.prostir.ua/?kb=efektyvni-komunikatsiji-chomu-yak-dlya-koho-koly-de-3>
13. Методи та канали зв'язку в плані комунікацій проєкту. Навчальний ресурс FoxmindED. URL: <https://foxminded.ua/plan-komunikatsii-proiektu/#:~:text=частиною%20проєктного%20менеджменту,-,Що%20це%20таке?,проєкту%20та%20його%20зацікавленими%20сторонами>
14. Почепцов Г. Сучасні інформаційні війни. Всеукраїнська експертна мережа. URL: http://www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=112800
15. FIMI: на шляху до європейського переосмислення іноземного втручання. Європейський ресурс з протидії дезінформації Disinfo.eu. URL: <https://www.disinfo.eu>
16. Кембриджський словник (Cambridge Dictionary). URL: <https://dictionary.cambridge.org/dictionary/english/disinformatio>

ЛАБОРАТОРНА РОБОТА 7-10. ПРАВОВИЙ І ЕТИЧНИЙ АУДИТ МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ.

ВСТУП

Робота є логічним продовженням лекції 6 «Правові та етичні аспекти моніторингу соціальних мереж». Якщо лекція сформувала теоретичне розуміння правових вимог GDPR, умов використання платформ та етичних принципів, то дана робота переводить ці знання у площину практичного застосування.

Знання правових норм набуває сенсу лише тоді, коли фахівець здатний оцінити конкретний сценарій на відповідність цим нормам і розробити систему, що відповідає одночасно правовим вимогам, умовам платформ та етичним стандартам. Це є ключовою компетентністю аналітика соціальних мереж в умовах, коли штрафи GDPR перевищують 4,5 мільярда євро, а порушення умов API призводить до блокування інструментів і судових позовів.

Актуальна статистика застосування GDPR доступна на ресурсі GDPR Enforcement Tracker: <https://www.enforcementtracker.com/>

Кожен студент отримує власний варіант - унікальну комбінацію типу організації та сценарію моніторингу, для яких необхідно провести правовий і етичний аудит та розробити Ethical Monitoring Charter (Хартію відповідального моніторингу). Усі варіанти передбачають однакову структуру завдань, але для різних організаційних контекстів.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Основні поняття та аббревіатури

Перш ніж розпочати виконання роботи, необхідно ознайомитися з основними термінами та аббревіатурами, що використовуються у завданнях.

Абревіатура / Термін	Повна назва	Пояснення
GDPR	General Data Protection Regulation - Загальний регламент ЄС про захист даних	Регламент ЄС 2016/679, чинний з 25 травня 2018 р. Захищає персональні дані громадян ЄС. Повний текст: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
ПД	Персональні дані	Будь-яка інформація, що стосується ідентифікованої або ідентифіковної фізичної особи (суб'єкта даних)

ToS	Terms of Service - Умови використання / Умови надання послуг	Юридично обов'язковий договір між платформою та користувачем. Порухення ToS може призвести до блокування акаунту або судового позову
API	Application Programming Interface - Інтерфейс програмування застосунків	Офіційний технічний інтерфейс доступу до даних платформи. Використання API є правомірним методом збору даних
PIA / DPIA	Privacy Impact Assessment / Data Protection Impact Assessment - Оцінка впливу на приватність / Оцінка впливу на захист даних	Обов'язковий документ (ст. 35 GDPR) перед запуском системи, що обробляє великі масиви персональних даних. Оцінює ризики та заходи їх мінімізації
DPO	Data Protection Officer - Уповноважений із захисту даних	Посадова особа, відповідальна за дотримання вимог GDPR в організації. Обов'язкова посада для певних типів організацій
CISO	Chief Information Security Officer - Директор з інформаційної безпеки	Керівник підрозділу, відповідального за кібербезпеку та захист інформації в організації
LIA	Legitimate Interest Assessment - Оцінка законного інтересу	Документований тристадійний тест для обґрунтування обробки даних на підставі ст. 6(1)(f) GDPR
PbD	Privacy by Design - Приватність за здумом	Принцип проектування систем, за яким захист даних вбудовується від початку розробки (ст. 25 GDPR)
Scraping / Парсинг	Web scraping - автоматизований збір даних із веб- сторінок	Технічний метод збору даних без офіційного API. Як правило, є порушенням ToS платформ
Sentiment- аналіз	Аналіз тональності тексту	Автоматичне визначення емоційного забарвлення тексту (позитивне / нейтральне / негативне). Є похідними персональними даними

Таблиця 1. Основні аббревіатури та терміни роботи

Розшифрування посилань на статті GDPR

У методичних матеріалах та прикладі виконання використовуються посилання на конкретні статті GDPR. Нижче наведено детальне пояснення кожного посилання та де знайти первинне джерело.

Ст. 4(1) GDPR - Визначення персональних даних.

Стаття 4, пункт 1. «Персональні дані» означають будь-яку інформацію, що стосується ідентифікованої або ідентифікованій фізичної особи («суб'єкта даних»); ідентифікованою фізичною особою є та, яку можна ідентифікувати прямо або опосередковано, зокрема за допомогою ідентифікатора, такого як ім'я, ідентифікаційний номер, дані про місцезнаходження, мережевий ідентифікатор або за допомогою одного чи кількох факторів, що стосуються фізичної, фізіологічної, генетичної, психічної, економічної, культурної або соціальної ідентичності цієї фізичної особи.

Де знайти: офіційний текст GDPR англійською мовою: <https://eur-lex.europa.eu/legal-content/EN/TXT/>.
Неофіційний українськомовний переклад: https://zakon.rada.gov.ua/laws/show/995_i63

Ст. 4(4) GDPR - Визначення профілювання.

Стаття 4, пункт 4. «Профільовання» означає будь-яку форму автоматизованої обробки персональних даних, що полягає у використанні таких даних для оцінки певних особистих аспектів, що стосуються фізичної особи, зокрема для аналізу або прогнозування аспектів, пов'язаних з результатами роботи на виробництві, економічним становищем, станом здоров'я, особистими уподобаннями, інтересами, надійністю, поведінкою, місцезнаходженням або переміщеннями.

Ст. 5 GDPR - Сім принципів обробки персональних даних.

Ст. 5(1)(a) - законність, справедливість, прозорість; Ст. 5(1)(b) - обмеження мети; Ст. 5(1)(c) - мінімізація даних; Ст. 5(1)(d) - точність; Ст. 5(1)(e) - обмеження зберігання; Ст. 5(1)(f) - цілісність і конфіденційність; Ст. 5(2) - підзвітність.

Ст. 6(1)(f) GDPR - Законний інтерес як правова підстава обробки.

Обробка є законною, якщо вона необхідна для цілей законних інтересів, яких прагне досягти контролер або третя сторона, крім випадків, коли такі інтереси переважають інтереси чи основоположні права і свободи суб'єкта даних. УВАГА: ця підстава вимагає обов'язкового тристадійного тесту LIA.

Ст. 9 GDPR - Спеціальні категорії персональних даних.

Забороняється обробка даних, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках, генетичні дані, біометричні дані з метою однозначної ідентифікації фізичної особи, дані про здоров'я, дані про статеве життя або сексуальну орієнтацію. Обробка можлива лише при наявності однієї з підстав ст. 9(2): явна згода, обробка у сфері трудового права, захист інтересів тощо. Фотографії авторів, якщо вони дозволяють ідентифікувати особу, є БІОМЕТРИЧНИМИ ДАНИМИ і підпадають під ст. 9.

Ст. 12(3) GDPR - Строк відповіді на запити суб'єктів.

Контролер надає суб'єкту даних інформацію про заходи, вжиті за запитом відповідно до статей 15-22, без необґрунтованих затримок і в будь-якому випадку протягом одного місяця з моменту отримання запиту. Цей строк може бути продовжений ще на два місяці з урахуванням складності і кількості запитів.

Ст. 25 GDPR - Privacy by Design (Приватність за задумом).

Контролер зобов'язаний як під час визначення засобів обробки, так і під час самої обробки впроваджувати належні технічні та організаційні заходи, розроблені для ефективного дотримання принципів захисту даних.

Ст. 33 GDPR - Повідомлення про порушення захисту даних наглядовому органу.

У разі порушення захисту персональних даних контролер без необґрунтованих затримок і, якщо можливо, не пізніше 72 годин після того, як йому стало відомо про порушення, повідомляє про нього компетентний наглядовий орган. **ВАЖЛИВО:** в Україні наглядовий орган - Уповноважений Верховної Ради України з прав людини (Омбудсмен). Контакт: <https://www.ombudsman.gov.ua/>

Ст. 34 GDPR - Повідомлення суб'єктів даних про порушення.

Якщо порушення захисту персональних даних може спричинити високий ризик для прав і свобод фізичних осіб, контролер без необґрунтованих затримок повідомляє суб'єкта даних про таке порушення. Повідомлення має бути зрозумілою мовою.

Ст. 35 GDPR - Оцінка впливу на захист даних (DPIA / PIA).

Якщо певний вид обробки, зокрема із застосуванням нових технологій, та з урахуванням характеру, обсягу, контексту і цілей обробки може становити високий ризик для прав і свобод фізичних осіб, контролер до початку обробки проводить оцінку впливу запланованих операцій обробки на захист персональних даних. PIA є обов'язковою при масовому моніторингу соціальних мереж.

3. Правові підстави обробки даних у моніторингу соціальних мереж

GDPR (Regulation (EU) 2016/679) визначає шість правових підстав для обробки персональних даних (стаття 6). Для моніторингу соціальних мереж практично релевантними є дві з них.

Згода суб'єкта даних (стаття 6(1)(a)). Підходить для ситуацій, коли організація має прямий контакт із суб'єктами і може отримати явну згоду. Для масового моніторингу публічних соціальних мереж ця підстава, як правило, є непрактичною.

Законний інтерес контролера (стаття 6(1)(f)). Найпоширеніша підстава для комерційного моніторингу. Вимагає проходження тристадійного тесту: (1) ідентифікація конкретного законного інтересу; (2) перевірка необхідності обробки для досягнення цього інтересу; (3) балансування інтересів контролера та прав суб'єктів. Якщо інтереси суб'єктів переважають - ця підстава не може застосовуватись.

Важливо: публічність даних НЕ є самостійною правовою підставою. Принцип контекстної цілісності (Nissenbaum H. Privacy as Contextual Integrity. Washington Law Review, 2004, Vol. 79(1), P. 119-157) стверджує: публічний пост опублікований в одному контексті і не дає дозволу на будь-яке використання. Автоматизований масовий збір, агрегація та профілювання є принципово іншими діями, ніж читання окремих публічних публікацій, і вимагають окремого обґрунтування.

4. Умови використання платформ (ToS) як правовий обмежувач

Умови використання соціальних мереж є юридично обов'язковими договорами. Їх порушення може спричинити блокування акаунтів і токенів доступу, судові позови, адміністративні санкції.

