

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

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

та індивідуальні завдання для самостійної роботи студентів

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 та індивідуальні завдання для самостійної роботи студентів з дисципліни «**Риск-моніторинг в соціальних мережах**» підготовки фахівців на першому (бакалаврському) 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

Сучасний етап розвитку глобального інформаційного суспільства характеризується безпрецедентним рівнем інтеграції соціальних мереж у всі сфери людської життєдіяльності що перетворює їх з простих інструментів комунікації на потужні майданчики формування суспільної думки економічних трендів та політичних процесів.

Дисципліна Риск-моніторинг у соціальних мережах виникає як критично необхідна відповідь на виклики цифрової епохи де швидкість розповсюдження інформації та її обсяги створюють нові типи загроз для державних інституцій комерційних структур та окремих особистостей. Вивчення цього курсу передбачає глибоке розуміння механізмів функціонування соціальних медіа як складних соціотехнічних систем де кожен вузол мережі може стати джерелом або ретранслятором деструктивного контенту дезінформації або кіберзагроз. Актуальність предмета обумовлена динамічною зміною ландшафту цифрових ризиків які еволюціонують від звичайного спаму та маніпуляцій до складних операцій впливу з використанням штучного інтелекту та великих даних.

У межах даного курсу особлива увага приділяється методології системного спостереження за віртуальним простором з метою раннього виявлення потенційно небезпечних явищ та процесів. Риск-моніторинг розглядається не просто як пасивне збирання даних а як активна аналітична діяльність спрямована на прогнозування кризових ситуацій та розробку стратегій їх нейтралізації. Студенти опановують інструментарій автоматизованого аналізу текстової та візуальної інформації вчать ідентифікувати ознаки інформаційних атак розрізняти органічну активність користувачів від скоординованої роботи бот-мереж та оцінювати репутаційні втрати в режимі реального часу. Важливим аспектом дисципліни є етична складова та правове регулювання моніторингової діяльності адже межа між забезпеченням безпеки та порушенням приватності є надзвичайно тонкою і вимагає високої професійної відповідальності.

Комплексний підхід до вивчення ризиків у соціальних мережах дозволяє сформувати цілісну картину вразливостей сучасного медіапростору. Ми аналізуємо психологічні чинники сприйняття інформації аудиторією

алгоритмічні особливості формування стрічок новин та технічні параметри збору відкритих даних.

Практична цінність курсу полягає у здатності майбутнього фахівця трансформувати величезні масиви неструктурованих даних у чіткі аналітичні звіти що слугують основою для прийняття управлінських рішень. Вивчення дисципліни дозволяє зрозуміти природу віральності інформації специфіку ехо-камер та механізми радикалізації в цифровому середовищі що є ключовим для побудови стійких систем захисту в умовах постійного інформаційного протиборства.

Завершення теоретичного та практичного блоків курсу забезпечує формування фахівця здатного не лише реагувати на існуючі загрози але й передбачати появу нових форм цифрових ризиків. Інтеграція знань з соціології психології програмування та аналізу даних створює міцний фундамент для професійної діяльності у сфері інформаційної безпеки стратегічних комунікацій та державного управління.

Таким чином дисципліна Риск-моніторинг у соціальних мережах є невід'ємною складовою сучасної вищої освіти яка готує лідерів здатних ефективно працювати у нестабільному та високотехнологічному світі де інформація стала головним ресурсом і водночас головною зброєю. Розгляд кейсів реальних криз та їх подолання за допомогою моніторингових технологій дозволяє закріпити отримані знання та виробити навички критичного мислення необхідні для успішної адаптації до будь-яких змін у глобальному мережевому просторі.

Ця методичка є логічним доповненням до комплекту лабораторних робіт з дисципліни «Риск-моніторинг у соціальних мережах». Вона не замінює лабораторні роботи, а розширює їх - пропонує додаткові кейси, теоретичні питання та тести, щоб студент міг самостійно перевірити та закріпити рівень засвоєння матеріалу.

Структура методички відповідає структурі курсу:

Розділ	Тема	Лабораторна робота
1	Репутаційні ризики та метрики моніторингу	Лаб. № 1
2	Мережний аналіз	Лаб. № 2
3	Архітектура систем моніторингу	Лаб. № 3–4
4	Кризовий менеджмент і Crisis Playbook	Лаб. № 5–6
5	Правові та етичні аспекти моніторингу	Лаб. № 7–10

Кожен розділ містить:

- теоретичні питання для самоперевірки (перевірте себе перед здачею лабораторної);
- додатковий практичний кейс - аналогічний до лабораторного, але на новому матеріалі;
- індивідуальні варіанти завдань для самостійного виконання;
- тест з вибором відповіді.

РОЗДІЛ 1. РЕПУТАЦІЙНІ РИСКИ ТА МЕТРИКИ МОНІТОРИНГУ

Відповідає лабораторній роботі № 1

1.1. Теоретичні питання для самоперевірки

Дайте розгорнуту відповідь (3–5 речень) на кожне питання самостійно, без заглядання у конспект. Потім звірте з лекційним матеріалом.

1. Що таке репутаційний ризик? Чим він відрізняється від операційного та фінансового ризику?
2. Поясніть «асиметрію репутації»: чому репутацію складніше відновити, ніж зруйнувати?
3. Опишіть формулу Net Sentiment Score (NSS). Яке значення вважається кризовим порогом і чому?
4. Що вимірює Share of Voice (SOV)? У яких сценаріях аналіз SOV є критично важливим?
5. Поясніть каскадний ефект репутаційної кризи на прикладі IT-компанії.
6. Чим відрізняється Crisis Velocity (CV) від загального обсягу згадок?
7. Назвіть чотири типи репутаційних ризиків за видом контенту та наведіть приклад для кожного.
8. Для чого використовується Engagement Rate (ER) у контексті ризик-моніторингу?

