

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

КОНСПЕКТ ЛЕКЦІЙ

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

Конспект лекцій з дисципліни **РИСК-МОНІТОРІНГ 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

ЛЕКЦІЯ 1. ВСТУП ДО РИСК-МОНІТОРИНГУ В СОЦІАЛЬНИХ МЕРЕЖАХ

7

ВСТУП	9
Соціальні мережі: еволюція та сучасний стан. Історична перспектива: від простих форумів до глобальних екосистем	10
Ключові віхи розвитку соціальних мереж.....	12
Сучасна статистика соціальних мереж (2026)	12
П'ять ключових характеристик сучасних соціальних мереж	13
Концепція риск-моніторингу. Визначення та фундаментальні цілі	14
П'ять основних цілей риск-моніторингу.....	15
Компоненти системи риск-моніторингу: архітектура та технічний стек	16
Практичний приклад повного циклу моніторингу: авіакомпанія.....	18
Правове регулювання та етичні аспекти.	18
Етичні принципи риск-моніторингу	21
Основні виклики та тренди	22
Тренди 2025–2026: майбутнє соціальних мереж.....	23
ПРАКТИЧНІ ПРИКЛАДИ З ПОСИЛАННЯМИ	24
КЛЮЧОВІ ТЕРМІНИ ЛЕКЦІЇ	26
ВИСНОВКИ	26
КОНТРОЛЬНІ ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ	27
Література	28
ЛЕКЦІЯ 2. РЕПУТАЦІЙНІ РИСКИ В СОЦІАЛЬНИХ МЕРЕЖАХ	30
ВСТУП	30
ПОНЯТТЯ, СУТНІСТЬ ТА ОСОБЛИВОСТІ РЕПУТАЦІЙНИХ РИСКІВ	31
Ключові характеристики репутаційних ризиків	32
КЛАСИФІКАЦІЯ РЕПУТАЦІЙНИХ РИСКІВ.....	32
МЕХАНІЗМ ВИНИКНЕННЯ ТА ПОШИРЕННЯ РЕПУТАЦІЙНИХ КРИЗ	34
АНАЛІЗ РЕЗОНАНСНИХ КЕЙСІВ.....	36
КОНТРОЛЬНІ ПИТАННЯ.....	40
Література	40
ЛЕКЦІЯ 3. КІЛЬКІСНІ МЕТОДИ ОЦІНКИ РЕПУТАЦІЙНИХ РИСКІВ У СОЦІАЛЬНИХ МЕРЕЖАХ	42
ВСТУП	42
МЕТОДИКА 1. NET SENTIMENT SCORE (NSS) - ІНДЕКС ТОНАЛЬНОСТІ ЗГАДОК	43
МЕТОДИКА 2. WEIGHTED REPUTATION INDEX (WRI) - ЗВАЖЕНИЙ ІНДЕКС РЕПУТАЦІЇ.....	45

МЕТОДИКА 3. CRISIS PROBABILITY SCORE (CPS) - ОЦІНКА ЙМОВІРНОСТІ РЕПУТАЦІЙНОЇ КРИЗИ	47
МЕТОДИКА 4. REPUTATION RISK MATRIX (RRM) - МАТРИЦЯ РЕПУТАЦІЙНИХ РИСКІВ.....	49
МЕТОДИКА 5. SENTIMENT TREND ANALYSIS (STA) - АНАЛІЗ ДИНАМІКИ ТОНАЛЬНОСТІ	51
МЕТОДИКА 6. CHANNEL RISK DISTRIBUTION (CRD) - РОЗПОДІЛ РИСКУ ЗА КАНАЛАМИ	53
КОМПЛЕКСНЕ ЗАСТОСУВАННЯ МЕТОДИК ТА ВЗАЄМОЗВ'ЯЗОК МІЖ НИМИ.....	55
ВИСНОВКИ	57
КОНТРОЛЬНІ ПИТАННЯ.....	58
Література	59
ЛЕКЦІЯ 4. МЕРЕЖНИЙ АНАЛІЗ У РИСК-МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ.....	60
ВСТУП	60
Де саме використовується мережний аналіз: конкретні сфери застосування	61
Виявлення дезінформації та координованих маніпулятивних кампаній	62
Аналіз виборчих кампаній та політичних комунікацій	62
Кризовий менеджмент у реальному часі	63
Кібербезпека та захист від соціальної інженерії	63
Маркетинг та аналіз споживчої поведінки.....	64
Компетентності, які формує вивчення мережного аналізу	64
МЕРЕЖНИЙ АНАЛІЗ (NETWORK ANALYSIS)	65
Метрики центральності та їх практичне значення	66
Базова робота з графами.....	72
Інструменти візуалізації мереж	73
ВИЯВЛЕННЯ БОТІВ ТА КООРДИНОВАНИХ МЕРЕЖ	75
Реальні кейси застосування мережного аналізу	76
ВИСНОВКИ	78
КОНТРОЛЬНІ ПИТАННЯ.....	79
Література	81
ЛЕКЦІЯ 5. ІНСТРУМЕНТИ МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ. 82	82
ВСТУП.	82
Безкоштовні інструменти моніторингу - з чого почати.....	83
Практичний висновок: що обрати для лабораторної роботи	86
Комерційні платформи моніторингу	87