Instagram Graph API (офіційний). Дозволяє збирати дані власного бізнес-акаунту та публікації, в яких відмічено бізнес-акаунт. Документація: <https://developers.facebook.com/docs/instagram-api/>. Meta Platform Terms (2024) забороняє скрапінг без дозволу: <https://developers.facebook.com/terms/>

TikTok Research API (офіційний). Доступний для академічних досліджень та схвалених організацій. Документація: <https://developers.tiktok.com/products/research-api/>. TikTok Terms of Service (розділ 5, 2023) забороняє автоматизований збір: <https://www.tiktok.com/legal/page/eea/terms-of-service/en>

LinkedIn. LinkedIn User Agreement прямо забороняє scraping будь-яких даних без письмового дозволу: <https://www.linkedin.com/legal/user-agreement>

Twitter/X Developer Agreement (2023). Забороняє масовий збір та повторне використання даних для навчання AI без окремої ліцензії: <https://developer.twitter.com/en/developer-terms/agreement-and-policy>

Прецедент LinkedIn Corp. v. hiQ Labs (2022). Верховний суд США підтвердив право платформ забороняти scraping навіть публічних даних. Цей прецедент враховується при розгляді аналогічних справ у ЄС: <https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf>

Мета роботи

Сформувати практичні навички правового та етичного аудиту систем моніторингу соціальних мереж і розробки нормативних документів, що регламентують відповідальне використання даних.

Завдання роботи

- провести правовий аудит запропонованого сценарію моніторингу: визначити правові підстави обробки даних, права суб'єктів та відповідність ключовим вимогам GDPR;

- здійснити аудит відповідності умовам використання платформ (ToS), оцінити правомірність методів збору даних та виявити потенційні порушення;
- провести етичний аудит за трьома принципами (приватність, пропорційність, прозорість) та заповнити практичний чеклист відповідального моніторингу;
- розробити Ethical Monitoring Charter (Хартію відповідального моніторингу) - внутрішній нормативний документ;
- скласти план реагування на запити суб'єктів даних та план дій у разі виявлення витоку даних (Data Breach Response Plan).

Загальна структура роботи

Робота складається з чотирьох обов'язкових частин, що виконуються послідовно у вказаному порядку.

Частина	Назва	Що потрібно зробити
Частина 1	Правовий аудит	Реєстр даних, тест LIA, таблиця відповідності GDPR, права суб'єктів
Частина 2	Аудит ToS платформ	Граф потоку даних в Excel, реєстр порушень ToS
Частина 3	Етичний аудит	Радар-діаграма в Excel, чеклист, PIA Risk Score в Excel
Частина 4	Ethical Monitoring Charter та плани реагування	Хартія, план відповіді на запити, Data Breach Response Plan

Таблиця 2. Структура лабораторно-практичної роботи

ДЕТАЛЬНІ ІНСТРУКЦІЇ ДО ВИКОНАННЯ КОЖНОЇ ЧАСТИНИ

ЧАСТИНА 1. ПРАВОВИЙ АУДИТ СЦЕНАРІЮ МОНІТОРИНГУ

Крок 1.1. Ідентифікація та класифікація даних - Реєстр даних

Що треба зробити: скласти таблицю-реєстр усіх категорій даних, які збирає система моніторингу згідно з умовами вашого варіанту. Для кожної категорії даних потрібно визначити три речі: правовий статус за GDPR, правову підставу обробки і рівень ризику.

Покрокова інструкція виконання:

1. Уважно прочитайте опис свого варіанту. Випишіть усі типи даних, що згадуються (наприклад: username, текст публікацій, фото, геолокація, кількість підписників тощо).
2. Для кожного типу даних визначте правовий статус: задайте собі питання - чи можна за цими даними ідентифікувати конкретну людину? Якщо так - це

- персональні дані (ПД) за ст. 4(1) GDPR. Якщо дані стосуються раси, здоров'я, біометрії, релігії, сексуальної орієнтації - це спеціальні категорії ПД за ст. 9 GDPR.
3. Username (нік у соціальній мережі) - це ПРЯМИЙ ідентифікатор особи за ст. 4(1) GDPR, навіть якщо це не справжнє ім'я. Чому? Тому що за username можна знайти конкретного користувача і всі його публікації. Username = персональні дані.
 4. Фотографії авторів - це персональні дані за ст. 4(1). Якщо система може розпізнавати обличчя на фото - це БІОМЕТРИЧНІ ДАНІ, спеціальна категорія за ст. 9 GDPR. Обробка без спеціальної правової підстави - заборонена.
 5. Геолокація - персональні дані за ст. 4(1), оскільки розкриває місцеперебування особи.
 6. Sentiment-оцінка (автоматичний висновок про тональність публікації особи) - це похідні персональні дані, результат профілювання за ст. 4(4) GDPR.
 7. Кількість підписників САМА по собі - не є персональними даними. АЛЕ якщо вона зберігається разом з username в одному записі - вона стає частиною профілю особи і набуває статусу ПД.
 8. Оформіть результати у таблицю за зразком Таблиці 1 прикладу виконання (Варіант 1). Таблиця повинна містити: Категорія даних / Правовий статус / Правова підстава (стаття GDPR) / Рівень ризику.

Де взяти статтю GDPR? Відкрийте офіційний текст GDPR: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>. Стаття 4 - в першій частині документу. Визначення «персональних даних» - ст. 4(1). Визначення «спеціальних категорій» - ст. 9.

Крок 1.2. Тест на законний інтерес (LIA) - Тристадійний тест

Що треба зробити: перевірити, чи може обробка даних у вашому сценарії спиратися на правову підставу «законний інтерес» за ст. 6(1)(f) GDPR. Цей тест складається рівно з трьох стадій, які потрібно пройти послідовно.

Покрокова інструкція виконання:

9. **СТАДІЯ 1 - Ідентифікація законного інтересу.** Запитайте: «Навіщо організація збирає ці дані? Яка конкретна мета?» Мета повинна бути конкретною (не «для покращення сервісу»), законною (не суперечити закону), та реальною (організація дійсно її переслідує). Приклад для варіанту 1: «Моніторинг репутації власного бренду в соціальних мережах» - конкретна і законна мета. «Аналіз публікацій конкурентів» - окрема мета, потребує окремого обґрунтування.
10. **СТАДІЯ 2 - Необхідність обробки.** Запитайте: «Чи є цей спосіб збору даних мінімально достатнім для досягнення мети? Чи можна досягти тієї самої мети,

збираючи менше даних?» Якщо для аналізу репутації достатньо тексту публікацій, то збір username, геолокації та фото є НАДЛИШКОВИМ і не пройде цю стадію.

11. **СТАДІЯ 3 - Балансування інтересів.** Запитайте: «Чи не переважають інтереси та права суб'єктів даних над інтересами організації?» Потрібно врахувати: чи можуть суб'єкти розумно очікувати таку обробку? Чи завдає обробка їм шкоди? Чи є додаткові гарантії захисту? Масове профілювання та необмежене зберігання, як правило, НЕ проходять тест балансування.

12. Оформіть результати у таблицю за зразком Таблиці 2 прикладу виконання. Для кожної стадії: сформулюйте питання, опишіть відповідь конкретно для вашого сценарію, вкажіть результат (пройдено / не пройдено).

Де взяти первинне джерело? Текст ст. 6(1)(f) GDPR: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#d1e1797-1-1>. Роз'яснення WP29 (Working Party 29) щодо законного інтересу: <https://ec.europa.eu/newsroom/article29/items/47812>

Крок 1.3. Профіль ризиків GDPR - Побудова діаграми в Excel

Що треба зробити: оцінити відповідність системи кожному з ключових принципів GDPR (ст. 5) та побудувати РАДАР-ДІАГРАМУ в Microsoft Excel або Google Sheets.

Що таке Радар-діаграма? Радар-діаграма (Radar Chart, також Spider Chart або Web Chart) - це вид діаграми, де кожна вісь відповідає окремому показнику, а значення відображаються у вигляді багатокутника. Використовується для одночасного порівняння кількох параметрів. У нашому випадку - відповідність кожному принципу GDPR.

Покрокова інструкція побудови Радар-діаграми в Excel:

1. Відкрийте Microsoft Excel (або Google Sheets: <https://sheets.google.com>).
2. Оцініть відповідність системи кожному принципу GDPR за шкалою від 1 до 3, де 1 = критично низький (пряме порушення), 2 = середній (часткова відповідність), 3 = відповідає. Принципи для оцінки: Обмеження мети (ст. 5(1)(b)), Мінімізація даних (ст. 5(1)(c)), Обмеження зберігання (ст. 5(1)(e)), Захист спецкатегорій (ст. 9), Підзвітність (ст. 5(2)).
3. Введіть дані в таблицю в Excel. Перший стовпець - назви принципів. Другий стовпець - ваша оцінка (1, 2 або 3). Третій стовпець - максимальний рівень (3 для всіх) для порівняння.
4. Виділіть усі три стовпці з даними (включаючи заголовки).
5. На вкладці «Вставка» (Insert) натисніть «Інші діаграми» (Other Charts) → «Пелюсткова» (Radar) → виберіть перший тип «Пелюсткова» (або «Radar»). У Google Sheets: Вставка → Діаграма → Тип діаграми: Радарна.
6. Діаграма має показувати два багатокутники: поточний стан (менший) та максимальний рівень (більший). Збережіть файл Excel як окремий додаток до звіту.

Де взяти офіційне пояснення принципів? Ст. 5 GDPR: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#d1e1797-1-1>. Посібник ICO щодо принципів: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/>

Дані для побудови Радар-діаграми профілю ризиків GDPR

Нижче наведено таблицю з конкретними числовими значеннями, за якими побудована радар-діаграма. Введіть ці дані в Excel: стовпець А - назва принципу, стовпець В - поточний рівень, стовпець С - максимальний рівень (3 для всіх). Рядок 1 - заголовки, рядки 2-6 - дані.

Принцип GDPR	Поточний рівень (1-3)	Максимальний рівень (3)
Обмеження мети (ст. 5(1)(b))	2	3
Мінімізація даних (ст. 5(1)(c))	2	3
Обмеження зберігання (ст. 5(1)(e))	2	3
Захист спецкатегорій (ст. 9)	1	3
Підзвітність (ст. 5(2))	2	3

Таблиця А1. Вхідні дані для побудови Радар-діаграми профілю ризиків GDPR (Варіант 1)

Як будувати в Excel: (1) Введіть дані з Таблиці А1. (2) Виділіть діапазон А1:С6 (всі три стовпці з заголовками). (3) Вкладка «Вставка» → «Інші діаграми» → «Пелюсткова». У Google Sheets: Вставка → Діаграма → Тип: Радарна. (4) Відформатуйте: ряд «Поточний рівень» - червоним, «Максимальний рівень» - синім або пунктирною лінією. (5) Додайте заголовок діаграми: «Профіль ризиків GDPR - Варіант 1».

Для чого потрібна ця діаграма: Радар-діаграма дозволяє одночасно побачити рівень відповідності системи всім п'яти принципам GDPR (ст. 5) та миттєво ідентифікувати «слабкі осі». У нашому прикладі вісь «Захист спецкатегорій (ст. 9)» отримала оцінку 1 (критичний рівень) - це чітко видно на діаграмі як «провал». Діаграма є обов'язковим елементом звіту: вона слугує доказом проведення РІА та виконання принципу підзвітності (ст. 5(2) GDPR). Нижче наведено готовий приклад діаграми, побудованої за цими даними.