1.2. Додатковий практичний кейс: Укрпошта

Контекст кейсу.

Листопад 2023 р. В соціальних мережах Facebook та Twitter/X з'явилася серія публікацій про масові затримки посилок Укрпошти через перевантаженість сортувальних центрів. Протягом 72 годин накопичились такі дані: всього 4 800 згадок, з них 2 600 негативних, 900 позитивних, 1 300 нейтральних. У перший день - 400 згадок/год, в пік другого дня - 1 850 згадок/год. Конкурент «Нова Пошта» отримав за той самий період 6 200 згадок, «Meest Express» - 1 100 згадок.

Завдання до кейсу (обов'язкові)

Завдання 1.1. Розрахунок метрик (30 балів)

Розрахуйте для Укрпошти на основі наведених даних:

- Net Sentiment Score (NSS) за формулою: $NSS = ((Pos - Neg) / Total) \times 100\%$
- Crisis Velocity (CV) у пікову годину
- Share of Voice (SOV) серед трьох операторів за формулою: $SOV = (Згадки\ бренду / \text{Сумарні згадки ринку}) \times 100\%$

- Зробіть висновок: чи є ситуація кризовою за порогами з лекції?

Завдання 1.2. Класифікація ризиків (20 балів)

Визначте, до якого типу репутаційного ризику відноситься кожна з наведених публікацій. Обґрунтуйте відповідь:

- Пост клієнта: «Посилка лежить 12 днів, служба підтримки не відповідає» (3 500 реакцій)
- Відео в TikTok: спаленіле відділення після пожежі, поширилось на 180 тис. переглядів
- Стаття без джерел: «Укрпошта планує підвищити тарифи вдвічі у грудні»
- Скріншот чату з відділу логістики з лайками на адресу клієнтів

Завдання 1.3. Антикризовий пріоритет (20 балів)

Побудуйте матрицю пріоритизації ризиків 3×3 (Ймовірність / Вплив від 1 до 3). Внесіть усі чотири ризики з Завдання 1.2 та розрахуйте Risk Score. Який ризик потребує реагування у першу чергу?

Індивідуальні варіанти (самостійна робота)

Оберіть варіант за списком групи. Виконайте Завдання 1.1–1.3 для свого варіанту, підставляючи відповідні дані.

Вар.	Бренд	Позитивні / Негативні / Нейтральні	CV пік (зг/год)	Конкурент (кількість згадок)
1	Нова Пошта	1 400 / 3 200 / 900	2 400	Meest - 2 100
2	Monobank	800 / 2 700 / 600	3 100	ПриватБанк - 4 400
3	Rozetka	2 100 / 1 800 / 1 100	1 600	Prom.ua - 3 200
4	Kyivstar	600 / 4 100 / 800	3 800	Vodafone UA - 5 000
5	АТБ-Маркет	1 900 / 2 400 / 700	2 000	Сільпо - 4 100
6	ПриватБанк	700 / 5 300 / 1 200	4 200	Ощадбанк - 3 700
7	Укрзалізниця	500 / 3 900 / 1 100	3 300	FlixBus - 900
8	Vodafone UA	900 / 2 900 / 800	2 600	Kyivstar - 6 100

1.3. Тест для самоперевірки (Розділ 1)

Оберіть одну правильну відповідь. Ключі - в зеленому рядку під кожним питанням.

1. Net Sentiment Score (NSS) рівний -52% . Що це означає?

- A. Більше половини публікацій є нейтральними
- B. Переважають негативні публікації; ситуація відповідає кризовому рівню
- C. Бренд має 52% ринку за кількістю згадок
- D. NSS не може бути від'ємним

Правильна відповідь: B - NSS нижче -40% є кризовим порогом за стандартною методологією курсу.

2. Crisis Velocity = 2 400 згадок/год. Як це інтерпретувати?

- A. Нормальний рівень активності, реагування не потрібне
- B. Криза середнього рівня, варто спостерігати
- C. Значно перевищено кризовий поріг ($>2\ 100$ /год) - необхідне негайне реагування
- D. CV вимірюється в днях, а не в годинах

Правильна відповідь: B - поріг кризового CV становить $>2\ 100$ згадок/год за метриками лекції.

3. Яка з наведених характеристик репутаційного ризику описує явище «один скандал знищує репутацію, побудовану роками»?

- A. Каскадний ефект
- B. Глобальність
- C. Асиметрія репутації
- D. Складність вимірювання

Правильна відповідь: B - асиметрія репутації означає, що побудова вимагає значно більше часу, ніж руйнування.

4. Бренд X має $SOV = 18\%$, бренд Y - $SOV = 55\%$, бренд Z - $SOV = 27\%$. Які висновки можна зробити?

- A. Бренд X у кризі, бо має найменший SOV
- B. Бренд Y домінує за обсягом обговорень у галузі
- C. SOV не пов'язаний з репутаційними ризиками
- D. Бренд Z має найбільш позитивну репутацію

Правильна відповідь: B - SOV відображає частку голосу бренду, а не тональність. Бренд Y домінує кількісно.

5. Що таке Engagement Rate (ER) у контексті риск-моніторингу?

- A. Кількість публікацій про бренд за добу
- B. Відношення кількості взаємодій (лайки, коментарі, шери) до охоплення публікації
- C. Частка негативних публікацій у загальному потоці
- D. Швидкість реагування PR-команди на кризу

Правильна відповідь: Б - ER показує рівень залученості аудиторії, що дозволяє оцінити «глибину» впливу публікацій.