ЯК ОБИРАТИ КОМЕРЦІЙНУ ПЛАТФОРМУ	89
ПОБУДОВА ВЛАСНОЇ СИСТЕМИ МОНІТОРИНГУ	92
П'ятишарова архітектура системи моніторингу	92
ВИСНОВКИ	95
Контрольні питання	96
Література	96
Лекція 6. КРИЗОВИЙ МЕНЕДЖМЕНТ ТА АНТИКРИЗОВА КОМУНІКАЦІЯ В СОЦІАЛЬНИХ МЕРЕЖАХ	98
ВСТУП.	98
АНАТОМІЯ РЕПУТАЦІЙНОЇ КРИЗИ В СОЦІАЛЬНИХ МЕРЕЖАХ	99
СТАДІЇ РОЗВИТКУ КРИЗИ	100
Типологія кризових тригерів	101
ПРЕВЕНТИВНИЙ КРИЗОВИЙ МЕНЕДЖМЕНТ	102
СТРАТЕГІЇ АНТИКРИЗОВОЇ КОМУНІКАЦІЇ	105
ОСОБЛИВОСТІ КРИЗОВОЇ КОМУНІКАЦІЇ ДЛЯ РІЗНИХ ТИПІВ КРИЗ ТА АУДИТОРІЙ.....	109
ВІДНОВЛЕННЯ РЕПУТАЦІЇ ПІСЛЯ КРИЗИ	112
РЕАЛЬНІ KEYCИ: АНАЛІЗ УСПІХІВ І НЕВДАЧ	113
КОНТРОЛЬНІ ПИТАННЯ.....	115
ВИСНОВКИ	116
Література	117
Лекція 7. ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ.....	119
ВСТУП.	119
ПРАВОВЕ РЕГУЛЮВАННЯ ЗБОРУ ТА ОБРОБКИ ДАНИХ СОЦІАЛЬНИХ МЕРЕЖ	120
Ключові правові поняття для аналітика соціальних мереж	121
Правовий статус публічних даних у соціальних мережах	122
GDPR ТА ЙОГО ВПЛИВ НА МОНІТОРИНГ СОЦІАЛЬНИХ МЕРЕЖ.....	123
Законний інтерес як підстава для моніторингу	124
Права суб'єктів даних, що релевантні для моніторингу	125
Штрафні санкції та правозастосування	126
УМОВИ ВИКОРИСТАННЯ ПЛАТФОРМ (ToS): ЮРИДИЧНЕ ЗНАЧЕННЯ ТА ОБМЕЖЕННЯ	126
Telegram і особливості правового статусу в Україні	127
ЕТИЧНІ ОСНОВИ МОНІТОРИНГУ: ПРИВАТНІСТЬ, ПРОПОРЦІЙНІСТЬ, ПРОЗОРИСТЬ	128

ПРАКТИЧНІ КЕЙСИ: ПРАВОВІ ТА ЕТИЧНІ ПОРУШЕННЯ У МОНІТОРИНГУ	130
ПОБУДОВА ВІДПОВІДАЛЬНОГО МОНІТОРИНГУ: PRIVACY BY DESIGN ТА ETHICAL AI FRAMEWORK.....	132
Практичний чеклист відповідального моніторингу	134
КОНТРОЛЬНІ ПИТАННЯ.....	134
ВИСНОВКИ	135
Література	136

Соціальні мережі давно вийшли за межі простого інструменту спілкування. Сьогодні вони є повноцінним середовищем, у якому формується громадська думка, ведеться бізнес, розгортаються інформаційні кампанії та виникають репутаційні кризи. Мільярди публікацій, коментарів і реакцій щодня створюють безперервний потік даних, у якому приховані як можливості, так і загрози для організацій будь-якого масштабу. Здатність своєчасно виявляти ці загрози, оцінювати їх і реагувати на них - це і є риск-моніторинг у соціальних мережах.

Навчальна дисципліна “Риск-моніторинг в соціальних мережах” розроблена для студентів магістерського рівня вищої освіти спеціальності F3 (122 Комп’ютерні науки) освітньо-професійної програми “Консолідована інформація”. Вона поєднує теоретичну базу з практичними навичками роботи з реальними даними, інструментами та методиками, актуальними станом на 2026 рік.

Конспект лекцій охоплює шість тематичних блоків, кожен з яких присвячений окремому аспекту риск-моніторингу. Перша лекція закладає концептуальний фундамент: студенти знайомляться з еволюцією соціальних мереж, визначенням та цілями риск-моніторингу, архітектурою систем моніторингу, а також правовими й етичними рамками цієї діяльності. Друга лекція зосереджена на репутаційних ризиках - їх природі, класифікації, механізмах виникнення та поширення криз, підкріплених аналізом резонансних реальних кейсів. Третя лекція занурює студентів у світ кількісних методів: Net Sentiment Score, Weighted Reputation Index, Crisis Probability Score та інших аналітичних методик, що дають змогу перевести суб’єктивні враження у вимірювані показники. Четверта лекція присвячена мережному аналізу - потужному інструменту виявлення ботів, координованих маніпуляцій і прихованих зв’язків між акторами в цифровому просторі. П’ята лекція дає практичний огляд інструментів моніторингу - від безкоштовних рішень для початківців до комерційних платформ і власних архітектур збору даних. Шоста лекція завершує курс темою кризового менеджменту: стадії розвитку кризи,

стратегії антикризової комунікації, особливості роботи з різними аудиторіями та шляхи відновлення репутації.

Матеріал конспекту побудований за принципом наростаючої складності: кожна наступна тема спирається на знання, здобуті в попередніх лекціях. Теоретичні положення супроводжуються конкретними прикладами, кейсами та фрагментами програмного коду, що робить навчання максимально наближеним до реальних умов професійної діяльності. Кожна лекція завершується переліком контрольних питань для самоперевірки та рекомендованою літературою для поглибленого вивчення теми.

Опанувавши цей курс, студенти зможуть самостійно проектувати та налаштовувати системи риск-моніторингу, застосовувати кількісні методи оцінки репутаційних загроз, аналізувати мережні структури й виявляти маніпулятивні впливи, а також розробляти ефективні стратегії антикризової комунікації. Отримані компетентності є затребуваними у сферах кібербезпеки, корпоративних комунікацій, державного управління, медіааналітики та ІТ-індустрії загалом.

Конспект лекцій є основним навчальним матеріалом курсу і призначений для використання як під час аудиторних занять, так і в процесі самостійної підготовки.

ЛЕКЦІЯ 1. ВСТУП ДО РИСК-МОНІТОРИНГУ В СОЦІАЛЬНИХ МЕРЕЖАХ

ВСТУП

Сучасне інформаційне суспільство важко уявити без соціальних мереж. Вони давно перестали бути лише майданчиком для спілкування між друзями - сьогодні це потужна глобальна інфраструктура, що охоплює понад 5 мільярдів користувачів і генерує петабайти даних щодня. Соціальні мережі стали місцем, де формується громадська думка, приймаються ділові рішення, ведеться бізнес, розгортаються політичні кампанії та поширюється інформація - як достовірна, так і маніпулятивна.

Стрімкий розвиток цифрового середовища породив абсолютно нові виклики для бізнесу, державних інституцій і громадян. Репутаційна криза, що виникає внаслідок одного вірусного поста, може коштувати компанії мільярди доларів упродовж кількох годин. Витік персональних даних, поширення дезінформації, скоординовані атаки ботів, фішинг через соціальні мережі - усе це реальні загрози, які потребують системного реагування. Саме тут на допомогу приходить ризик-моніторинг у соціальних мережах.