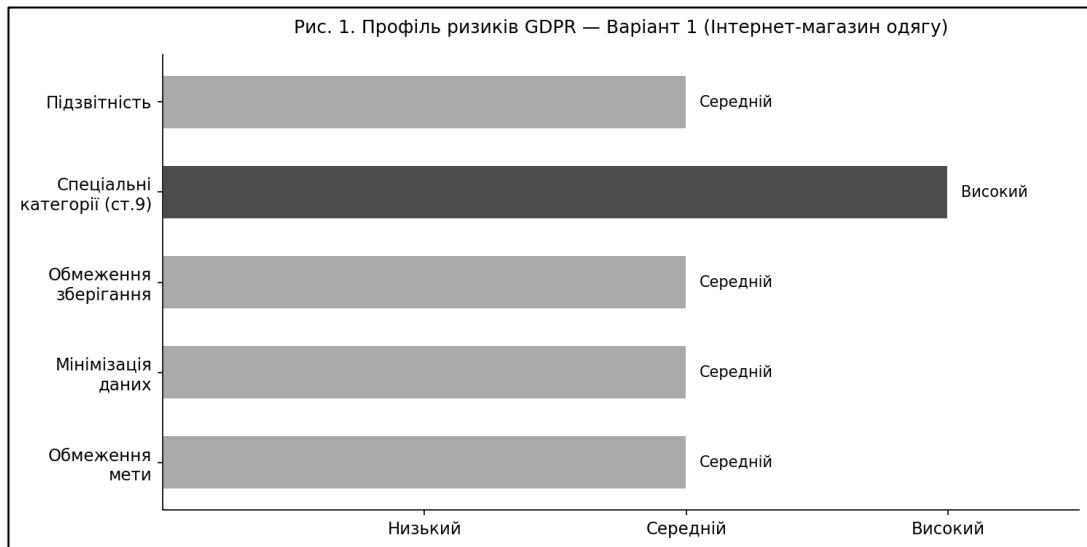


Рис. 1. Профіль ризиків GDPR - Варіант 1 (оцінка до впровадження рекомендацій)

ЧАСТИНА 2. АУДИТ ВІДПОВІДНОСТІ УМОВАМ ВИКОРИСТАННЯ ПЛАТФОРМ (ToS)

Крок 2.1. Граф потоків даних - Побудова DFD (Data Flow Diagram) в Excel

Що таке Граф потоку даних (DFD)? DFD (Data Flow Diagram - Діаграма потоків даних) - це схема, що показує, звідки дані надходять, куди передаються, де зберігаються і хто їх обробляє. Складається з чотирьох елементів: Джерело даних (зовнішній об'єкт, наприклад «Instagram»), Процес обробки (наприклад «Парсинг публікацій»), Сховище даних (наприклад «База даних системи»), Потік даних (стрілка між елементами).

Покрокова інструкція побудови DFD в Excel:

1. Відкрийте Microsoft Excel.
2. На вкладці «Вставка» (Insert) натисніть «Фігури» (Shapes). Вам знадобляться: Прямокутник із заокругленими кутами - для процесів обробки, Паралелограм або прямий прямокутник - для зовнішніх об'єктів (платформ), Циліндр або прямокутник з подвійною рисою - для сховищ даних, Стрілки - для потоків даних між елементами.
3. Намалуйте схему: починайте з джерел (платформи: Instagram, TikTok тощо) → процеси збору (парсер або API) → первинна база даних → процеси аналізу → вторинне сховище (звіти) → отримувачі (відділ маркетингу тощо).
4. На кожній стрілці підпишіть, ЯКІ САМЕ ДАНІ передаються (наприклад: «username + текст + геолокація»).

5. **КРИТИЧНО ВАЖЛИВО:** позначте червоним кольором (або червоною стрілкою) точки, де відбувається ПОРУШЕННЯ ToS або GDPR. Це робиться, щоб наочно показати проблемні місця в системі.

6. Збережіть файл Excel та вставте скріншот або копію схеми у звіт Word, або додайте файл як додаток.

7. **Альтернатива:** DFD можна побудувати у безкоштовному онлайн-сервісі draw.io (<https://app.diagrams.net/>) - там є готові шаблони DFD. Після побудови схеми експоруйте її як зображення (PNG або JPG) і вставте у звіт.

Крок 2.2. Реєстр порушень ToS

Що треба зробити: скласти таблицю всіх виявлених порушень умов використання платформ. Для кожного порушення треба вказати: що саме робить система, який конкретний пункт ToS це порушує, яка платформа, рівень ризику і рекомендацію.

Покрокова інструкція виконання:

1. Визначте метод збору даних у вашому варіанті: офіційний API чи неофіційний парсер (scraping).

2. Якщо використовується ПАРСИНГ (scraping): відкрийте умови відповідної платформи. Для Instagram: <https://developers.facebook.com/terms/>. Для TikTok: <https://www.tiktok.com/legal/page/eea/terms-of-service/en>. Для LinkedIn: <https://www.linkedin.com/legal/user-agreement>

3. Знайдіть у тексті ToS розділи, що стосуються автоматизованого збору даних. Для Meta (Facebook/Instagram) це Розділ 3 Platform Terms. Для TikTok - Розділ 5 Terms of Service. Запишіть точні посилання на ці пункти у таблицю.

4. Оформіть таблицю за зразком Таблиці 4 прикладу виконання.

ЧАСТИНА 3. ЕТИЧНИЙ АУДИТ

Крок 3.1. Радар-діаграма «Поточний стан vs. Необхідний рівень» в Excel

Що треба зробити: оцінити систему за трьома принципами етичного моніторингу (приватність, пропорційність, прозорість) і побудувати РАДАР-ДІАГРАМУ в Excel, що показує поточний стан (червоним) і мінімально необхідний рівень (зеленим).

Три принципи та шкала оцінювання:

- Приватність (Privacy): чи поважається право авторів на контроль над власними даними? 1 = критично (обробляються надлишкові дані та спецкатегорії), 3 = задовільно (мінімальні дані), 5 = відмінно (мінімум даних + анонімізація).

- Пропорційність (Proportionality): чи відповідає масштаб збору меті? 1 = критично (масове профілювання без обґрунтованої мети), 3 = задовільно (мета обґрунтована, але методи надмірні), 5 = відмінно (найменш інвазивний метод).
- Прозорість (Transparency): чи знають суб'єкти про обробку? 1 = критично (ніякого Privacy Notice), 3 = задовільно (обмежений Privacy Notice), 5 = відмінно (повний Privacy Notice + повідомлення суб'єктів).

Покрокова інструкція побудови Радар-діаграми в Excel:

1. Відкрийте Excel, введіть таблицю: Рядок 1 (заголовки): Принцип | Поточний стан | Необхідний рівень. Рядок 2: Приватність | [ваша оцінка 1-5] | 3. Рядок 3: Пропорційність | [ваша оцінка 1-5] | 3. Рядок 4: Прозорість | [ваша оцінка 1-5] | 3.
2. Виділіть всю таблицю (включаючи заголовки).
3. Вставка → Діаграми → Інші діаграми → Пелюсткова (Radar). У Google Sheets: Вставка → Діаграма → Тип: Радарна.
4. Відформатуйте: ряд «Поточний стан» - червоним кольором і суцільною лінією. Ряд «Необхідний рівень» - зеленим кольором і пунктирною лінією.
5. Збережіть діаграму та вставте у звіт.

Дані для побудови Радар-діаграми «Поточний стан vs. Необхідний рівень»

Нижче наведено таблицю з числовими оцінками за трьома принципами етичного моніторингу. Ці дані є основою для побудови радар-діаграми в Excel. Введіть їх точно у такому форматі: стовпець А - назва принципу, стовпець В - поточний стан, стовпець С - необхідний рівень.

Принцип	Поточний стан (1-5)	Необхідний рівень (3)
Приватність (Privacy)	2	3
Пропорційність (Proportionality)	1	3
Прозорість (Transparency)	1	3

*Таблиця А3. Вхідні дані для Радар-діаграми «Поточний стан vs. Необхідний рівень»
(Варіант 1)*

Як будувати в Excel: (1) Введіть дані з Таблиці А3. Рядок 1 - заголовки (Принцип | Поточний стан | Необхідний рівень), рядки 2-4 - дані. (2) Виділіть весь діапазон А1:С4. (3) Вставка → Інші діаграми → Пелюсткова (Radar). (4) Форматування: ряд «Поточний стан» - суцільна червона лінія; ряд «Необхідний рівень» - зелена пунктирна лінія. (5) Заголовок діаграми: «Поточний стан vs. Необхідний рівень». (6) Вставте у звіт.

Для чого потрібна ця діаграма: Ця радар-діаграма наочно показує відстань між поточним станом системи та мінімально прийнятним рівнем (3/5) за кожним із трьох етичних принципів. Два оцінки 1/5 (пропорційність та прозорість) формують маленький «стиснутий» червоний трикутник у порівнянні з зеленим - це миттєво сигналізує перевіряючому або DPO про критичну невідповідність. Діаграма є частиною етичного аудиту та додається до РІА-документації.

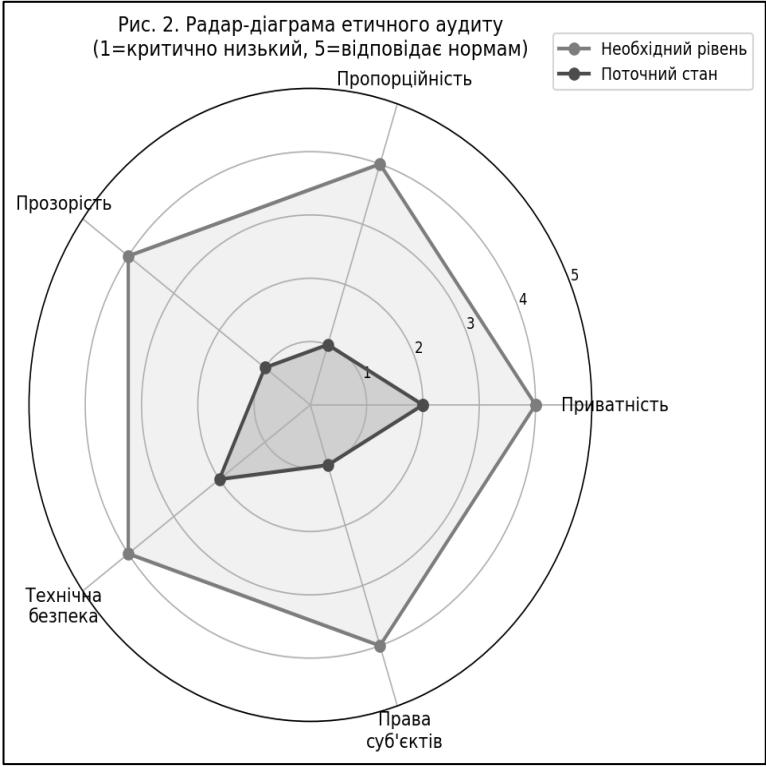


Рис. 3. Радар-діаграма: поточний стан системи (червоний) vs. мінімально необхідний рівень (зелений)

Крок 3.2. Чек лист відповідального моніторингу

Що треба зробити: заповнити таблицю-чеклист з 10 питань. **ВАЖЛИВО:** чеклист НЕ заповнюється у форматі «так/ні». Для кожного пункту потрібно: вказати стан (Так / Ні / Частково / Невідомо / Порушено), написати конкретне обґрунтування із посиланням на норму права або факт зі сценарію, вказати необхідну дію для виправлення.