РОЗДІЛ 2. МЕРЕЖНИЙ АНАЛІЗ У РИСК-МОНІТОРИНГУ

Відповідає лабораторній роботі № 2

2.1. Теоретичні питання для самоперевірки

1. Що таке граф у контексті мережного аналізу? Що є вершинами та ребрами у соціальній мережі?
2. Поясніть різницю між спрямованим і неспрямованим графом та наведіть приклад кожного.
3. Що вимірює показник Betweenness Centrality? Чому він важливий для виявлення «мостів»?
4. Опишіть Degree Centrality та поясніть, які вузли отримують найвище значення.
5. Що таке «broker» у мережному аналізі? Яку роль він відіграє у поширенні дезінформації?
6. Порівняйте PageRank і Degree Centrality: у яких випадках PageRank точніший?
7. Що означає модульність (modularity) мережі? Як висока модульність пов'язана з «ехо-камерами»?

2.2. Додатковий практичний кейс: Фейкова кампанія в Telegram

Контекст кейсу

Виявлено скоординовану мережу Telegram-акаунтів, що поширює фейки про ПриватБанк. Дослідник зібрав дані та визначив ключові характеристики мережі: 148 вузлів (акаунти), 612 ребер (пересилання / реакції). Вузол А: Degree = 87, Betweenness = 0.41. Вузол Б: Degree = 12, Betweenness = 0.78. Вузол В: Degree = 63, Betweenness = 0.09. Три чітко виражені кластери (модульність = 0.68). Кластер 1 - «новини», Кластер 2 - «скарги клієнтів», Кластер 3 - «пересилання без коментарів».

Завдання до кейсу

Завдання 2.1. Аналіз центральності (35 балів)

- Який з вузлів (А, Б або В) є найважливішим для БЛОКУВАННЯ поширення інформації? Обґрунтуйте, спираючись на значення Betweenness Centrality.
- Який вузол має найбільше прямих зв'язків? Що це означає з точки зору впливу?
- Вузол Б має низький Degree, але високий Betweenness. Що це свідчить про його роль у мережі?

Завдання 2.2. Аналіз кластерів (35 балів)

- Значення модульності = 0.68. Що це означає для структури мережі? Чи є вона «ехо-камерою»?
- Назвіть, який кластер є найбільш небезпечним з точки зору репутаційних ризиків для ПриватБанку та чому?
- Запропонуйте стратегію протидії: яку дію (видалення вузла, блокування ребер, контент-відповідь) варто застосувати першочергово?

Завдання 2.3. Псевдокод алгоритму виявлення (30 балів)

Напишіть псевдокод алгоритму (мовою Python або у вільній формі), який із переліку вузлів графа відбирає «пріоритетні для моніторингу»: вузли з $\text{Betweenness} > 0.5$ АБО $\text{Degree} > 50$. Виведіть їх ідентифікатори та значення метрик.

Індивідуальні варіанти (самостійна робота)

Оберіть варіант. Проаналізуйте мережу за наведеними параметрами та дайте відповіді на запитання Завдань 2.1–2.2.

Вар.	Платформа / контекст	Вузлів	Ребер	Deg A	Betw A	Deg Б	Betw Б / Modular.
1	Twitter/X витік даних	210	880	94	0.37	15	0.82 / 0.71
2	Facebook скандал персоналом	165	540	71	0.55	8	0.63 / 0.59
3	Telegram дезінформація про банк	302	1140	110	0.29	22	0.74 / 0.65
4	Instagram вірусний відгук	88	310	55	0.48	9	0.69 / 0.73
5	Reddit - атака на ігрову компанію	240	970	130	0.22	18	0.85 / 0.61
6	YouTube кампанія проти ритейлера	175	690	80	0.44	11	0.58 / 0.67
7	Telegram Facebook хібридна	390	1520	148	0.31	27	0.79 / 0.72
8	TikTok вірусний скандал	121	420	66	0.52	7	0.61 / 0.55

2.3. Тест для самоперевірки (Розділ 2)

1. Вузол має Betweenness Centrality = 0.89 і Degree Centrality = 8. Що це означає?

- A. Вузол має багато прямих зв'язків і є найбільш впливовим
- B. Вузол є «мостом» - через нього проходять більшість найкоротших шляхів мережі, навіть маючи мало прямих зв'язків
- C. Вузол є ізольованим і не впливає на поширення інформації
- D. Значення несумісні - такий вузол не може існувати

Правильна відповідь: Б - висока Betweenness при низькому Degree - ознака «брокера», через якого проходять критичні інформаційні потоки.

2. Модульність мережі = 0.74. Що це означає?

- A. Мережа є однорідною, без помітних кластерів
- B. Мережа має чіткі кластери, що може свідчити про «ехо-камери» або скоординовані групи
- C. Лише 74% вузлів беруть участь в обміні інформацією
- D. Модульність понад 0.5 означає, що мережа штучно створена

Правильна відповідь: Б - модульність >0.6 свідчить про добре виражену кластерну структуру.

3. Яка метрика центральності найкраще виявляє «суперрозповсюджувача» фейків?

- A. Betweenness Centrality
- B. Closeness Centrality
- C. Degree Centrality
- D. Clustering Coefficient

Правильна відповідь: В - Degree Centrality показує кількість прямих зв'язків, що означає пряму аудиторію поширення.

4. Для чого в мережному аналізі використовується PageRank?

- A. Для визначення найстарішого вузла мережі
- B. Для оцінки «авторитетності» вузла з урахуванням якості, а не лише кількості зв'язків
- C. Для підрахунку загальної кількості публікацій
- D. Для вимірювання швидкості поширення інформації

Правильна відповідь: Б - PageRank враховує не лише кількість зв'язків, але й авторитетність джерел, що посиляються.

5. Для виявлення «містків» між кластерами в мережі потрібно визначити вузли з:

- A.** Найвищим Degree Centrality
- B.** Найвищим Betweenness Centrality
- C.** Найнижчим Clustering Coefficient
- D.** Найвищим PageRank

Правильна відповідь: Б - Betweenness Centrality максимальна у вузлів, що з'єднують різні частини мережі.