Ризик-моніторинг є відносно молодю, але надзвичайно важливою дисципліною, що поєднує в собі елементи інформаційних технологій, лінгвістики, кібербезпеки, права та комунікаційних наук. Фахівець, здатний налагодити ефективну систему моніторингу, є надзвичайно затребуваним на ринку праці: від стартапів до транснаціональних корпорацій, від медіа-компаній до урядових агентств розвідки та контррозвідки.

Ця дисципліна безпосередньо пов'язана зі спеціальністю 122 - Комп'ютерні науки у напрямі «Консолідована інформація». Поняття «консолідована інформація» означає процес збирання, інтеграції та аналізу даних із різних джерел з метою отримання цілісної картини. Соціальні мережі є одним із найбільших та найдинамічніших джерел таких даних. Вміти працювати з ними - завантажувати, очищати, аналізувати, інтерпретувати та захищати - є ключовою компетентністю сучасного спеціаліста з комп'ютерних наук.

У першій лекції ми закладаємо фундамент: розглянемо, як розвивались соціальні мережі та яке місце вони займають сьогодні, що таке риск-моніторинг і навіщо він потрібен організаціям, з яких компонентів складається типова система моніторингу, яке правове та етичне підґрунтя забезпечує законність цієї діяльності, і нарешті - які виклики та тренди формують майбутнє галузі.

Дисципліна є практично орієнтованою. Студенти навчатися не лише розуміти теоретичні концепції, а й застосовувати реальні інструменти: Brand24, Brandwatch, Mention, VADER, спакі, Apache Kafka, Elasticsearch та інші. Знання, отримані в рамках курсу, дозволять проектувати, впроваджувати та обслуговувати повноцінні системи риск-моніторингу - від збору даних через API соціальних мереж до побудови автоматизованих дашбордів і налаштування тригерів кризового реагування.

ПЛАН ЛЕКЦІЇ

1. Соціальні мережі: еволюція та сучасний стан
2. Концепція риск-моніторингу: цілі, завдання, архітектура системи
3. Правове регулювання: GDPR, CCPA, DSA, Закон України «Про захист персональних даних»
4. Етичні аспекти роботи з даними соціальних мереж
5. Основні виклики риск-моніторингу
6. Сучасні тренди 2025–2026 років
7. Практичні приклади та кейси
8. Висновки та контрольні питання

Соціальні мережі: еволюція та сучасний стан. Історична перспектива: від простих форумів до глобальних екосистем

Соціальні мережі - це онлайн-платформи, що дозволяють користувачам створювати персональні або корпоративні профілі, встановлювати соціальні зв'язки, публікувати, поширювати та обговорювати контент різних форматів. Поняття «соціальна мережа» у цифровому контексті з'явилося на початку 2000-х років, хоча передумови для їхнього виникнення закладалися ще в 1990-х - у

форумах, чатах, дошках оголошень (BBS) і перших системах обміну миттєвими повідомленнями.

Перший прообраз сучасної соціальної мережі - SixDegrees.com - з'явився у 1997 році і базувався на теорії «шести рукостискань», сформульованій соціологом Стенлі Мілгредом ще у 1967 році. Ця теорія стверджує, що будь-яких двох людей у світі можна пов'язати ланцюжком не більше ніж із шести взаємних знайомств. SixDegrees дозволяв створювати профілі і переглядати списки друзів, однак не міг запропонувати достатньо контенту, щоб утримати аудиторію, і закрився у 2001 році.

Справжній прорив стався у 2003–2004 роках із появою LinkedIn та Facebook. LinkedIn відкрив нову нішу - професійне нетворкінгове середовище для ділових контактів, пошуку роботи та рекрутингу. Facebook, запущений студентом Гарварду Марком Цукербергом у 2004 році, стрімко вийшов за межі університетського кампусу і вже до 2008 року мав 100 мільйонів зареєстрованих користувачів. Ключовими інноваціями Facebook стали: стрічка новин (News Feed, 2006), кнопка «Подобається» (Like, 2009) та таргетована реклама, що перетворила платформу на одну з найприбутковіших медіакомпаній світу.

У 2006 році з'явився Twitter - платформа мікроблогінгу, де кожне повідомлення обмежувалося 140 символами (пізніше розширеними до 280). Twitter відразу зайняв нішу джерела новин у реальному часі, майданчика для публічних дискусій і інструменту активізму. Під час «Арабської весни» (2011) та численних виборчих кампаній Twitter продемонстрував здатність впливати на реальні суспільні процеси. У 2022 році компанію придбав Ілон Маск і у 2023 перейменував на X, що стало початком кардинальної зміни бізнес-моделі та принципів модерації.

2010-ті роки ознаменувалися візуалізацією соціальних мереж. Instagram (2010) зробив ставку на фотоконтент і фільтри, перетворившись на платформу для інфлюєнсерів і візуального маркетингу. YouTube, хоча й запущений ще у 2005 році, у цей період вийшов на безпрецедентні показники: у 2022 році на платформу завантажувалося понад 500 годин відео щохвилини. Нарешті, TikTok (міжнародна версія - 2018 рік, злиття з Musical.ly) здійснив революцію у

споживанні контенту, зробивши короткі вертикальні відео головним форматом комунікації покоління Z.

Кожна нова платформа не просто виходила на ринок - вона змінювала поведінку сотень мільйонів людей, відкривала нові можливості для бізнесу та породжувала нові risks: поширення дезінформації, кібербулінг, маніпуляції із суспільною думкою, порушення приватності. Саме зростання risks паралельно зі зростанням аудиторій і зумовило виникнення риск-моніторингу як окремої фахової дисципліни.