Приклад правильного та неправильного заповнення:

Питання	НЕПРАВИЛЬНО	ПРАВИЛЬНО
Чи визначена законна правова підстава?	Так	Частково: для тексту публікацій можна обґрунтувати законним інтересом (ст. 6(1)(f) GDPR), але збір username та геолокації не проходить тест балансування. Необхідна дія: обмежити збір лише текстом публікацій.

Таблиця 3. Приклад заповнення чеклисту

Крок 3.3. PIA Risk Score - Побудова стовпчастої діаграми в Excel

Що таке PIA Risk Score? PIA (Privacy Impact Assessment - Оцінка впливу на приватність) - це документована процедура оцінки ризиків для приватності суб'єктів даних перед запуском системи (вимога ст. 35 GDPR). PIA Risk Score - числова оцінка кожного виявленого ризику за шкалою від 1 до 5.

Покрокова інструкція побудови порівняльної діаграми в Excel:

1. Визначте категорії ризику для вашого сценарію (наприклад: Обсяг збору ПД, Риск ідентифікації, Строки зберігання, Методи збору (ToS), Правова підстава, Спецкатегорії).
2. Для кожної категорії оцініть: Score ЗАРАЗ (поточний стан, 1-5) та Score ПІСЛЯ впровадження рекомендацій (що можна покращити, 1-5).
3. Введіть дані в Excel. Стовпець А - назви категорій. Стовпець В - Score зараз. Стовпець С - Score після.
4. Виділіть все → Вставка → Гістограма (Bar Chart) → Згрупована гістограма (Clustered Bar). Або: Стовпчаста діаграма (Column Chart).
5. Додайте горизонтальну лінію «порог прийняттого ризику» на рівні 2: на діаграмі клацніть правою кнопкою → «Додати лінію тренду» або намалюйте лінію вручну. Відформатуйте: стовпці «Score зараз» - червоним, стовпці «Score після» - зеленим.
6. Збережіть файл Excel та вставте діаграму у звіт.

ЧАСТИНА 4. ETHICAL MONITORING CHARTER ТА ПЛАНИ РЕАГУВАННЯ

Дані для побудови стовпчастої діаграми PIA Risk Score

Нижче наведено повну таблицю з числовими оцінками для кожної категорії ризику. Червоним позначено критичні рівні (4-5), зеленим - цільові значення після впровадження рекомендацій. Саме ці числа вводяться в Excel для побудови порівняльної діаграми.

Категорія ризику	Score зараз (1-5)	Score після (1-5)	Ключова дія	GDPR
Обсяг збору ПД (username, геолокація, фото)	3	1	Виключити username, геолокацію	Ст. 5(1)(с)
Риск ідентифікації (профілі авторів)	4	2	Анонімізація перед збереженням	Ст. 4(5)

Строки зберігання (необмежено)	4	1	Встановити 90 днів / 24 місяці	Ст. 5(1)(e)
Методи збору (порушення ToS)	5	1	Перейти на офіційний API	Meta Terms п.3
Правова підстава (LIA не пройдено)	3	2	Документувати LIA для кожної мети	Ст. 6(1)(f)
Спецкатегорії - фото авторів (ст. 9)	5	1	Негайно припинити обробку фото	Ст. 9 GDPR

Таблиця А4. Вхідні дані для стовпчастої діаграми PIA Risk Score (Варіант 1)

Як будувати стовпчасту діаграму в Excel: (1) Введіть дані: стовпець А - назви категорій ризику (6 рядків), стовпець В - Score зараз, стовпець С - Score після. (2) Виділіть діапазон А1:С7 (рядок 1 - заголовки). (3) Вставка → Гістограма → Згрупована гістограма (Clustered Bar) або Стовпчаста (Column Chart). (4) Форматування: стовпці «Score зараз» - червоний колір; стовпці «Score після» - зелений колір. (5) Додайте горизонтальну пунктирну лінію на рівні 2 (поріг прийнятного ризику). Для цього: правою кнопкою на діаграму → «Додати ряд даних» → новий ряд зі значеннями 2 для всіх категорій → змінити тип ряду на «Лінія». (6) Підпишіть вісі: вертикальна - «Рівень ризику (1-5)», горизонтальна - «Категорія ризику». (7) Вставте у звіт.

Для чого потрібна ця діаграма: Стовпчаста діаграма PIA Risk Score - це кількісна частина оцінки впливу на приватність (ст. 35 GDPR). Вона виконує три функції: (а) Порівняння «до/після» - поруч стоять два стовпці для кожної категорії: поточний стан (червоний) і цільовий рівень після виправлень (зелений). Це дозволяє оцінити ефективність запропонованих рекомендацій. (б) Пріоритизація - категорії з оцінкою 5/5 (методи збору, спецкатегорії) відразу видно як найвищі стовпці - це першочергові завдання. (в) Документування PIA - числовий score (24/30 зараз → 8/30 після) є обов'язковим елементом PIA-документа за ст. 35 GDPR та доводить, що організація провела оцінку і розробила план покращення.

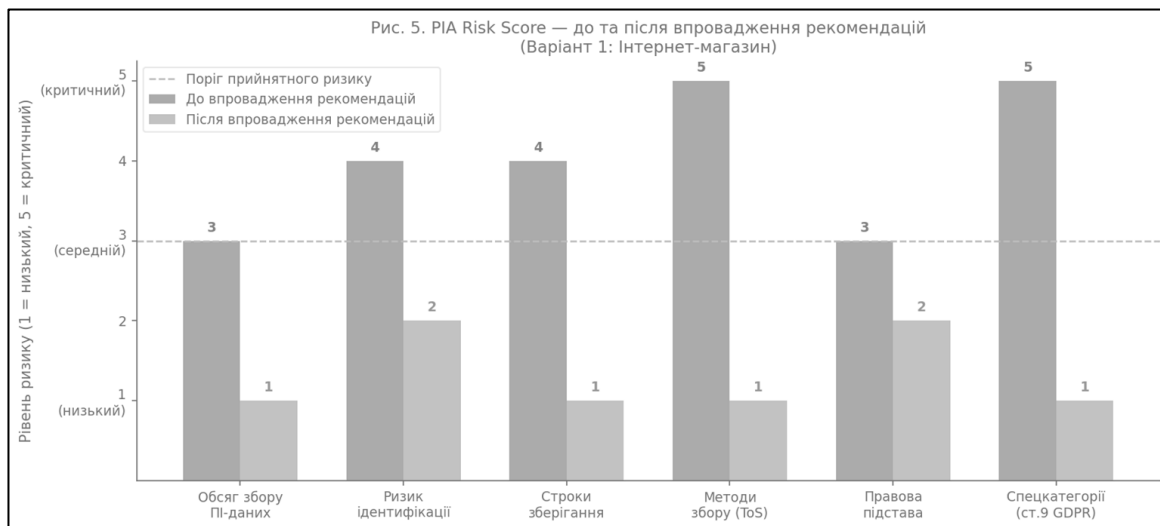


Рис. 4. PIA Risk Score: порівняння поточного стану (червоний) та стану після впровадження рекомендацій (зелений). Пунктирна лінія - поріг прийнятної ризику (2).

Крок 4.1. Ethical Monitoring Charter (Хартія відповідального моніторингу)

Що таке Ethical Monitoring Charter? Це внутрішній нормативний документ організації, який визначає: що дозволено збирати, скільки зберігати, хто має доступ, які дії є забороненими, як реагувати на запити суб'єктів. Наявність Charter є доказом виконання вимоги підзвітності (ст. 5(2) GDPR).

Обов'язкові розділи Charter:

7. Розділ 1. Мета та сфера застосування. Для кого обов'язковий документ (усі співробітники з доступом до системи).
8. Розділ 2. Дозволені цілі моніторингу. Таблиця: Ціль | Дозволені дані | Строк зберігання | Правова підстава.
9. Розділ 3. Заборонені дії. Конкретний перелік (не загальні фрази). Наприклад: «Збір username поза межами відповіді на відгуки».
10. Розділ 4. Дозволені методи збору даних. Виключно офіційні API з вказівкою документації.
11. Розділ 5. Строки зберігання та механізм видалення. Конкретні строки в днях/місяцях + хто відповідає за видалення.
12. Розділ 6. Права суб'єктів даних. Email для запитів + строки відповіді + відповідальна особа.
13. Розділ 7. Перегляд та підзвітність. Щорічний перегляд + відповідальний.

Крок 4.2. План реагування на запити суб'єктів даних

Що треба зробити: розписати покроковий алгоритм дій при отриманні будь-якого запиту від суб'єкта даних. Важливо вказати КОНКРЕТНІ СТРОКИ та ВІДПОВІДАЛЬНИХ осіб. Строки визначені ст. 12(3) GDPR - відповідь протягом 1 місяця (30 днів).

Обов'язкові кроки плану: День 1 - отримання та підтвердження запиту; Дні 2-5 - пошук даних суб'єкта у системі; Дні 6-28 - обробка запиту (доступ / стирання / заперечення); День 30 - надіслати офіційну письмову відповідь. У разі неможливості виконати у строк - повідомити про продовження на 2 місяці (ст. 12(3) GDPR).

Крок 4.3. Data Breach Response Plan (План реагування на витік даних)

Що таке Data Breach? Порухення захисту персональних даних (Data Breach) - це випадкове або незаконне знищення, втрата, зміна, несанкціоноване розкриття або доступ до персональних даних (ст. 4(12) GDPR).

Покрокова інструкція виконання:

1. **0-1 год - Виявлення та оцінка.** Хто виявив? (CISO). Яка кількість записів постраждала? Який тип даних? (звичайні ПД або спеціальні категорії ст. 9). Чи є ризик для прав суб'єктів? Ізолювати систему.

2. **1-24 год - Документування.** Скласти хронологію інциденту. Зафіксувати всі вжиті технічні заходи. Відповідальний: DPO + CISO.

3. **До 72 год - Повідомлення регулятора (ОБОВ'ЯЗКОВО).** За ст. 33 GDPR - повідомити наглядовий орган. В Україні це Уповноважений Верховної Ради з прав людини. Контакт: <https://www.ombudsman.gov.ua/>. Повідомлення має містити: опис інциденту, кількість суб'єктів, типи даних, заходи реагування. **УВАГА:** Порухення 72-годинного строку є самостійною підставою для штрафу до 10 млн євро або 2% від глобального обороту (ст. 83(4) GDPR).

4. **Без затримки - Повідомлення суб'єктів (якщо є «високий ризик»).** За ст. 34 GDPR - повідомити постраждалих зрозумілою мовою. Що сталося, які дані, що вжито, куди звертатись.

5. **Через 2 тижні - Посткризовий аналіз.** Технічний аналіз причин. Оновити Charter та заходи захисту. Задokumentувати для аудиту.

ЗРАЗОК ВИКОНАННЯ - ВАРІАНТ 1

Інтернет-магазин одягу: Правовий і Етичний Аудит Моніторингу

ЧАСТИНА 1. ПРАВОВИЙ АУДИТ СЦЕНАРІЮ МОНІТОРИНГУ

Крок 1.1. Ідентифікація та класифікація даних

Першим кроком правового аудиту є точна інвентаризація всіх даних, що обробляються системою. Нижче наведено реєстр даних із зазначенням правового статусу кожної категорії відповідно до GDPR.