РОЗДІЛ 3. АРХІТЕКТУРА СИСТЕМ МОНІТОРИНГУ

Відповідає лабораторним роботам № 3–4

3.1. Теоретичні питання для самоперевірки

1. Опишіть п'ятишарову архітектуру системи моніторингу. Яку функцію виконує кожен шар?
2. У чому різниця між збором даних через API та web scraping? Яке з двох є правомірним?
3. Чому SQLite обрано для локального зберігання в навчальних проєктах? Які його обмеження?
4. Поясніть, чому VADER потребує адаптації для українського та російського тексту.
5. Що таке Streamlit і чому він є оптимальним для швидкого прототипування дашборду?
6. Яку роль відіграє бібліотека Telethon у системі моніторингу українського ринку?
7. Назвіть п'ять контрольних питань, на які має відповідати висновок до роботи.

3.2. Додатковий практичний кейс: Моніторинг ринку доставки їжі

Контекст кейсу

Студент будує систему моніторингу для порівняння репутації трьох сервісів доставки їжі: Glovo, Bolt Food та Raketa. Джерела: Telegram-канали відгуків (3 канали), коментарі в Instagram (публічні пости брендів), Reddit-спільнота r/ukraine. Завдання - побудувати 5-шарову архітектуру та описати реалізацію кожного шару

Завдання до кейсу

Завдання 3.1. Проектування архітектури (40 балів)

Заповніть таблицю для системи моніторингу ринку доставки їжі:

#	Шар архітектури	Інструмент технологія /	Що конкретно збирає / робить	Обмеження
1	Collection (збір)	??? - заповнити	??? - заповнити	??? - заповнити
2	Storage (зберігання)	??? - заповнити	??? - заповнити	??? - заповнити
3	Processing (обробка)	??? - заповнити	??? - заповнити	??? - заповнити
4	Analytics (аналітика)	??? - заповнити	??? - заповнити	??? - заповнити

5	Visualization (дашборд)	??? - заповнити	??? - заповнити	??? - заповнити
---	----------------------------	-----------------	-----------------	-----------------

Завдання 3.2. Схема бази даних (30 балів)

Напишіть SQL-скрипт CREATE TABLE для таблиці posts, яка зберігає: ідентифікатор запису, назву платформи, бренд (Glovo/Bolt/Raketa), текст публікації, дату, мову публікації, тональність (positive/neutral/negative), NSS за день. Вкажіть типи даних і обмеження (PRIMARY KEY, NOT NULL тощо).

Завдання 3.3. Код збору даних (30 балів)

Напишіть фрагмент Python-коду (25–40 рядків), що зчитує повідомлення з публічного Telegram-каналу за допомогою Telethon і зберігає їх у таблицю SQLite. Увага: замість реальних credentials використовуйте змінні api_id, api_hash.

Індивідуальні варіанти (самостійна робота)

Виконайте завдання 3.1–3.2 для свого варіанту об'єкта моніторингу.

Вар.	Об'єкт моніторингу	Джерела даних	Аналітичне завдання
1	Телеком-оператори (Kyivstar, Vodafone, lifecell)	Telegram, Twitter/X	Добова динаміка тональності по кожному бренду
2	Банківські сервіси (Mono, Приват, ПУМБ)	Facebook, Telegram	Порівняння NSS у проукраїнських і нейтральних спільнотах
3	Маркетплейси (Rozetka, Prom, OLX)	Instagram, Google Play відгуки	Порівняльний аналіз тональності для двох брендів
4	Сервіси доставки (Нова Пошта, Укрпошта, Meest)	Telegram, Facebook	Частота згадок по тижнях; пікові дні
5	Медіаплатформи (YouTube UA, Megogo, OLL.TV)	Twitter/X, Reddit	Виявлення найбільш обговорюваних тем
6	Ритейл (АТБ, Сільпо, Novus)	Facebook, Instagram, Google Maps	Аналіз тональності відгуків за містами
7	ІТ-компанії (Ерам, SoftServe, GlobalLogic)	LinkedIn, Telegram, DOU	Порівняння репутації на ринку праці та серед клієнтів
8	Авіакомпанії (МАУ, SkyUp, Ryanair UA)	Twitter/X, Facebook, TripAdvisor	Вплив затримок рейсів на NSS у реальному часі

3.3. Тест для самоперевірки (Розділ 3)

1. Який шар п'ятишарової архітектури відповідає за перетворення тексту в структуровані дані (видалення HTML-тегів, нормалізацію, визначення мови)?

- A. Collection (збір)
- B. Storage (зберігання)
- C. Processing (обробка)
- D. Analytics (аналітика)

Правильна відповідь: В - шар Processing (обробка) відповідає за очищення, нормалізацію та підготовку тексту.

2. Чому web scraping є ризикованим методом збору даних у порівнянні з API?

- A. Він повільніший і дає менше даних
- B. Він порушує Terms of Service більшості платформ і може призвести до блокування або судового позову
- C. Він вимагає знання мов програмування
- D. Він не підтримується Python

Правильна відповідь: Б - scraping порушує ToS платформ і є неправомірним методом збору даних (тема Лаб. № 7–10).

3. Що таке NSS і в якому шарі архітектури він розраховується?

- A. Net Sentiment Score; розраховується у шарі Analytics
- B. Network Safety Score; розраховується у шарі Processing
- C. Net Sentiment Score; розраховується у шарі Collection
- D. Normalized Search Score; розраховується у шарі Visualization

Правильна відповідь: А - NSS (Net Sentiment Score) розраховується у шарі Analytics після визначення тональності.

4. Яка команда запускає Streamlit-дашборд?