Ключові віхи розвитку соціальних мереж

Рік	Платформа	Значення та інновації
1997	SixDegrees.com	Перша соціальна мережа в сучасному розумінні. Базується на теорії «шести рукошестикань». Користувачі могли створювати профілі і переглядати списки знайомих. Закрита у 2001 році.
2003	LinkedIn	Револуція у професійному нетворкінгу. Орієнтована на бізнес-комунікації, пошук роботи та рекрутинг. Сьогодні - провідна платформа для B2B-маркетингу.
2004	Facebook	Глобальний феномен, запущений Марком Цукербергом. Ввів News Feed (2006), кнопку «Like» (2009), таргетовану рекламу. Станом на 2026 рік - понад 3 млрд активних користувачів.
2005	YouTube	Перша масова відеоплатформа. Куплена Google у 2006 р. за \$1,65 млрд. Сьогодні - другий за відвідуваністю сайт у світі.
2006	Twitter	Мікроблогінг до 140 (пізніше 280) символів. Платформа новин у реальному часі. У 2022 придбана Маском, перейменована на X у 2023.
2010	Instagram	Фокус на фотоконтент і фільтри. Введення Stories (2016), Reels (2020). Куплена Facebook за \$1 млрд у 2012 р. Платформа №1 для інфлюєнсер-маркетингу.
2013	Telegram	Месенджер із наскрізним шифруванням, каналами та ботами. Особливо популярний в Україні та країнах пострадянського простору.
2018	TikTok	Злиття ByteDance з Musical.ly. Короткі вертикальні відео, революційний AI-алгоритм рекомендацій (FYP). Найшвидше зростаюча платформа серед покоління Z.

Сучасна статистика соціальних мереж (2026)

За даними глобальних аналітичних платформ DataReportal (<https://datareportal.com>) та Statista (<https://www.statista.com/topics/1164/social-networks/>), станом на початок 2026 року соціальними мережами користується понад 5,2 мільярда людей - це майже 64% населення Землі. Щодня у світі

публікується близько 500 мільйонів твітів, 95 мільйонів фото та відео в Instagram, а на YouTube завантажується понад 500 годин відеоматеріалу щохвилини. Ці цифри не просто вражають - вони показують масштаб задачі, з якою стикається фахівець із риск-моніторингу.

Платформа	Активні користувачі	Ключові особливості
Facebook (Meta)	3,0 млрд	Універсальна платформа. Середній час використання - 34 хв/день. 98% заходять з мобільних пристроїв. Домінує у віковій групі 25–54 роки. Річний дохід від реклами - понад \$130 млрд.
YouTube (Google)	2,7 млрд	Відеохостинг і стрімінг. 500 год відео завантажується щохвилини. YouTube Shorts - 70 млрд переглядів на день. Основна платформа для навчального контенту та відеомаркетингу.
Instagram (Meta)	2,0 млрд	Фото, Stories, Reels. 80% користувачів підписані на бізнес-акаунти. Платформа №1 для інфлюєнсер-маркетингу. Рівень залученості (engagement rate) вищий, ніж у Facebook.
TikTok (ByteDance)	1,8 млрд	Короткі відео (15–60 сек). Найвищий середній час сесії - 95 хв/день. 60% аудиторії у віці 16–24 роки. Революційний алгоритм «For You Page».
Telegram	800 млн	Месенджер + канали. Дуже популярний в Україні. Шифрування, боти, канали до 200 000 підписників. Широко використовується для новин та автоматизації бізнесу.
LinkedIn (Microsoft)	950 млн	Професійна мережа. 67 млн компаній. 58 млн активних вакансій. 80% B2B-лідів із соцмереж приходять через LinkedIn.
Twitter / X	600 млн	Мікроблогінг, breaking news. 500 млн постів на день. Після придбання Маском - введення X Premium, монетизація контенту, зміни в системі модерації.

П'ять ключових характеристик сучасних соціальних мереж

Масштаб. Мільярди користувачів генерують петабайти даних щодня. Щодня у світі публікується близько 500 мільйонів твітів, 95 мільйонів фото та відео в Instagram, а на YouTube завантажується понад 500 годин матеріалів щохвилини. Такий обсяг створює як величезні аналітичні можливості, так і серйозні виклики зберігання та обробки.

Швидкість. Інформація поширюється миттєво через вірусний ефект. Пост може набрати мільйон переглядів за кілька годин. Це вимагає систем моніторингу в режимі реального часу (real-time processing), де затримка обробки не перевищує секунди.

Вплив. Соціальні мережі формують громадську думку, впливають на вибори (США 2016, 2020), визначають результати голосувань (Brexit, 2016) і здатні запускати масові соціальні рухи (#MeToo, #BlackLivesMatter). Дезінформація в соцмережах може мати геополітичні наслідки.

Монетизація. У 2025 році глобальні витрати на рекламу в соціальних мережах перевищили \$230 млрд. Meta (Facebook + Instagram) заробила \$131 млрд лише на рекламі у 2024 році. Це робить платформи критично важливими для бізнесу будь-якого масштабу.

Алгоритмізація. Машинне навчання та штучний інтелект визначають, який контент бачить кожен конкретний користувач. Алгоритм TikTok «For You Page» здатний утримувати увагу годинами. Це породжує «фільтрові бульбашки» та «луна-камери», що має серйозні наслідки для якості суспільного дискурсу та демократії.

Концепція риск-моніторингу. Визначення та фундаментальні цілі

Риск-моніторинг у соціальних мережах (Social Media Risk Monitoring)

- це систематичний, безперервний процес виявлення, оцінки та відстеження потенційних загроз і ризиків, що виникають у соціальних медіа та можуть негативно вплинути на організацію, бренд, репутацію або конкретних осіб.

Цей процес поєднує автоматизований аналіз великих масивів даних із вибірковою ручною верифікацією для раннього виявлення проблемних ситуацій - ще до того, як вони переростуть у повноцінну кризу. Риск-моніторинг є міждисциплінарною галуззю: він використовує методи обробки природної мови (NLP), машинного навчання, мережевого аналізу, теорії графів і традиційного PR-менеджменту одночасно.

Важливо розрізняти риск-моніторинг та звичайний моніторинг соціальних мереж. Звичайний моніторинг відстежує кількісні показники - кількість підписників, рівень залученості (engagement rate), охоплення публікацій. Риск-

моніторинг іде глибше: він аналізує тональність (sentiment), виявляє аномалії, ідентифікує потенційні загрози та ініціює протоколи реагування. Це принципово різні рівні аналізу з різними інструментами та кваліфікаційними вимогами до персоналу.

П'ять основних цілей риск-моніторингу

Раннє виявлення загроз. Основна мета - детектувати проблеми до того, як вони переростуть у кризу. Системи моніторингу відстежують аномальні сплески згадок, різкі зміни тональності, появу нових негативних ключових слів, поширення неправдивої інформації. Ранній сигнал дає організації час для підготовки відповіді, а не реагування постфактум.