Категорія даних	Правовий статус	Підстава (GDPR)	Риск та пояснення
Username / нік користувача	Персональні дані (ПД)	Ст. 4(1) - будь-який мережевий ідентифікатор	Середній. Прямий ідентифікатор особи. Дозволяє знайти всі публікації конкретного користувача
Текст публікацій	ПД, якщо автор ідентифікований	Ст. 4(1)	Середній. Потребує мінімізації: для аналізу репутації достатньо тексту без збереження username
Геолокація (якщо вказана)	ПД / дані про місцеперебування	Ст. 4(1)	Середній. Розкриває місцеперебування особи. Надлишкова для мети аналізу репутації
Кількість підписників	Не ПД (ізолювано)	- (само по собі не ідентифікує)	Низький. Але якщо зберігається разом з username - стає частиною профілю особи і набуває статусу ПД
Sentiment-оцінка (автоматичний висновок)	Похідні ПД (профіль особи)	Ст. 4(4) - профілювання	Середній. Автоматизований висновок про особу. Потенційно ст. 22 GDPR (автоматизоване прийняття рішень)
Фото авторів (спеціальна умова варіанту)	СПЕЦІАЛЬНА КАТЕГОРІЯ ПД. При ідентифікації осіб - БІОМЕТРИЧНІ ДАНІ	Ст. 9 GDPR (біометричні дані). Обробка заборонена без підстави ст. 9(2)	Критичний. Заборонено без явної згоди або іншої підстави ст. 9(2). Необхідно негайно припинити або отримати правову підставу

Таблиця 4. Реєстр даних системи моніторингу (Варіант 1)

Висновок: система обробляє персональні дані у розумінні ст. 4(1) GDPR. Автори публікацій з ЄС (польська діаспора) підпадають під повний захист GDPR. Обробка фото авторів з ідентифікацією осіб підпадає під ст. 9 GDPR (спеціальні категорії) і є ЗАБОРОНЕНОЮ без окремої правової підстави.

Крок 1.2. Тест на законний інтерес (LIA) - Тристадійний тест

Тест застосовується до обробки персональних даних на підставі ст. 6(1)(f) GDPR (законний інтерес контролера). Нижче наведено результати проходження тесту для сценарію моніторингу інтернет-магазину одягу.

Стадія тесту	Питання для перевірки	Відповідь для сценарію Варіанту 1	Результат
1. Законний інтерес	Чи є інтерес організації конкретним і законним?	Моніторинг репутації власного бренду - конкретна, законна, типова для комерційної організації мета. Аналіз конкурентів - окрема мета, потребує окремого обґрунтування.	Пройдено (лише для власного бренду)
2. Необхідність обробки	Чи є обробка мінімально достатньою для досягнення мети? Чи можна досягти мети, збираючи менше даних?	Текст публікацій - необхідний для аналізу репутації. Username, геолокація, фото - надлишкові. Для аналізу sentiment достатньо тексту без ідентифікатора автора.	Не пройдено (username, фото - зайві)
3. Балансування інтересів	Чи не переважають права суб'єктів над інтересами організації?	Масове профілювання авторів + зберігання необмежено + обробка фото виходять за межі розумних очікувань. Інтереси суб'єктів переважають.	Не пройдено (баланс на користь суб'єктів)

Таблиця 5. Тристадійний тест на законний інтерес (LIA) - Варіант 1

Висновок: збір тексту публікацій (без username) може пройти тест за умови мінімізації та визначення строків зберігання. Збір username, геолокації та фото авторів - НЕ проходить тест у поточному вигляді. Обробка фотографій з розпізнаванням осіб - заборонена без підстави ст. 9 GDPR.

Крок 1.3. Профіль ризиків GDPR - Таблиця відповідності принципам

На основі аудиту відповідності ключовим принципам GDPR (ст. 5) складено профіль ризиків системи. Після виконання цієї таблиці необхідно побудувати Радар-діаграму в Excel (детальна інструкція - у розділі «Детальні інструкції»).

Принцип GDPR	Рівень ризику (1-3)	Конкретне порушення у сценарії	Пріоритет та рекомендація
Обмеження мети (ст. 5(1)(b)): дані збираються лише для вказаних цілей	2 - Середній	Аналіз конкурентів - інша мета, не обґрунтована окремо	Пріоритет 2. Визначити мету аналізу конкурентів окремо або відмовитись
Мінімізація даних (ст. 5(1)(c)): збирати тільки необхідні дані	2 - Середній	Username, геолокація, фото - зайві для мети аналізу репутації	Пріоритет 1. Терміново виключити надлишкові поля зі збору
Обмеження зберігання (ст. 5(1)(e)): не зберігати довше, ніж потрібно	2 - Середній	Зберігання «необмежено» - пряме порушення принципу	Пріоритет 1. Терміново встановити строки: 90 днів для сирих даних, 24 місяці для звітів
Захист спецкатегорій (ст. 9): біометрія, здоров'я, раса тощо	1 - Критичний	Фото авторів обробляються без правової підстави ст. 9	Пріоритет 0. Негайно! Припинити обробку фото або отримати явну згоду за ст. 9(2)(a)
Підзвітність (ст. 5(2)): організація повинна доводити дотримання GDPR	2 - Середній	Відсутній Privacy Notice на сайті та внутрішня документація обробки	Пріоритет 2. Опублікувати Privacy Notice та розробити Charter

Таблиця 6. Відповідність принципам GDPR з оцінкою ризиків (Варіант 1)

Після заповнення таблиці побудуйте **Радар-діаграму в Excel** за інструкцією у розділі «Крок 1.3. Детальні інструкції» та вставте її у звіт. Шкала для діаграми: 1 = критичний, 2 = середній, 3 = відповідає.

ЧАСТИНА 2. АУДИТ ВІДПОВІДНОСТІ УМОВАМ ВИКОРИСТАННЯ ПЛАТФОРМ (ToS)

Крок 2.1. Граф потоків даних (DFD)

Перед аналізом ToS необхідно візуалізувати потоки даних системи для ідентифікації точок, де виникають правові ризики. Побудуйте DFD за інструкцією з розділу «Детальні інструкції до Кроку 2.1» у Excel або draw.io (<https://app.diagrams.net/>).

Схема DFD для Варіанту 1 повинна показувати: Instagram та TikTok (джерела даних) → Неофіційний парсер (точка порушення ToS - позначити червоним) → База даних системи (первинне сховище) → Модуль sentiment-аналізу (обробка) → Звіти (вторинне сховище, передача відділу маркетингу). На кожній стрілці підписати типи переданих даних: «username + текст + геолокація + кількість підписників + фото».

Дані для побудови Графу потоків даних (DFD) - Варіант 1

Нижче наведено таблицю всіх потоків даних системи моніторингу. Червоним виділено критичні точки порушення ToS та GDPR, жовтим - risks середнього рівня. Саме ця таблиця є основою для побудови DFD у Excel або draw.io.

Від (джерело)	Що передається (дані)	До (отримувач)	Порушення
Instagram (публічна стрічка)	username + текст публікацій + геолокація + к-сть підписників + фото	Неофіційний парсер	ToS Meta п. 3; GDPR ст. 9
TikTok (публічна стрічка)	username + текст + відео-метадані + к-сть переглядів + фото	Неофіційний парсер	ToS TikTok розд. 5
Неофіційний парсер	Зібрані записи (всі поля)	База даних системи	GDPR ст. 5(1)(с) - надлишок
База даних системи	Текст + username + sentiment-оцінка	Модуль sentiment-аналізу	GDPR ст. 4(4) - профілювання
Модуль sentiment-аналізу	Профілі авторів + sentiment-оцінки + агреговані метрики	Вторинна база (звіти)	GDPR ст. 5(1)(е) - зберігання ∞
Вторинна база (звіти)	Звіт: топ-авторів, тренди, конкуренти	Відділ маркетингу	-

Таблиця А2. Потоків даних системи моніторингу Instagram/TikTok з позначенням точок порушень (Варіант 1)

Як будувати DFD в Excel або draw.io: ВАРІАНТ А - Excel: (1) Вкладка «Вставка» → «Фігури». Намалюйте: прямокутники з заокругленими кутами для платформ (Instagram, TikTok) - заливка блакитна; прямокутники для процесів (Парсер, Модуль аналізу) - заливка жовта; паралелограми або циліндри для сховищ (База даних, Звіти) - заливка зелена. (2) З'єднайте фігури стрілками. На кожній стрілці підпишіть дані з колонки «Що передається» Таблиці А2. (3) Стрілки та фігури, що відповідають рядкам з порушеннями ToS/GDPR - позначте червоним кольором. ВАРІАНТ Б - draw.io (рекомендований): (1) Відкрийте <https://app.diagrams.net>. Виберіть шаблон «Data Flow Diagram». (2) Перетягніть елементи відповідно до схеми Таблиці А2. (3) Експоруйте PNG і вставте у звіт.

Для чого потрібен граф потоків даних: DFD - це карта руху персональних даних у системі. Він необхідний для виконання декількох правових вимог одночасно: (а) Визначення точок порушення ToS - граф наочно показує, на якому саме етапі неофіційний парсер збирає дані всупереч Meta Platform Terms п. 3 та TikTok ToS розд. 5; (б) Відповідність вимогам GDPR ст. 35 (DPIA/PIA) - документ «Data Protection Impact Assessment» обов'язково включає схему потоків даних як підтвердження того, що організація розуміє, які дані і куди передаються; (в) Ідентифікація надлишкового збору (ст.

5(1)(с)) - граф показує, що з платформ збираються фото та геолокація, які не потрібні на жодному з наступних етапів обробки; (г) Контроль передачі третім особам - видно, що звіти передаються відділу маркетингу, що потребує окремого обґрунтування. Червоні позначки на графі відповідають конкретним рядкам Таблиці А2. Нижче наведено готовий приклад графу.

Рис. 3. Граф потоків даних — система моніторингу Instagram/TikTok

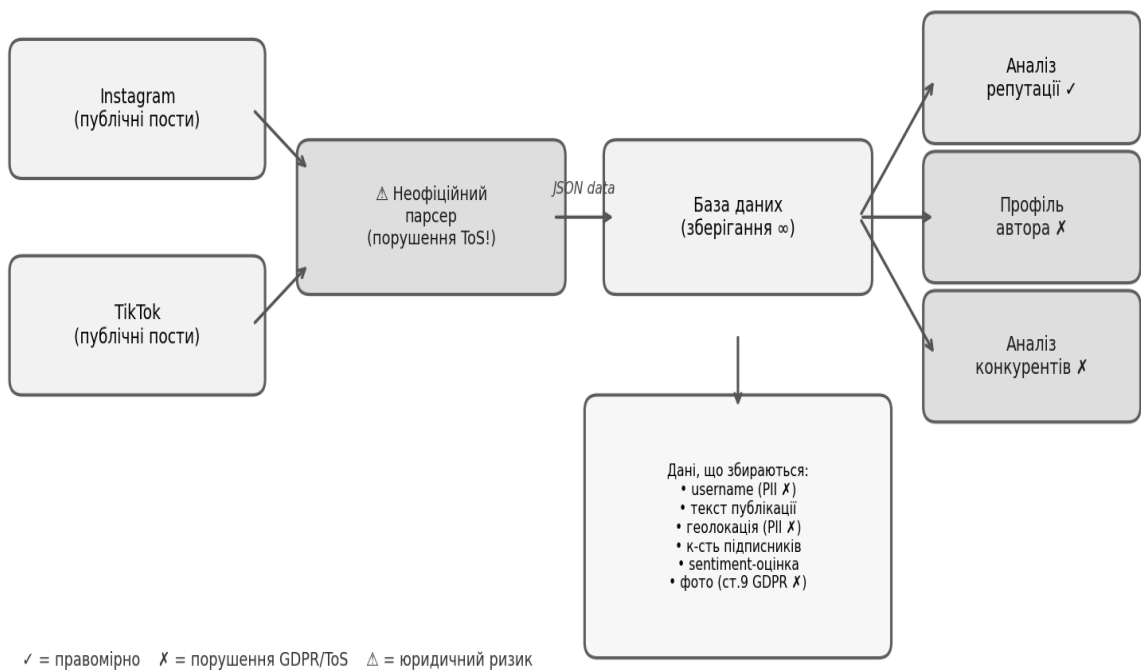


Рис. 2. Граф потоків даних - система моніторингу Instagram/TikTok. Червоним позначено точки порушення GDPR та ToS.