- A. python dashboard.py
- B. streamlit run dashboard.py
- C. flask run dashboard.py
- D. node dashboard.js

Правильна відповідь: Б - команда streamlit run запускає веб-сервер та відкриває дашборд у браузері.

5. Чому для моніторингу українського ринку Telegram є пріоритетним джерелом порівняно з Twitter/X?

- A.** Twitter/X заблокований в Україні
- B.** Telegram є основним каналом комунікації в Україні, де часто першими з'являються скарги та кризові сигнали
- C.** Telegram надає повний API без обмежень
- D.** Twitter/X не підтримує кирилицю

Правильна відповідь: Б - Telegram домінує як комунікаційний канал в Україні, особливо після 2022 р.

РОЗДІЛ 4. КРИЗОВИЙ МЕНЕДЖМЕНТ ТА CRISIS PLAYBOOK

Відповідає лабораторним роботам № 5–6

4.1. Теоретичні питання для самоперевірки

1. Що таке Crisis Playbook? Навіщо він потрібен ще до початку кризи?
2. Опишіть матрицю RACI: що означає кожна літера? Наведіть приклад для кризової команди.
3. Що таке протокол MARC-L? Розшифруйте кожний елемент та поясніть його роль.
4. Поясніть Alert Thresholds: за якими числовими метриками переходять між рівнями тривоги?
5. Як розраховується Response Time KPI? Яке його еталонне значення та чому?
6. Що таке Tone of Voice і чому він є критично важливим під час кризи?
9. Опишіть структуру посткризового плану відновлення репутації.

4.2. Додатковий практичний кейс: VitaFit - криза з неякісним продуктом

Контекст кейсу

VitaFit - українська компанія спортивного харчування. У вівторок, 14:23, у TikTok з'явилося відео фітнес-блогера (620 тис. підписників), де він стверджує, що у протеїні VitaFit знайшов пліснявий стиков. Відео набрало 180 000 переглядів за 3 години. До 17:00 NSS впав до -58%, CV = 2 900 зг/год, надійшло 340 скарг у Facebook, 18 медіазапитів. Компанія публічно не реагувала

Завдання до кейсу

Завдання 4.1. Vulnerability Audit (25 балів)

Визначте рівень тривоги кризи (Alert Level 1/2/3) за метриками NSS та CV з лекції. Побудуйте матрицю вразливостей: внесіть не менше 4 потенційних сценаріїв кризи для VitaFit з розрахунком Risk Score (Ймовірність × Вплив, шкала 1–5). Поточний сценарій є одним із них.

Завдання 4.2. Crisis Playbook - перша реакція (35 балів)

Опишіть кроки першої реакції VitaFit за протоколом MARC-L. Для кожного елемента (Моніторинг / Аналіз / Реагування / Комунікація / Логування) вкажіть конкретну дію в перші 60 хвилин. Складіть матрицю RACI для кризової команди (мінімум 4 ролі).

Завдання 4.3. Тексти першої реакції (40 балів)

Напишіть три тексти:

- Перша публічна відповідь у коментарях TikTok (до 120 слів, у перші 30 хв після виявлення)
- Розгорнута заява у Facebook (200–300 слів, через 2–3 години)
- Особисте повідомлення блогеру від імені PR-директора (100–150 слів)

Дотримуйтесь принципів Tone of Voice: визнання → співчуття → дія → зобов'язання.

Індивідуальні варіанти (самостійна робота)

Виконайте завдання 4.1–4.3 для свого варіанту.

Вар.	Бренд	Кризовий сценарій	NSS / CV	Тип аудиторії
1	Silpo (мережа супермаркетів)	Відео: миші у торговому залі - 340K переглядів за 4 год	-61% / 3 100/год	Споживачі, ЗМІ
2	ДТЕК Енерго (електропостачання)	Скоординована кампанія в Telegram про «штучні відключення»	-55% / 4 400/год	Населення, регулятори
3	Ажах Systems (охоронні системи)	Хакери опублікували нібито вразливість у прошивці	-48% / 2 600/год	B2B клієнти, партнери
4	Comfy (техніка та електроніка)	Продавець конфліктував із клієнтом - відео 200K	-44% / 1 900/год	Споживачі
5	Укренерго (системний оператор)	Фейк про «зупинку ГЕС» - масове поширення в Telegram	-67% / 5 200/год	Населення, іноземні ЗМІ
6	Foxtrot (ритейл електроніки)	Масові скарги на продаж рефарбованих ноутбуків	-51% / 2 200/год	Споживачі, Укрзахист
7	Genesis (IT-компанія)	Витік внутрішнього чату з дискримінаційними жартами	-57% / 3 700/год	IT-спільнота, співробітники
8	Eva (мережа дрогерій)	Відео: співробітник сварить покупця - 150K TikTok	-39% / 1 700/год	Споживачі (переважно жінки)

4.3. Тест для самоперевірки (Розділ 4)

1. $NSS = -58\%$, $CV = 2\ 900$ зг/год. Який рівень тривоги (Alert Level) це відповідає?

- A. Alert Level 1 (спостереження)
- B. Alert Level 2 (підготовка)
- C. Alert Level 3 (активна криза - максимальне реагування)
- D. Нормальний стан - реагування не потрібне

Правильна відповідь: B - NSS нижче -40% і CV вище $2\ 100$ /год одночасно відповідають Alert Level 3.

2. У матриці RACI літера «A» (Accountable) означає:

- A. Людина, яка виконує завдання безпосередньо
- B. Людина, яка несе кінцеву відповідальність за результат
- C. Людина, яку необхідно поінформувати про результат
- D. Людина, консультація з якою обов'язкова

Правильна відповідь: B - Accountable - особа, що несе кінцеву відповідальність і приймає рішення.