***Практичний приклад:** Показовим прикладом наслідків відсутності раннього моніторингу є кейс авіакомпанії United Airlines (2017). Коли у мережі з'явилося відео насильного виселення пасажирів з літака, компанія не відреагувала оперативно. Результат: акції впали на \$1,4 млрд за один торговий день, CEO опинився під шаленим тиском. Інструменти раннього моніторингу (Brand24, Mention, Brandwatch) здатні фіксувати такі ситуації вже через хвилини після появи першого поширення.*

Захист репутації. Постійний моніторинг згадок бренду та аналіз тональності дозволяє компаніям відстежувати стан своєї репутації в реальному часі. Ключові показники: Share of Voice (частка згадок бренду порівняно з конкурентами), Net Sentiment Score (баланс позитивних і негативних відгуків), Influence Score (вплив авторів, що пишуть про бренд).

***Практичний приклад:** Скандал «Dieselgate» (Volkswagen, 2015) демонструє, чим обертається репутаційна криза у цифрову епоху. Після виявлення фальсифікацій тестів на викиди негативні згадки компанії в соцмережах зросли на 3000% упродовж доби. Ринкова капіталізація впала на €15 млрд. Постфактум Volkswagen інвестував мільярди в PR і комунікаційні стратегії відновлення довіри.*

Кібербезпека. Соціальні мережі є каналом для кібератак: фішингові посилання розповсюджуються через особисті повідомлення та публічні пости, скомпрометовані акаунти вживаються для соціальної інженерії, а ботнети організовують координовані атаки на репутацію. Риск-моніторинг у частині

кібербезпеки включає виявлення підозрілих облікових записів, аналіз аномалій активності, відстеження витоків корпоративних даних.

Практичний приклад: У 2020 році зловмисники зламали акаунти Білла Гейтса, Ілона Маска і Джо Байдена в Twitter і використали їх для шахрайської схеми з Bitcoin, зібравши понад \$120 000 за кілька годин. Атака стала можливою через соціальну інженерію - маніпуляцію з внутрішніми співробітниками платформи. Системи виявлення аномалій (ZeroFOX, RiskIQ) могли б ідентифікувати підозрілу активність на ранньому етапі.

Комплаєнс (правова відповідність). Обробка даних користувачів соціальних мереж підпадає під дію численних правових актів: GDPR (ЄС), CCPA (Каліфорнія), DSA (ЄС) та національних законів про захист персональних даних. Риск-моніторинг у частині комплаєнсу забезпечує відповідність цим нормам: контроль згоди на обробку даних, дотримання термінів зберігання, повідомлення про порушення у встановлені строки.

Практичний приклад: У 2023 році Meta була оштрафована на €1,2 млрд - це найбільший штраф в історії GDPR - за передачу персональних даних європейських користувачів на сервери у США без відповідних гарантій. Сума відповідала 4% від глобального річного обороту компанії. Приклад наочно демонструє, наскільки серйозними є фінансові наслідки недотримання правових норм.

Конкурентна розвідка. Відкриті дані соціальних мереж є безцінним джерелом для аналізу конкурентного середовища. Моніторинг акаунтів конкурентів, аналіз відгуків їхніх клієнтів, відстеження нових продуктів і маркетингових кампаній - усе це допомагає формувати власну стратегію, виявляти слабкі місця суперників і реагувати на ринкові зміни раніше за інших.

Практичний приклад: Компанія Apple, перед запуском iPhone 15 у 2023 році, аналізувала реакцію споживачів на Samsung Galaxy S23 у соціальних мережах. Дані про найпоширеніші скарги (перегрів, якість зарядки, камера в темряві) були враховані у фінальному позиціюванні продукту та акцентах маркетингової кампанії.

Компоненти системи риск-моніторингу: архітектура та технічний стек

Ефективна система риск-моніторингу складається з п'яти взаємопов'язаних компонентів, що працюють у безперервному циклі. Кожен компонент обробляє потік даних і передає його наступному - від первинного збору до кінцевого рішення про реагування. Нижче наведено детальний опис кожного рівня.

Компонент	Технології та інструменти	Опис
1. Збір даних	Twitter API v2, Facebook Graph API, Instagram API, Telegram API, Web scraping (BeautifulSoup, Scrapy), RSS-стрічки	Автоматизований збір публічних даних із платформ за ключовими словами, хештегами, акаунтами. Twitter API (Free tier) надає до 500 000 твітів на місяць. Для масштабних задач використовується Academic Research Access або комерційні плани.
2. Зберігання	MongoDB, Cassandra (NoSQL), PostgreSQL (SQL), Elasticsearch, AWS S3 / Azure Blob Storage	Вибір залежить від обсягу та структури даних. NoSQL (MongoDB) - для неструктурованих JSON-постів. Elasticsearch - для повнотекстового пошуку. AWS S3 - для архіву даних, старших за 90 днів.
3. Аналітика	spaCy, BERT, GPT, VADER, TextBlob (NLP); scikit-learn, TensorFlow (ML); Neo4j (графовий аналіз); Z-score (виявлення аномалій)	Аналіз тональності (sentiment analysis), виявлення тематик (topic modeling), аналіз мережі акаунтів для ідентифікації ботів, прогнозування вірусного поширення.
4. Візуалізація	Grafana, Tableau, Power BI, React (кастомні дашборди), PagerDuty, Slack-боти для сповіщень	Дашборди реального часу відображають KPI: кількість згадок, динаміка тональності, топ-інфлюєнсери, географічні теплові карти. Slack-бот надсилає автоматичні тривоги при аномаліях.
5. Реагування	Антикризові протоколи (playbooks), матриці ескалації, шаблони відповідей, Crisis Management Software	Чіткі протоколи дій для різних рівнів загрози: від звичайного негативного відгуку (відповідь SMM-менеджера за 2 год) до повноцінної кризи (збір кризового комітету, заява CEO за 4 год).