Примітка щодо використання неофіційного парсера: Meta Platform Terms п. 3 (2024) забороняє «automated data collection without explicit written permission from Meta.» Порушення може призвести до: блокування IP та акаунтів, анулювання доступу до платформи, судового позову (аналогічно LinkedIn Corp. v. hiQ Labs, 2022).

Крок 2.2. Реєстр порушень ToS

Дія системи	Порушений пункт ToS	Платформа	Рівень ризику	Рекомендація
Парсинг без офіційного API - неофіційний збір даних	Meta Platform Terms, п. 3 (2024): заборона автоматизованого збору без дозволу	Instagram	Критичний	Перейти на Instagram Graph API (https://developers.facebook.com/docs/instagram-api/)
Автоматичний збір	TikTok ToS, розд. 5 (2023):	TikTok	Критичний	TikTok Research API або відмова від збору даних TikTok

відео та постів	заборона scraping та автоматизованого збору			
Збір даних про конкурентів	Обидві платформи: збір дозволений лише у власних цілях	Instagram / TikTok	Середній	Окреме обґрунтування мети або повна відмова від моніторингу конкурентів
Зберігання даних необмежено	Meta ToS, п. 10.2: дані не повинні зберігатися довше, ніж це необхідно	Instagram	Середній	Визначити строки зберігання: 90 днів для сирих даних

Таблиця 7. Реєстр порушень ToS з оцінкою ризику (Варіант 1)

Прецедент: LinkedIn Corp. v. hiQ Labs (2022). Дев'ятий апеляційний округ США підтвердив право платформ забороняти scraping публічних даних. Рішення суду: <https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf>. Цей прецедент враховується при розгляді аналогічних справ у ЄС.

ЧАСТИНА 3. ЕТИЧНИЙ АУДИТ

Крок 3.1. Оцінка за трьома принципами та Радар-діаграма

Оцініть поточний стан системи за трьома принципами за шкалою 1-5. Побудуйте Радар-діаграму в Excel за інструкцією з розділу «Детальні інструкції до Кроку 3.1». Нижче наведено оцінку для Варіанту 1.

Принцип поваги до приватності - Оцінка: 2 / 5 (частково дотримується).

Обробляються лише публічні публікації (позитивно). Але збір username, геолокації, фото та sentiment-профілю разом є агрегацією, що виходить за межі розумних очікувань авторів. Принцип контекстної цілісності (Nissenbaum, 2004): автор публікував пост для своєї аудиторії, а не для бази даних комерційної компанії.

Принцип пропорційності - Оцінка: 1 / 5 (порушений).

Мета (аналіз репутації бренду) є законною, але обраний метод (повне профілювання авторів) є НАДМІРНИМ. Аналіз тексту публікацій без збереження ідентифікаторів - достатній для мети. Зберігання необмежено - непропорційне для будь-якої мети аналізу репутації.

Принцип прозорості - Оцінка: 1 / 5 (не дотримується).

Відсутній публічний Privacy Notice на сайті компанії. Суб'єкти даних не мають можливості дізнатися про факт обробки їхніх даних. Виправлення: опублікувати Privacy Notice з описом цілей, обсягу та строків. Зразок Privacy Notice: <https://ico.org.uk/for-organisations/make-your-own-privacy-notice/>

Крок 3.2. Чек лист відповідального моніторингу

Питання для перевірки	Стан	Обґрунтування (конкретно для сценарію)	Необхідна дія
Чи визначена законна правова підстава (ст. 6 GDPR)?	Частково	Лише для тексту публікацій (ст. 6(1)(f)). Профілі авторів не проходять тест балансування	Провести LIA окремо для кожної категорії даних
Чи пройдений тест балансування для законного інтересу (LIA)?	Ні	Профілювання авторів + зберігання необмежено не проходять балансування	Обмежити збір: лише текст публікацій без username
Чи дотримується принцип мінімізації даних (ст. 5(1)(c))?	Ні	Збираються username, геолокація, фото - надлишкові для мети аналізу репутації бренду	Видалити зайві поля збору, анонімізувати джерела
Чи визначені строки зберігання та механізм видалення (ст. 5(1)(e))?	Ні	Зберігання «необмежено» - пряме порушення ст. 5(1)(e) GDPR	Встановити: 90 днів для сирих даних, 24 місяці для звітів
Чи є технічна можливість реалізувати права суб'єктів (ст. 15, 17, 21)?	Ні	Не передбачено механізму відповіді на запити доступу або стирання	Реалізувати пошук і видалення за username у системі
Чи використовується офіційний API (не scraping)?	Ні	Неофіційний парсер порушує Meta Platform Terms п. 3 (2024)	Перейти на Instagram Graph API та TikTok Research API
Чи проведена Privacy Impact Assessment - PIA (ст. 35 GDPR)?	Ні	PIA відсутня; є обов'язковою при масовому зборі даних (ст. 35)	Провести PIA до перезапуску системи
Чи задокументовані підстави обробки у Privacy Notice?	Ні	Privacy Notice відсутній на сайті компанії	Опублікувати Privacy Notice з описом цілей та строків
Чи не обробляються спеціальні категорії без підстави (ст. 9 GDPR)?	Порушено	Фото авторів обробляються без правової підстави ст. 9	Негайно припинити обробку фото або отримати явну згоду за ст. 9(2)(a)

Чи є Human Oversight (людський нагляд) для AI-компонентів (ст. 22)?	Невідомо	Sentiment-аналіз виконується автоматично без опису процедури нагляду	Описати процедуру перевірки та корекції автоматичних висновків
---	----------	--	--

Таблиця 8. Чеклист відповідального моніторингу з обґрунтуванням (Варіант 1)

Крок 3.3. PIA Risk Score - Кількісна оцінка ризиків

Після заповнення таблиці нижче побудуйте порівняльну стовпчасту діаграму в Excel за інструкцією з розділу «Детальні інструкції до Кроку 3.3». Шкала: 1 = низький ризик, 5 = критичний.

Категорія ризику	Score зараз (1-5)	Score після (1-5)	Ключова дія	Статус GDPR
Обсяг збору ПД (username, геолокація, фото)	3 / 5	1 / 5	Виключити username, геолокацію	Ст. 5(1)(с)
Ризик ідентифікації (профілі авторів)	4 / 5	2 / 5	Анонімізація перед збереженням	Ст. 4(5) - анонімізація
Строки зберігання (необмежено)	4 / 5	1 / 5	Встановити 90 днів / 24 місяці	Ст. 5(1)(е)
Методи збору (порушення ToS)	5 / 5	1 / 5	Перейти на офіційний API	Meta Terms п. 3
Правова підстава (LIA не пройдено)	3 / 5	2 / 5	Документувати LIA для кожної мети	Ст. 6(1)(f)
Спецкатегорії (фото авторів, ст. 9)	5 / 5	1 / 5	Негайно припинити обробку фото	Ст. 9 GDPR
ЗАГАЛЬНИЙ PIA SCORE	24 / 30	8 / 30	Комплекс заходів відповідно до Charter	Ст. 35 GDPR - обов'язкова PIA

Таблиця 9. PIA Risk Score - кількісна оцінка до та після впровадження рекомендацій (Варіант 1)

Побудуйте порівняльну стовпчасту діаграму в Excel на основі цих даних за інструкцією у розділі «Крок 3.3. Детальні інструкції». Позначте порогове значення прийнятного ризику = 2.

ЧАСТИНА 4. ETHICAL MONITORING CHARTER ТА ПЛАНИ РЕАГУВАННЯ

Крок 4.1. Ethical Monitoring Charter інтернет-магазину

ETHICAL MONITORING CHARTER (ХАРТІЯ ВІДПОВІДАЛЬНОГО МОНІТОРИНГУ)

[Назва організації] | Затверджено: _____ | Версія 1.0

Статус: обов'язковий внутрішній нормативний документ (ст. 5(2) GDPR - підзвітність)

Розділ 1. Мета та сфера застосування

Цей документ визначає правила, обмеження та процедури для системи моніторингу соціальних мереж організації. Він є обов'язковим для всіх співробітників, що мають доступ до системи або її результатів.

Розділ 2. Дозволені цілі та категорії даних

Ціль моніторингу	Дозволені категорії даних	Строк зберігання	Правова підстава
Аналіз репутації власного бренду	Текст публікацій (анонімізований, без username)	90 днів (сирі дані)	Ст. 6(1)(f) GDPR - законний інтерес
Зведені аналітичні звіти	Агреговані метрики без ідентифікаторів авторів	24 місяці	Ст. 6(1)(f) GDPR - законний інтерес
Відповідь на відгуки клієнтів	Username (тільки для прямої відповіді на конкретний відгук)	14 днів після відповіді	Ст. 6(1)(b) GDPR - виконання договору

Таблиця 10. Дозволені цілі та категорії даних (Варіант 1)

Розділ 3. Заборонені дії (вичерпний перелік).

- Збір та зберігання username або ідентифікаторів авторів поза межами відповіді на відгуки.
- Обробка фотографій авторів з метою ідентифікації осіб (порушення ст. 9 GDPR).
- Використання будь-яких неофіційних парсерів або scraping-інструментів (порушення ToS Meta Platform Terms п. 3).
- Зберігання будь-яких даних після закінчення встановленого строку.
- Передача ідентифікаторів авторів третім особам без окремої правової підстави.
- Моніторинг закритих або приватних акаунтів.
- Використання даних моніторингу для оцінки конкретних осіб або прийняття рішень щодо них.

Розділ 4. Дозволені методи збору даних.

Виключно через офіційні API платформ: Instagram Graph API (документація: <https://developers.facebook.com/docs/instagram-api/>) та TikTok Research API (документація:

<https://developers.tiktok.com/products/research-api/>). Збір здійснюється лише для публікацій, що містять назву бренду, офіційний хештег або пряме посилання на бренд.

Розділ 5. Технічні вимоги Privacy by Design (ст. 25 GDPR).