3. Яка мета тексту першої реакції на кризу (у перші 30–60 хвилин)?

- A. Надати повне пояснення причин кризи та список винних
- B. Підтвердити, що компанія поінформована про ситуацію та вживає заходів, не вдаючись до деталей
- C. Спростувати всі обвинувачення та перекласти відповідальність
- D. Оголосити про компенсації клієнтам

Правильна відповідь: B - перша реакція - це «ми знаємо, ми діємо». Деталі - у розгорнутій заяві через 2–4 год.

4. Response Time KPI = 45 хвилин. Як це оцінити?

- A. Погано - перевищено норму 30 хвилин
- B. Нормально - укладається в ціль <60 хвилин, але є резерв для покращення
- C. Відмінно - це еталонне значення
- D. Незадовільно - криза вже завершилась

Правильна відповідь: B - ціль <60 хв досягнута, але еталон - <30 хв (дані Institute for Crisis Management).

5. Компанії з підготовленим Crisis Playbook відновлюють докризовий Net Sentiment Score за:

- A.** 14 місяців (стільки ж, як не підготовлені)
- B.** 4 місяці проти 14 місяців у не підготовлених (дослідження Deloitte 2022)
- C.** 6 тижнів незалежно від наявності Playbook
- D.** Репутація не відновлюється після серйозної кризи

Правильна відповідь: Б - за даними Deloitte (2022), підготовлені компанії відновлюються у 3,5 рази швидше.

РОЗДІЛ 5. ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ

Відповідає лабораторним роботам № 7–10

5.1. Теоретичні питання для самоперевірки

1. Що таке GDPR? На яких осіб і організації він поширюється?
2. Перерахуйте шість правових підстав для обробки персональних даних (ст. 6 GDPR).
3. Що таке DPIA (Data Protection Impact Assessment) і коли він є обов'язковим?
4. Поясніть тристадійний тест LIA. Коли «законний інтерес» є виправданою підставою обробки?
5. Чим відрізняються API-доступ та scraping з точки зору Terms of Service платформи?
6. Що таке Privacy by Design (PbD)? Наведіть три конкретні заходи реалізації в системі моніторингу.
7. Які штрафні санкції передбачені GDPR (ст. 83)? Наведіть реальний приклад.
8. Що таке Ethical Monitoring Charter? Яку структуру вона повинна мати?

5.2. Додатковий практичний кейс: EdTech-стартап «LearnUA»

Контекст кейсу

LearnUA - освітня платформа (30 000 зареєстрованих студентів, у т.ч. 3 500 громадян ЄС). Команда маркетингу хоче запустити систему моніторингу соціальних мереж для відстеження згадок про платформу. Технічний план: збір публікацій у Twitter/X (через scraping, без API), Facebook (публічні пости) і Telegram-каналів. Збираються: текст публікацій, username автора, фото профілю, геолокація (якщо вказана), аналіз sentiment - зокрема, визначення «незадоволених студентів» за іменем та email для прямого контакту. Дані зберігаються 5 років без шифрування.

Завдання до кейсу

Завдання 5.1. Реєстр персональних даних (25 балів)

Заповніть таблицю реєстру даних (як у лабораторній роботі). Для кожного типу даних визначте:

Тип даних	Чи є ПД?	Правовий статус	Стаття GDPR	Рівень ризику (1–5)
Username автора	Заповнити	Заповнити	Заповнити	Заповнити
Текст публікації	Заповнити	Заповнити	Заповнити	Заповнити

Фото профілю	Заповнити	Заповнити	Заповнити	Заповнити
Геолокація	Заповнити	Заповнити	Заповнити	Заповнити
Sentiment email контакту + для	Заповнити	Заповнити	Заповнити	Заповнити

Завдання 5.2. Аудит відповідності ToS (25 балів)

- Визначте, які методи збору даних у плані LearnUA порушують Terms of Service платформ. Обґрунтуйте по кожній платформі.
- Запропонуйте правомірну альтернативу для кожного порушення.

Завдання 5.3. Розробка Ethical Monitoring Charter (50 балів)

Розробіть скорочену версію Ethical Monitoring Charter для LearnUA. Вона повинна містити:

- Мету і сферу дії системи моніторингу
- Перелік даних, що збираються (після корекції плану)
- Правові підстави обробки з посиланнями на статті GDPR
- Заходи Privacy by Design (мінімум 3 конкретні технічні заходи)
- Права суб'єктів даних та процедуру їх реалізації
- Термін зберігання і процедуру видалення даних

Індивідуальні варіанти (самостійна робота)

Оберіть варіант і виконайте Завдання 5.1–5.3 для свого типу організації.

Вар.	Тип організації	Сценарій моніторингу	Проблемний елемент	Ключова стаття GDPR
1	Новинне агентство	Моніторинг Telegram-каналів щодо відомих осіб	Збір фото та біометрії з відкритих джерел	Ст. 9 (спецкатегорії)
2	HR-агентство	Моніторинг соцмереж кандидатів без їх відома	Відсутня правова підстава, немає згоди	Ст. 6 (підстави обробки)
3	Маркетингова агенція	Парсинг відгуків конкурентів для клієнта	Порушення ToS + відсутній DPIA	Ст. 35 (DPIA)
4	Університет (заклад освіти)	Моніторинг акаунтів студентів у соцмережах	Немає законного інтересу (LIA не пройдено)	Ст. 6(1)(f) (законний інтерес)
5	Банк (фінансова установа)	Моніторинг ЗМІ та соцмереж для	Зберігання даних без визначеного строку	Ст. 5(1)(e) (обмеження зберігання)

		виявлення шахрайства		
6	Державна установа	Моніторинг «негативного» контенту про чиновників	Відсутня PbD, дані передаються третім особам	Ст. 25 (Privacy by Design)
7	ІТ-компанія (SaaS)	Продаж інсайтів на основі даних моніторингу	Зміна мети обробки без інформування суб'єктів	Ст. 5(1)(b) (обмеження мети)
8	Громадська організація	Моніторинг дискримінаційного контенту в соцмережах	Збір спецкатегорій без окремої підстави	Ст. 9(2) (виключення для спецкатегорій)

5.3. Тест для самоперевірки (Розділ 5)

1. На яких суб'єктів поширюється GDPR?