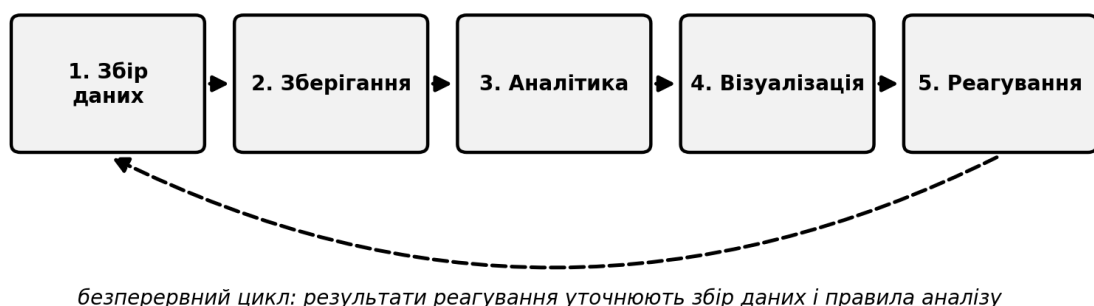


Рис. 1.1. П'ять взаємопов'язаних компонентів системи риск-моніторингу

Практичний приклад повного циклу моніторингу: авіакомпанія

Розглянемо, як повний цикл риск-моніторингу виглядає на конкретному прикладі. Уявімо середню авіакомпанію, яка обслуговує 50 рейсів на день і підтримує акаунти в Twitter/X, Facebook, Instagram та Telegram.

Крок 1. Збір даних. Twitter API відстежує @airline_name, хештег #airline_name і ключові слова «затримка рейсу», «загублений багаж», «груба поведінка персоналу». Facebook Graph API збирає публічні пости на сторінці компанії. Instagram API аналізує Stories та пости з геотегами аеропортів. Через веб-скрейпінг монітуються тематичні суб-редити Reddit (r/travel, r/ukraine) та форуми авіапасажирів.

Крок 2. Зберігання. Усі зібрані дані у форматі JSON зберігаються в MongoDB (10 ГБ/день). Elasticsearch індексує текстові поля для миттєвого повнотекстового пошуку. Дані, старші за 90 днів, архівуються на AWS S3 з метою довгострокового аналізу та відповідності правовим вимогам.

Крок 3. Аналітика. VADER-алгоритм автоматично класифікує тональність кожного посту: «рейс затримали на 5 годин, найгірша авіакомпанія» → негатив (score -0.87). Система виявлення аномалій фіксує: за годину надійшло 500 згадок (норма - 50/год) → тривога. Алгоритм topic modeling автоматично кластеризує повідомлення за темами: «затримки», «обслуговування», «ціни». Аккаунт із 150 000 підписників написав негативний пост → пріоритет HIGH.

Крок 4. Візуалізація. Grafana-дашборд відображає графік кількості згадок за останні 24 год, динаміку тональності, топ-5 авторів за охопленням і теплову карту географії скарг. Slack-бот надсилає сповіщення: «АНОМАЛІЯ: 500 згадок за останню годину, тональність - 75% негативна. Тема: затримки у JFK».

Крок 5. Реагування. Кризовий комітет збирається протягом 30 хвилин. Через 2 години CEO публікує заяву в Twitter: «Вибачаємося за затримки через погодні умови. Ось конкретні кроки, які ми вживаємо». Чат-бот автоматично відповідає на типові запити пасажирів. Після закінчення кризи - postmortem-аналіз: виявлення першопричини, коригування процесів, оновлення кризового плану.

Правове регулювання та етичні аспекти.

Ключові нормативні акти

Будь-яка діяльність із моніторингу та обробки даних соціальних мереж здійснюється у строго визначеному правовому полі. Незнання або ігнорування цих норм може призвести до мільйонних штрафів, кримінального переслідування та незворотних репутаційних втрат. Нижче детально розглянуто чотири основні нормативні акти, з якими стикається кожен фахівець із риск-моніторингу.

1. GDPR - Загальний регламент захисту даних (ЄС, 2018)

Офіційний сайт: <https://gdpr.eu>. GDPR набув чинності у травні 2018 року і є найбільш впливовим законодавчим актом у сфері захисту персональних даних. Його дія поширюється на *будь-яку організацію у світі*, що обробляє дані резидентів Європейського Союзу, - незалежно від місцезнаходження самої організації. Це означає, що українська компанія, яка збирає email-адреси громадян ЄС через форму на сайті, зобов'язана дотримуватись GDPR.

Ключові положення GDPR включають: право на забуття (Right to be Forgotten) - користувач може вимагати повного видалення своїх даних; право на перенесення даних (Data Portability) - отримання власних даних у машиночитаному форматі (CSV, JSON); обов'язкове повідомлення регулятора про витік даних протягом 72 годин; заборону pre-checked boxes при отриманні згоди; вимогу призначати Уповноваженого із захисту даних (DPO) для організацій, що обробляють значні обсяги чутливої інформації. Максимальний штраф - €20 млн або 4% від глобального річного обороту компанії (більша сума з двох).

Найбільші штрафи за порушення GDPR

Компанія	Штраф	Причина порушення
Meta (Facebook)	€1,2 млрд (2023)	Передача персональних даних громадян ЄС на сервери США без належних правових гарантій.
Amazon	€746 млн (2021)	Порушення правил таргетованої реклами без отримання належної згоди від користувачів.
Google	€90 млн (2022)	Незаконне використання cookies без згоди користувачів у Франції (рішення CNIL).
H&M	€35,3 млн (2020)	Незаконний збір і зберігання детальних особистих даних про сотні співробітників у Німеччині.

2. CCPA - Закон Каліфорнії про захист приватності споживачів (США, 2020)

Офіційна інформація: <https://oag.ca.gov/privacy/ccpa>. CCPA вважається американським аналогом GDPR - хоча і дещо менш суворим. Закон поширюється на компанії з річним доходом понад \$25 млн або ті, що обробляють дані більш як 50 000 резидентів Каліфорнії. Серед ключових прав: право знати, які дані збираються і кому продаються; право вимагати видалення даних; право відмовитися від продажу власних даних (кнопка «Do Not Sell My Info»); заборона дискримінувати споживачів за реалізацію їхніх прав. Штрафи: \$2 500 за ненавмисне порушення і \$7 500 за навмисне - за кожен окремий випадок.

3. DSA - Акт про цифрові послуги (ЄС, 2024)

Офіційна інформація: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>. DSA - принципово новий тип регулювання: він стосується не обробки персональних даних, а *відповідальності платформ за контент*. Великі платформи (Facebook, TikTok, YouTube, Twitter/X) зобов'язані: оперативно видаляти незаконний контент, дезінформацію та hate speech; забезпечувати прозорість рекомендаційних алгоритмів; надавати дослідникам доступ до даних; заборонити «темні шаблони» (dark patterns) - маніпулятивні UI-елементи, що схиляють користувача до небажаних дій. Штраф за порушення - до 6% від глобального річного обороту.