Вимога PbD	Технічне рішення	Відповідальний
Анонімізація за замовчуванням	Хешування username до збереження у базі даних. Алгоритм: SHA-256 або аналог	Технічний директор / розробник системи
Автоматичне видалення даних	Скрон-завдання: очищення бази даних кожні 90 днів. Логування факту видалення	Адміністратор системи
Контроль доступу	Role-based access control (RBAC): доступ до системи лише у відповідальних підрозділів	Адміністратор бази даних
Аудит доступу	Логування всіх запитів до системи та вивантажень даних (зберігання логів 6 міс.)	CISO / DPO
Публічний Privacy Notice	Публічна сторінка на сайті компанії + оновлення при змінах у системі	Відділ маркетингу + DPO

Таблиця 11. Технічні вимоги Privacy by Design та відповідальні (Варіант 1)

Крок 4.2. План реагування на запити суб'єктів даних

Строк	Крок	Конкретні дії	Відповідальний	Правова підстава
День 1	Отримання та підтвердження	Надіслати підтвердження отримання запиту. Верифікувати особу заявника (запросити документ, що підтверджує особу, якщо ідентичність неочевидна). Зафіксувати дату (старт 30-денного строку за ст. 12(3)).	DPO / відповідальний за дані	Ст. 12(1) GDPR
Дні 2-5	Пошук даних	Здійснити пошук за username або email у всіх базах системи. Зафіксувати перелік знайдених записів або письмово підтвердити відсутність даних.	DPO + технічний спеціаліст	Ст. 15 GDPR
Дні 6-28	Обробка запиту	Право на доступ (ст. 15): підготувати копію всіх даних. Право на стирання (ст. 17): видалити всі записи і підтвердити видалення. Право на заперечення (ст.	DPO	Ст. 15, 17, 21 GDPR

		21): оцінити законні підстави; якщо їх немає - припинити обробку.		
День 30	Офіційна відповідь	Надіслати офіційну письмову відповідь. Якщо строк не може бути дотриманий - повідомити про продовження на 2 місяці (ст. 12(3) GDPR).	DPO	Ст. 12(3) GDPR

Таблиця 12. Алгоритм реагування на запити суб'єктів даних (Варіант 1)

Крок 4.3. Data Breach Response Plan (План реагування на витік даних)

Для чого потрібна часова шкала реагування: Графічна шкала часу реагування на витік даних є обов'язковим елементом Data Breach Response Plan. Вона виконує дві ключові функції: (а) Нагадування про юридичні строки - 72-годинний строк повідомлення регулятора (ст. 33 GDPR) є жорстким: порушення цього строку є самостійною підставою для штрафу до 10 млн євро або 2% від глобального обороту (ст. 83(4) GDPR), навіть якщо сам витік не заподіяв шкоди. (б) Чіткий розподіл відповідальності - кожен крок шкали прив'язаний до конкретної посадової особи (CISO, DPO, PR), що унеможливорює розмиття відповідальності під час кризи.

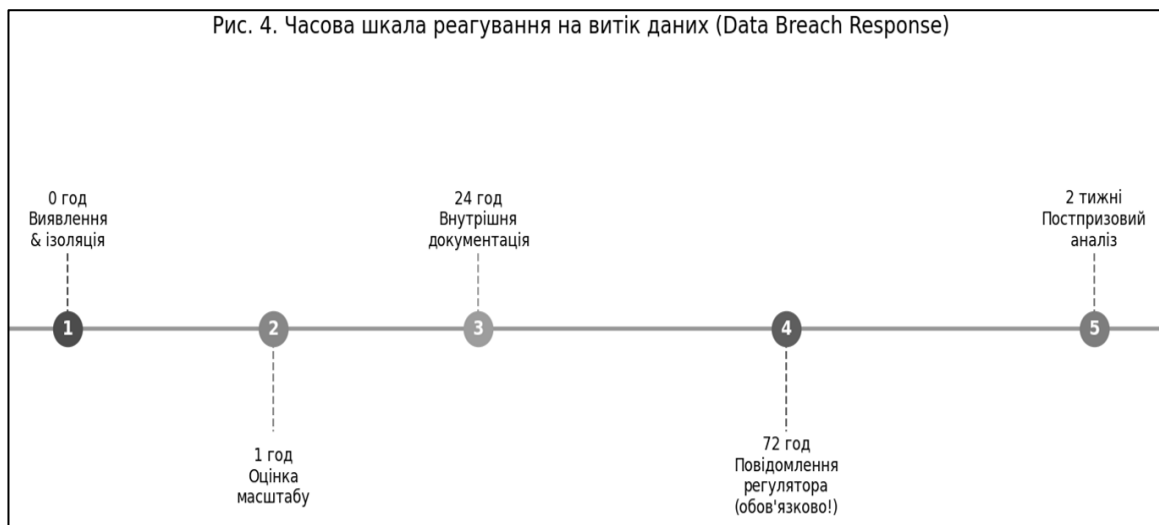


Рис. 5. Часова шкала реагування на витік даних. Крок на позначці 72 год є юридично обов'язковим за ст. 33 GDPR.

Етап	Строк	Конкретні дії	Відповідальний	Норма GDPR
1. Виявлення	0-1 год	Ідентифікувати факт витоку. Ізолювати систему. Визначити масштаб: кількість записів, тип даних (звичайні ПД чи спецкатегорії ст. 9).	CISO	-

		Призначити відповідального за координацію.		
2. Оцінка	1-24 год	Документувати хронологію: коли стався витік, що саме витекло. Оцінити ймовірний вплив на суб'єктів. Зафіксувати категорії постраждалих даних.	DPO + CISO	Ст. 33(3) GDPR
3. Регулятор	До 72 год (ОБОВ'ЯЗКОВО)	Повідомити Уповноваженого ВРУ з прав людини (https://www.ombudsman.gov.ua/). Надати: опис інциденту, кількість суб'єктів та записів, типи даних, вжиті заходи. УВАГА: порушення цього строку - штраф до 10 млн євро або 2% обороту (ст. 83(4) GDPR).	DPO	Ст. 33 GDPR
4. Суб'єкти	Без затримки (якщо «високий ризик»)	Якщо витік становить «високий ризик» для прав суб'єктів (ст. 34): повідомити постраждалих зрозумілою мовою: що сталося, які дані, що вжито, куди звертатись.	DPO + PR	Ст. 34 GDPR
5. Аналіз	Через 2 тижні	Провести технічний аналіз причин інциденту. Оновити Charter та технічні заходи захисту. Задokumentувати уроки для внутрішнього аудиту.	Весь комітет безпеки	Ст. 5(2) GDPR

Таблиця 13. Data Breach Response Plan відповідно до ст. 33-34 GDPR (Варіант 1)

ВИСНОВКИ ДО ВАРІАНТУ 1

Проведений правовий та етичний аудит системи моніторингу Instagram та TikTok для інтернет-магазину одягу виявив низку суттєвих порушень вимог GDPR та умов використання платформ, які вимагають негайного усунення.

1. Критичне порушення - обробка фотографій авторів (ст. 9 GDPR). Система обробляє фотографії авторів без правової підстави за ст. 9 GDPR. Це є найбільш серйозним виявленим порушенням. Необхідно негайно припинити обробку фото або отримати явну згоду суб'єктів за ст. 9(2)(а).

2. Критичне порушення - використання неофіційного парсера (ToS). Неофіційний парсер Instagram порушує Meta Platform Terms п. 3 (2024) та TikTok ToS розд. 5 (2023). Необхідно перейти на офіційні API або припинити збір даних.

3. Порушення принципу мінімізації (ст. 5(1)(с)). Збір username, геолокації та sentiment-профілів є надлишковим для заявленої мети аналізу репутації бренду. Рекомендована дія: обмежити збір лише текстом публікацій з подальшою анонімізацією.

4. Порухення принципу обмеження зберігання (ст. 5(1)(e)). Зберігання даних «необмежено» є прямим порушенням GDPR. Рекомендовані строки: 90 днів для сирих даних, 24 місяці для агрегованих звітів.

5. Відсутність Privacy Notice та документації. Відсутність публічного Privacy Notice порушує принцип прозорості та підзвітності (ст. 5(2)). Необхідно опублікувати Privacy Notice та розробити внутрішній Charter.

6. Загальний PIA Risk Score. Поточний стан - 24/30 (критично). Після впровадження рекомендацій - 8/30 (прийнятний рівень). Ключовим інструментом покращення є розроблений Ethical Monitoring Charter.

Виконана робота демонструє, що правомірний моніторинг соціальних мереж є можливим, але вимагає системного підходу: чіткого визначення мети, мінімізації даних, офіційних методів збору та документованих процедур. Перехід від поточного стану до відповідального моніторингу є реалістичним при умові виконання рекомендацій Charter.

ВАРІАНТИ ЗАВДАНЬ

Студент отримує варіант, що визначає організацію та сценарій моніторингу. Усі варіанти передбачають однакову структуру завдань, описану у цих методичних рекомендаціях.

Варіант 1

Організація: Інтернет-магазин одягу (B2C, аудиторія - фізичні особи 18+, Україна та діаспора в ЄС).

Сценарій: Компанія запускає систему моніторингу Instagram та TikTok для відстеження відгуків про власний бренд та аналізу публікацій конкурентів. Збираються: текст публікацій, username автора, кількість підписників, геолокація (якщо вказана), sentiment-оцінка. Використовується неофіційний парсер Instagram без API. Дані зберігаються необмежено.

Спеціальна умова: Значна частина авторів публікацій - громадяни ЄС (польська діаспора). Частина публікацій містить фото авторів. Необхідно окремо проаналізувати ризики, пов'язані з обробкою фотографій (ст. 9 GDPR, біометричні дані).

Варіант 2

Організація: Мережа ресторанів (10 закладів у Києві та Львові).

Сценарій: HR-відділ переглядає публічні профілі кандидатів на вакансії у Facebook, Instagram та LinkedIn перед запрошенням на співбесіду. Інформацію агрегують у таблиці Excel: ім'я, посилання на профіль, фото, опис хобі та особистих інтересів, зовнішній вигляд

(оцінка за внутрішньою шкалою). Рішення про запрошення або відхилення приймається частково на основі цих даних.

Спеціальна умова: У деяких профілях є публікації релігійного та політичного характеру. Необхідно проаналізувати ризики обробки спеціальних категорій даних (ст. 9 GDPR - релігійні переконання, політичні погляди) та правомірність автоматизованого рішення щодо прийому на роботу (ст. 22 GDPR).

Варіант 3

Організація: Медіа-агентство, що надає послуги моніторингу соціальних мереж клієнтам (B2B).

Сценарій: Агентство збирає публікації у Facebook, Twitter/X та Telegram про бренди своїх клієнтів за допомогою Brand24 API та власного Telegram-парсера на Telethon (бібліотека Python). Дані передаються клієнтам у форматі щотижневих звітів, що містять цитати публікацій та username авторів. Дані зберігаються на серверах агентства впродовж 2 років.

Спеціальна умова: Один із клієнтів просить надати «повний профіль» конкретного критичного блогера (всі публікації, кількість підписників, географія). Необхідно проаналізувати правомірність такого запиту, розробити відповідь клієнту та оцінити, чи є агентство контролером чи обробником даних за ст. 4(7)-4(8) GDPR.

Варіант 4

Організація: Університет (державний заклад вищої освіти).

Сценарій: Відділ комунікацій моніторить згадки університету у Facebook, Instagram та TikTok. Додатково: адміністрація відстежує публічні акаунти студентів у соціальних мережах, де вказаний університет. Моніторинг ведеться без повідомлення студентів. Матеріали використовуються для оцінки «репутаційних ризиків» та, в окремих випадках, у дисциплінарних провадженнях.

Спеціальна умова: Деякі студенти є неповнолітніми (17 років). Необхідно проаналізувати додаткові вимоги щодо обробки даних неповнолітніх (Recital 38 GDPR, а також національне законодавство) та оцінити правомірність використання даних у дисциплінарних провадженнях.