- A. Лише на компанії, зареєстровані в ЄС
- B. На будь-яку організацію, що обробляє персональні дані громадян ЄС, незалежно від місця реєстрації
- C. Лише на державні установи ЄС
- D. На компанії з оборотом понад 10 млн євро

Правильна відповідь: Б - GDPR має екстериторіальну дію: будь-яка організація, що обробляє дані громадян ЄС, зобов'язана дотримуватися регламенту.

2. Система моніторингу збирає username та фото профілю користувачів Twitter/X без їхньої згоди. Яку статтю GDPR це порушує насамперед?

- A. Ст. 17 (право на забуття)
- B. Ст. 6 (відсутня правова підстава для обробки персональних даних)
- C. Ст. 83 (адміністративні штрафи)
- D. Ст. 28 (обробники даних)

Правильна відповідь: Б - відсутність правової підстави (ст. 6) є першочерговим порушенням.

3. Коли DPIA є обов'язковою відповідно до GDPR?

- A. Завжди, для будь-якої обробки персональних даних
- B. Лише якщо компанія має більше 250 співробітників

C. При обробці великих масивів ПД, профілюванні або обробці даних спецкатегорій

D. DPIA є рекомендованою, але не обов'язковою процедурою

Правильна відповідь: В - ст. 35 GDPR передбачає обов'язковий DPIA для ризикованих операцій обробки.

4. Privacy by Design означає:

A. Розробку конфіденційного дизайну застосунку

B. Вбудовування захисту персональних даних у систему з моменту її проектування

C. Приватний (закритий) режим роботи застосунку

D. Заборону публікувати дизайн системи

Правильна відповідь: Б - PbD (ст. 25 GDPR) вимагає враховувати захист даних на етапі проектування, а не після.

5. Який максимальний штраф передбачений GDPR за найбільш серйозні порушення (ст. 83(5))?

A. 500 000 євро

B. 5 млн євро або 1% річного обороту

C. 20 млн євро або 4% річного глобального обороту (більша сума)

D. 10 млн євро або 2% річного обороту

Правильна відповідь: В - ст. 83(5) передбачає штраф до 20 млн євро або 4% глобального річного обороту.

КРИТЕРІЇ ОЦІНЮВАННЯ САМОСТІЙНОЇ РОБОТИ

Самостійна робота є додатковою до лабораторних і оцінюється окремо. Максимальна оцінка - 100 балів за весь курс (по 20 балів за розділ).

Критерій	Відмінно (5)	Добре (4)	Задовільно (3)	Балів
Правильність розрахунків (метрики, формули)	Всі формули правильні	Незначні помилки	Є суттєві помилки	30
Глибина аналізу та обґрунтування висновків	Повний аналіз з посиланнями	Аналіз є, але поверховий	Лише перелік без аналізу	30
Тест (правильні відповіді на 25 питань)	23–25 правильних	18–22 правильних	13–17 правильних	25
Оформлення і дотримання структури роботи	Структура повністю дотримана	Незначні відхилення	Структура порушена	15

Важливо

Самостійна робота, що не містить реально виконаних розрахунків (скопійованих з чужих робіт або згенерованих без обґрунтування), до зарахування не приймається. Текст першої реакції (Розділ 4) повинен бути оригінальним.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Чалий І. В., Синявіна Ю. В., Бутенко Т. А., Сирий В. М. Комплексні системи захисту інформації (частина 1). Моніторинг соціальних мереж: навчальний посібник. Харків : [б.-в.], 2026. 211 с. URI <https://repo.btu.kharkiv.ua/handle/123456789/78025>
2. Почепцов Г. Сучасні інформаційні війни. *Всеукраїнська експертна мережа*. URL: http://www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=112800
3. Молчанова М.О., Мазурець О.В., Собко О.В., Віт Р.В., Назаров В.В. Алгоритм виявлення аб'юзивного вмісту в україномовному аудіоконтенті для імплементації в об'єктно-орієнтовану інформаційну систему. Науковий журнал «Вісник Хмельницького національного університету» серія: Технічні науки. Хмельницький, 2024. №1 (331). С. 101-106.
4. Волошин І. В., Кравченко Л. М. Особливості використання соціальних мереж для організації зв'язків з громадськістю. Теорія і практика сучасної економіки: матеріали XXIII Міжнародної науковопрактичної конференції: 20 жовтня 2022 р./ Уроряд.: Р. В. Манн, Н. В. Ільченко; відп. ред. Р. В. Манн; М-во освіти і науки України, Черкас. держ. технол. ун-т. Черкаси: ЧДТУ, 2022. С. 35–37
5. Гуляєва Л. Швидка SMM-допомога : як використовувати соціальні мережі для розвитку організації та особистого бренду? ТОП 12 порад від експертів: навчальний

посібник. Київ : АПСВТ, 2021. 30 с.