4. Закон України «Про захист персональних даних» (2010, редакція 2023)

Посилання: <https://zakon.rada.gov.ua/laws/show/2297-17>. Закон України гармонізується зі стандартами GDPR у рамках курсу на євроінтеграцію. Регулятором є Уповноважений Верховної Ради з прав людини. Закон визначає поняття персональних даних, права суб'єктів даних, обов'язки операторів і розпорядників. В умовах воєнного стану (з 2022 року) певні положення отримали додаткові виключення, що стосуються безпеки та оборони. Проте ключові принципи - законність обробки, мінімізація даних, забезпечення

безпеки - залишаються незмінними і для фахівців із риск-моніторингу є обов'язковими.

Етичні принципи риск-моніторингу

Правова відповідність - необхідна, але недостатня умова. Фахівець із риск-моніторингу часто опиняється перед ситуаціями, де закон дозволяє певні дії, але етика підказує утриматися. Нижче розглянуто чотири ключові етичні принципи.

Прозорість (Transparency). Користувачі мають право знати, що їхні публічні дані аналізуються. Politika Privacy Policy повинна чітко і зрозумілою мовою описувати, які дані збираються, як використовуються і скільки зберігаються. Протилежністю прозорості є скандал Cambridge Analytica (2018): дані 87 мільйонів користувачів Facebook були зібрані без їхнього відома через quiz-додаток і використані для мікротаргетованого політичного впливу під час виборів у США та Brexit.

Пропорційність (Proportionality). Принцип мінімізації даних: збирати лише те, що дійсно потрібне для конкретної задачі. Для аналізу тональності публічних відгуків достатньо тексту постів - немає жодної необхідності збирати фотографії, геолокацію або приватні повідомлення. Термін зберігання даних має бути мінімально необхідним: для більшості задач оперативного моніторингу достатньо 30–90 днів.

Безпека (Security). Зібрані дані мають зберігатися у зашифрованому вигляді (encryption at rest та in transit через TLS/SSL). Доступ до бази даних повинен надаватися лише авторизованому персоналу на принципі мінімально необхідних привілеїв (least privilege). Усі операції з даними мають протоколюватися в audit logs. Яскравий приклад недотримання безпеки: витік даних Twitter у 2023 році - 200 мільйонів email-адрес потрапили у відкритий доступ через вразливість у публічному API.

Відповідальність (Accountability). Організація несе відповідальність за справедливе та недискримінаційне використання алгоритмів моніторингу. Системи штучного інтелекту, що тренуються на необ'єктивних даних, можуть відтворювати та навіть посилювати суспільні упередження. Класичний приклад: внутрішній AI-інструмент Amazon для оцінки резюме (2018) систематично

знижував рейтинги кандидаток-жінок, оскільки модель тренувалася на резюме переважно чоловіків. Проект було закрито після публічного скандалу.

Основні виклики та тренди

Поточні виклики риск-моніторингу

Обсяг даних. За оцінками IDC (<https://www.idc.com>), у 2025 році людство створило 180 зетабайтів даних. Лише Twitter генерує 200 ТБ текстових даних щодня. Для обробки таких обсягів потрібні розподілені системи (Hadoop, Apache Spark), техніки стиснення та вибіркового sampling. Зберігання «всього підряд» є технічно можливим, але економічно недоцільним - тому критично важливо правильно налаштувати фільтри збору.

Швидкість. Вірусний контент може набрати мільйон переглядів за одну годину. Батч-обробка даних (раз на добу або раз на годину) є абсолютно неприйнятною для завдань кризового реагування. Необхідна потокова обробка (stream processing) із затримкою менше однієї секунди. Ключові технології: Apache Kafka (обробляє трильйон повідомлень на день у Uber), Apache Flink, AWS Kinesis.

Багатомовність. Facebook підтримує 111 мов, Twitter - понад 40. Більшість NLP-моделей тренуються переважно на англійськомовних даних, що призводить до значно нижчої точності для інших мов. Для вирішення цієї проблеми використовуються мультилінгвальні моделі: mBERT (Multilingual BERT від Google), XLM-RoBERTa. Додаткову складність становлять мовні змішування (суржик, Spanglish), сленг, аббревіатури та нові слова.

Контекст та іронія. Базові NLP-моделі погано справляються із сарказмом та іронією. Речення «Чудово! Ще одне відкликання продукту. Саме цього нам не вистачало» - формально позитивне, фактично - глибоко негативне. Трансформерні моделі (BERT, GPT) значно краще вловлюють контекст, але все одно потребують human-in-the-loop для перевірки складних випадків. Культурні нюанси додають ще один рівень складності: жест «ОК» в одній культурі є образливим в іншій.

Дипфейки. Технологія GAN (Generative Adversarial Networks) дозволяє створювати надреалістичні підроблені відео та аудіо. У 2022 році в Telegram

з'явилося дипфейк-відео Президента Зеленського із закликом до капітуляції - і хоча воно було швидко спростоване, встигло поширитися мільйонами переглядів. У 2019 році шахраї використали клонований голос СЕО британської компанії для телефонного шахрайства, вкравши \$243 000. Детекція дипфейків (Microsoft Video Authenticator, Sensity AI) залишається складним технічним завданням.

Приватність. Фундаментальна дилема: для ефективного моніторингу потрібно більше даних, але це суперечить праву на приватність. Поширення end-to-end шифрування (Signal, WhatsApp) взагалі блокує можливість моніторингу приватних комунікацій. Перспективні рішення: differential privacy (Apple використовує для збору телеметрії iOS), federated learning (навчання моделей без передачі даних на центральний сервер), homomorphic encryption.

Тренди 2025–2026: майбутнє соціальних мереж

AI-генерований контент. Великі мовні моделі (ChatGPT, Claude, Gemini, Llama) здатні генерувати тексти, невідрізнені від написаних людиною. Це породжує масштабну проблему: тисячі AI-згенерованих відгуків, коментарів, постів можуть маніпулювати громадською думкою. Amazon зафіксував сотні тисяч підозрілих AI-відгуків у 2024 році. Детекція AI-контенту (GPTZero - <https://gptzero.me>, Originality.ai - <https://originality.ai>) поки що забезпечує точність ~70–85%. OpenAI та Google впроваджують цифрові водяні знаки (watermarking) у генерований контент.