Варіант 5

Організація: Страхова компанія.

Сценарій: Відділ безпеки використовує соціальні мережі для перевірки страхових заявок: публічні профілі заявників аналізуються на наявність публікацій, що суперечать

задекларованим обставинам (наприклад, заявник стверджує, що не може ходити, але є фото з походу). Для цього використовується комерційний інструмент зі scraping-функціоналом. Результати аналізу впливають на рішення про виплату.

Спеціальна умова: Інструмент використовує розпізнавання облич для ідентифікації заявника на чужих фотографіях. Необхідно окремо проаналізувати статус біометричних даних (ст. 9 GDPR) та оцінити, чи є це автоматизованим прийняттям рішень у розумінні ст. 22 GDPR. Посилання на прецедент Clearview AI (ICO, 2022): <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-clearview-ai/>

Варіант 6

Організація: Громадська організація (правозахисний напрям).

Сценарій: ГО моніторить Telegram-канали та публічні групи Facebook для виявлення мови ненависті та дезінформації. Зібрані публікації (разом з username авторів) зберігаються у відкритій базі даних, яку може переглядати будь-хто. Частина матеріалів передається журналістам та правоохоронним органам.

Спеціальна умова: ГО стверджує, що її діяльність виконується в «публічних інтересах» і тому звільнена від вимог GDPR. Необхідно перевірити обґрунтованість цього твердження (ст. 6(1)(e) GDPR та Recital 4 GDPR), а також окремо проаналізувати правомірність передачі даних правоохоронним органам.

Варіант 7

Організація: Мобільний додаток для фітнесу (понад 200 000 українських користувачів).

Сценарій: Команда маркетингу аналізує публічні публікації користувачів у Instagram, що відмічають додаток або використовують відповідні хештеги. Збираються: username, текст поста, кількість підписників, геолокація, зображення. Найактивніші користувачі без їхньої згоди включаються до «амбасадорської програми»: їхні профілі та публікації використовуються в рекламних матеріалах компанії.

Спеціальна умова: Частина відібраних користувачів є неповнолітніми. Рекламні матеріали розповсюджуються серед аудиторії ЄС. Необхідно проаналізувати: правомірність використання публікацій у рекламних цілях без згоди, вимоги щодо неповнолітніх, та застосування авторського права до публікацій користувачів.

Варіант 8

Організація: Місцева рада (орган місцевого самоврядування середнього міста).

Сценарій: PR-відділ ради моніторить Facebook-групи та Telegram-канали міста для оцінки громадської думки щодо рішень ради. Список авторів критичних публікацій передається депутатам. В окремих випадках авторів запрошують «на бесіду» або надсилають їм листи з проханням видалити публікації.

Спеціальна умова: Рада є публічним органом влади. Необхідно проаналізувати: як статус публічного органу впливає на вимоги до обробки даних (ст. 6(1)(e) GDPR - публічний інтерес), чи є передача списку критиків депутатам правомірною, та чи є листи з проханням видалити публікації порушенням свободи слова (ст. 85 GDPR).

Варіант 9

Організація: Онлайн-платформа для пошуку роботи.

Сценарій: Платформа агрегує публічні профілі LinkedIn, GitHub та Twitter/X для автоматичного доповнення резюме зареєстрованих користувачів. Збір відбувається без явного запиту або дозволу - за email-адресою, що збігається. Алгоритм автоматично оцінює кандидата за публічною активністю (кількість публікацій, тематика, тональність коментарів) і присвоює «score», що впливає на видимість резюме для роботодавців.

Спеціальна умова: Платформа стверджує, що score є «рекомендаційним» і не є автоматизованим рішенням у розумінні ст. 22 GDPR. Необхідно оцінити обґрунтованість цього твердження (Guidelines WP29 щодо автоматизованого прийняття рішень: <https://ec.europa.eu/newsroom/article29/items/612053>), а також проаналізувати правомірність збору даних LinkedIn без їхнього API.

Варіант 10

Організація: Банк (середній за розміром, ліцензований Національним банком України - НБУ).

Сценарій: Відділ ризиків аналізує соціальні мережі позичальників при оцінці кредитних заявок: перевіряються Facebook, Instagram та публічні Telegram-канали на наявність «ризикових» публікацій (фото дорогих покупок, скарги на борги, ознаки азартних ігор). Аналіз здійснюється вручну співробітниками банку без повідомлення клієнта. Результати вносяться в кредитне досьє.

Спеціальна умова: Банк підпадає під спеціальне фінансове регулювання (НБУ). Необхідно проаналізувати: як галузеве регулювання взаємодіє з вимогами GDPR та Закону України «Про захист персональних даних», правомірність збору даних без повідомлення клієнта, та чи є аналіз «ризикових» публікацій обробкою даних про фінансове становище (спеціальна категорія в деяких юрисдикціях).

КРИТЕРІЇ ОЦІНЮВАННЯ ТА ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Частина роботи	Балів	Вимоги для отримання максимального балу
Частина 1. Правовий аудит	25	Ідентифіковані всі типи даних зі статусом за GDPR; пройдений тристадійний тест LIA з конкретними аргументами; таблиця відповідності принципам GDPR заповнена з обґрунтуванням; визначені права суб'єктів та технічні заходи для їх реалізації; побудована Радар-діаграма в Excel.
Частина 2. Аудит ToS платформ	20	Побудований DFD (граф потоків даних) в Excel або draw.io з позначенням точок порушень; оцінені методи збору з конкретними посиланнями на пункти ToS; реєстр порушень заповнений з описом ризиків та рекомендаціями; обґрунтований правомірний альтернативний метод збору.
Частина 3. Етичний аудит	20	Оцінка за трьома принципами з конкретними прикладами з варіанту; побудована Радар-діаграма «поточний стан vs. необхідний рівень» в Excel; чеклист заповнений з обґрунтуванням КОЖНОГО пункту (не у форматі «так/ні»); побудована стовпчаста діаграма PIA Risk Score в Excel.
Частина 4. Charter та плани реагування	25	Charter містить усі 7 обов'язкових розділів, заборони та дозволи конкретні та обґрунтовані нормами; план реагування на запити суб'єктів містить конкретні строки та відповідальних; Data Breach Response Plan відповідає вимогам ст. 33-34 GDPR.
Оформлення та посилання	10	Обсяг не менше 12 сторінок; посилання на конкретні статті GDPR та пункти ToS є обов'язковими; наявний список літератури (не менше 10 джерел); грамотна українська мова; структура відповідає вимогам; Excel-файл з діаграмами додано.
РАЗОМ	100	

Таблиця 14. Критерії оцінювання лабораторно-практичної роботи

Вимоги до оформлення звіту

Формат файлу: .docx або .pdf. Додатково: файл Excel (.xlsx) з усіма трьома діаграмами.

Обсяг: мінімум 12-15 сторінок основного тексту (без титульної сторінки, списку літератури та додатків).

Шрифт: Times New Roman, 14 пт, чорний колір.

Міжрядковий інтервал: 1,5 рядки.

Поля: верхнє та нижнє - 2 см, ліве - 3 см, праве - 1,5 см.

Обов'язкова структура звіту:

1. Титульна сторінка (назва дисципліни, тема, прізвище студента, група, дата, викладач).

2. Вступ до власного варіанту (0,5-1 сторінка): опишіть своїми словами отриманий сценарій та його особливості.
3. Частина 1: Правовий аудит (таблиці, тест LIA, Радар-діаграма з Excel).
4. Частина 2: Аудит ToS (DFD з Excel або draw.io, реєстр порушень).
5. Частина 3: Етичний аудит (оцінка за 3 принципами, Радар-діаграма, чеклист, PIA Risk Score з Excel).
6. Частина 4: Ethical Monitoring Charter та плани реагування.
7. Висновки (0,5-1 сторінка): підсумок знайдених порушень та рекомендацій.
8. Список літератури (не менше 10 джерел з активними посиланнями).

Вимоги до посилань: кожне твердження або рекомендація мають бути підкріплені посиланням на конкретну статтю GDPR, конкретний пункт ToS платформи або реальний прецедент. Посилання без конкретної статті (наприклад, просто «GDPR») не зараховуються.

Вимоги до діаграм у Excel: три обов'язкові діаграми: Радар-діаграма профілю ризиків GDPR (Крок 1.3), Радар-діаграма «поточний стан vs. необхідний рівень» (Крок 3.1), Стовпчаста діаграма PIA Risk Score «до та після» (Крок 3.3). Кожна діаграма вставляється у звіт як зображення та додається у файлі Excel.

Заборонено: заповнювати чеклист у форматі «так/ні» без обґрунтування; писати загальні фрази без посилань на конкретні норми; копіювати текст зі зразка виконання (Варіант 1) для інших варіантів без адаптації.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Нормативно-правові акти

1. Загальний регламент ЄС про захист даних (GDPR), Regulation (EU) 2016/679. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>
2. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
3. Конвенція Ради Європи 108+ (оновлена редакція, 2018). URL: <https://rm.coe.int/convention-108/16808b36f1>
4. Регламент ЄС про штучний інтелект (EU AI Act, 2024). URL: <https://artificialintelligenceact.eu/>

Наукова та навчальна література

1. Шемшученко Ю. С., Бошицький Ю. Л. Захист персональних даних в умовах цифрової трансформації. Київ: Юрінком Інтер, 2023. 286 с.
2. Voigt P., von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. 2nd ed. Springer, 2022. 380 p.

3. Solove D. J., Schwartz P. M. Privacy Law Fundamentals. 4th ed. IAPP, 2022. 296 p.
4. Cavoukian A. Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, 2011. URL: <https://www.ipc.on.ca/privacy/privacy-by-design/>
5. Nissenbaum H. Privacy as Contextual Integrity. Washington Law Review. 2004. Vol. 79(1). P. 119-157.

Умови використання платформ (ToS)

1. Meta Platform Terms (2024). URL: <https://developers.facebook.com/terms/>
2. Instagram Graph API. URL: <https://developers.facebook.com/docs/instagram-api/>
3. TikTok Terms of Service (2023). URL: <https://www.tiktok.com/legal/page/eea/terms-of-service/en>
4. TikTok Research API. URL: <https://developers.tiktok.com/products/research-api/>
5. Twitter/X Developer Agreement (2023). URL: <https://developer.twitter.com/en/developer-terms/agreement-and-policy>
6. LinkedIn User Agreement. URL: <https://www.linkedin.com/legal/user-agreement>

Інтернет-ресурси та правозастосовча практика

1. GDPR Enforcement Tracker (актуальна статистика штрафів). URL: <https://www.enforcementtracker.com/>
2. ICO (UK). Guide to GDPR. URL: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>
3. ICO. Clearview AI - penalty notice (2022). URL: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-clearview-ai-inc-more-than-7-5million/>
4. Уповноважений ВПУ з прав людини. Захист персональних даних. URL: <https://www.ombudsman.gov.ua/>
5. Guidelines on Automated individual decision-making and Profiling (WP29). URL: <https://ec.europa.eu/newsroom/article29/items/612053>
6. LinkedIn Corp. v. hiQ Labs, Inc. (2022). URL: <https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf>
7. FTC. Facebook - \$5 Billion Penalty (2019). URL: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-facebook>
8. draw.io - безкоштовний інструмент для побудови DFD. URL: <https://app.diagrams.net/>