<http://www.dut.edu.ua/ua/lib/1/category/743/view/2222>

Допоміжна

1. Чирак, І. (2021). Економіка соціальних медіа: сучасні тренди та особливості розвитку. Ефективна економіка, 12. URL:http://www.economy.nayka.com.ua/pdf/12_2021/94.pdf.
2. Чирак І. М. (2022). Методичні рекомендації з вивчення дисципліни «Економіка соціальних медіа» для студентів денної форми навчання першого (бакалаврського) рівня вищої освіти галузі знань 05 Соціальні та поведінкові науки спеціальності 051 Економіка освітньо-професійної програми “Економіка та управління бізнесом”. Тернопіль: ЗУНУ, 30 с
3. Харьковчук, О. (2021). Динаміка зростання аудиторії соціальних мереж: порівнюємо квартальні звіти DataReportal за 2020 і 2021 роки. URL:<https://web-promo.ua/ua/blog/dinamika-rosta-auditorii-socialnyh-setej-cravniwajem-kvartalnye-otchety-datareportal-za-2020-i-2021-gody/>.
4. Синчак, Б. (2022). Прямоефірна інформаційна війна та російсько-українська війна 2022-го на медійному плацдармі. Теорія і практика журналістики, 10, с. 85-97.
5. Савченко, С. В., & Караман, О. Л. (2021). Кіберсоціалізація молоді в умовах інформаційної війни росії проти України. Вісник Національної академії педагогічних наук України, 3(1), 1–5.
6. Романюк, В., & Чуранова, О. (2020, 22 вересня). Україна в інформаційному просторі росії та Білорусі. Інститут масової інформації.
7. Михайленко О. (2021). Навіщо бізнесу мобільний додаток? URL: <https://msb.aval.ua/news/?id=24743>.
8. Stengel, R. (2022). Information Wars: How We Lost the Global Battle Against Disinformation & What We Can Do About It. Atlantic Monthly Press, 410 p.
9. Said-Moorhouse, L., Haq, S. N., Ravindran, J., Alfonso, F., Vera, A., Regan, H., & Lendon, B. (2022). The Latest on the Ukraine-Russia Crisis. CNN.
10. Riehle, K. P. (2021). Winners and Losers in Russia's Information War. Intelligence and National Security, 36(7), 1057–1064.
11. Fridman, O., Kabernik, V., & Granelli, F. (Eds.). (2021). Info Ops: From World War I to the Twitter Era. Lynne Rienner Publishers.

Інструменти ризик-моніторингу

1. Brandwatch: <https://www.brandwatch.com>
2. Brand24: <https://brand24.com>
3. Mention: <https://mention.com>
4. Sprout Social: <https://sproutsocial.com>
5. Hootsuite Insights: <https://www.hootsuite.com/products/insights>
6. Talkwalker: <https://www.talkwalker.com>

Офіційна документація та регуляторні органи

1. GDPR Official Site: <https://gdpr.eu>
2. European Data Protection Board: <https://edpb.europa.eu>
3. CCPA Official Information: <https://oag.ca.gov/privacy/ccpa>
4. Digital Services Act (EU): <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
5. Закон України про захист персональних даних: <https://zakon.rada.gov.ua/laws/show/2297-17>

Кібербезпека та виявлення загроз

1. ZeroFOX: <https://www.zerofox.com>
2. RiskIQ (Microsoft): <https://www.riskiq.com>
3. Recorded Future: <https://www.recordedfuture.com>
4. Microsoft Video Authenticator (Deepfakes): <https://www.microsoft.com/en-us/research/project/video-authenticator>

Статистика та дослідження

1. DataReportal – Global Digital Reports: <https://datareportal.com>
2. Statista – Social Media Statistics: <https://www.statista.com/topics/1164/social-networks/>
3. Pew Research Center – Social Media: <https://www.pewresearch.org/internet/fact-sheet/social-media/>
4. IDC – Data & Analytics: <https://www.idc.com>

NLP та AI інструменти

1. Hugging Face – NLP Models: <https://huggingface.co/models>
2. spaCy – Industrial NLP: <https://spacy.io>
3. NLTK – Natural Language Toolkit: <https://www.nltk.org>
4. OpenAI Whisper: <https://openai.com/research/whisper>
5. GPTZero – AI Content Detection: <https://gptzero.me>

Факт-чекінг та верифікація

1. VoxUkraine – Ukrainian Fact-Checkers: <https://voxukraine.org>
2. StopFake Ukraine: <https://www.stopfake.org/uk>
3. IFCN – International Fact-Checking Network: <https://www.poynter.org/ifcn>
4. VADER Sentiment Analysis: <https://github.com/cjhutto/vaderSentiment>
5. Brandwatch Consumer Research: <https://www.brandwatch.com/blog/reputation-management/>
6. DataReportal Global Digital Reports: <https://datareportal.com>
7. Google Alerts: офіційний сервіс. URL: <https://alerts.google.com>
8. Hootsuite: безкоштовний план. URL: <https://hootsuite.com>
9. Mention: безкоштовний trial 14 днів. URL: <https://mention.com>
10. Brand24: безкоштовний trial 14 днів. URL: <https://brand24.com> (дата звернення: 2024).
11. Tweepy: офіційна документація. URL: <https://docs.tweepy.org/en/stable/>
12. PRAW - Python Reddit API Wrapper: документація. URL: <https://praw.readthedocs.io/>
13. Instaloader: офіційна документація. URL: <https://instaloader.github.io/>
14. Telethon - Python Telegram MTProto API: документація. URL: <https://docs.telethon.dev/>
15. Social-Analyzer: GitHub. URL: <https://github.com/qeeqbox/social-analyzer>
16. Apache Kafka: офіційна документація. URL: <https://kafka.apache.org/documentation/>
17. Elasticsearch / Kibana: офіційна документація. URL: <https://www.elastic.co/guide/>
18. Кембриджський словник (Cambridge Dictionary). URL: <https://dictionary.cambridge.org/dictionary/english/disinformation>
19. Grafana: офіційна документація. URL: <https://grafana.com/docs/>
20. Streamlit: офіційна документація. URL: <https://docs.streamlit.io/>
21. DataReportal - Global Digital Overview 2024. URL: <https://datareportal.com/global-digital-overview>