Децентралізовані соціальні мережі. Web3-платформи (Mastodon, Bluesky, Lens Protocol) розподіляють дані між незалежними серверами без єдиного власника. Mastodon має 14 мільйонів користувачів (2026), Bluesky - 3 мільйони. Відсутність централізованого API ускладнює моніторинг: дані розпорошені між тисячами незалежних серверів (instance), кожен із власними правилами і API. Monokultureнні ризики централізованих платформ замінюються складністю децентралізованої архітектури.

Video-First. YouTube Shorts генерує 70 мільярдів переглядів на день. Instagram Reels і TikTok перетворили короткі вертикальні відео на домінуючий формат контенту. Відеоаналітика значно складніша за текстову: вона вимагає

computer vision (YOLO для розпізнавання об'єктів), speech-to-text (OpenAI Whisper - <https://openai.com/research/whisper>), аналізу аудіодоріжки та відеоряду одночасно. Вартість обробки відео на порядки вища, ніж тексту.

Голосові та аудіо-формати. Глобальна аудиторія подкастів перевищила 500 мільйонів слухачів у 2026 році. Аудіосоціальні мережі (Twitter Spaces, Discord voice channels, Spotify Live) набирають популярності. Клонування голосу (ElevenLabs - <https://elevenlabs.io>) дозволяє відтворити голос будь-якої людини за 30 секунд запису. Аудіодипфейки стають новою загрозою, а транскрипція й аналіз аудіо залишаються ресурсомісткими технічними задачами.

Метавсесвіт. Meta Horizon Worlds, Roblox (70+ млн щоденних користувачів), Decentraland і The Sandbox - соціалізація перетікає у тривимірні віртуальні простори. Apple Vision Pro (2024) відкрив еру просторових обчислень. Для риск-моніторингу це нові виклики: одночасний аналіз текстового та голосового чату, поведінки аватарів у 3D-просторі, ідентифікація harassment у VR-середовищі. Правова база для таких ситуацій лише починає формуватися.

ПРАКТИЧНІ ПРИКЛАДИ З ПОСИЛАННЯМИ

Приклад 1. Вірусна кампанія #IceBucketChallenge (2014)

У 2014 році в соціальних мережах розгорнулася одна з найуспішніших вірусних кампаній з підвищення обізнаності про хворобу ALS (бічний аміотрофічний склероз). Механіка проста: учасник виливає на себе відро крижаної води, знімає відео, публікує в соцмережах і номінує друзів зробити те саме або пожертвувати гроші на дослідження ALS. Кампанія за кілька тижнів охопила увесь світ: 17 мільйонів відео, 440 мільйонів переглядів, участь Білла Гейтса, Марка Цукерберга, Опри Вінфрі. Результат: зібрано \$115 мільйонів для Асоціації ALS - у 35 разів більше, ніж за аналогічний період попереднього року. Кошти дозволили фінансувати дослідження, що призвели до відкриття нового гена, пов'язаного з ALS. Детальна інформація: <https://www.als.org/stories-news/ice-bucket-challenge>. Ця кампанія є класичним прикладом того, як риск-моніторинг у режимі real-time дозволяє відстежувати вірусний потенціал контенту та вчасно підключатися до трендів.

Приклад 2. GameStop Short Squeeze (2021)

У січні 2021 року користувачі спільноти r/WallStreetBets на Reddit організували скоординовану купівлю акцій GameStop - мережі магазинів відеоігор, яка вважалася приреченою. Мета: «задушити» хедж-фонди, що зробили ставку на падіння акцій (short position). Протягом одного тижня акції GameStop злетіли з \$20 до \$483. Хедж-фонди зазнали збитків на понад \$5 млрд. Ця подія стала предметом слухань у Конгресі США та поставила питання про регулювання координованих ринкових маніпуляцій через соціальні мережі. Офіційний звіт SEC: <https://www.sec.gov/news/press-release/2021-212>. Для риск-моніторингу - це демонстрація того, як sentiment аналіз текстів у Reddit і виявлення аномальної активності ботів могло б попередити банки та інвесторів про майбутній squeeze.

Приклад 3. Telegram в Україні під час повномасштабного вторгнення (2022–2026)

З 24 лютого 2022 року Telegram став основним каналом оперативної інформації для мільйонів українців. Канал «Повітряна тривога» набрав 3+ мільйони підписників і забезпечував сповіщення про ракетні загрози в режимі реального часу. Офіційний Telegram-канал Президента Зеленського має понад 7 мільйонів підписників. Паралельно Telegram став майданчиком для активної дезінформаційної кампанії: російські канали поширювали фейки про хід бойових дій, капітуляцію, жертв серед цивільного населення. Для фахівців із риск-моніторингу це - реальний кейс боротьби з ворожою дезінформацією в умовах активного збройного конфлікту: факт-чекінг, виявлення мереж фейкових акаунтів, аналіз джерел і патернів поширення неправдивих наративів. Детально про роботу Ukrainian fact-checkers: <https://voxukraine.org>.

Приклад 4. Скандал Cambridge Analytica (2018)

Cambridge Analytica - британська компанія з аналізу даних - отримала через quiz-додаток на Facebook персональні дані 87 мільйонів користувачів без їхнього відома. Ці дані були використані для побудови психографічних профілів і мікротаргетованої політичної реклами під час президентських виборів у США (2016) і референдуму Brexit. Скандал спровокував падіння акцій Facebook на 7% за два дні (\$37 млрд ринкової капіталізації). Марк Цукерберг виступив перед

Конгресом. Штраф від FTC (Федеральна торгова комісія США): \$5 млрд - рекорд на той час. Детальний розбір: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Цей кейс є ключовим у розумінні того, чому GDPR і ССРА виникли саме у 2018–2020 роках - як пряма реакція на зловживання даними.

КЛЮЧОВІ ТЕРМІНИ ЛЕКЦІЇ

Термін	Визначення
Social Media Risk Monitoring	Систематичний процес виявлення, оцінки та відстеження потенційних загроз у соціальних медіа, що можуть вплинути на організацію або бренд.
Sentiment Analysis	Аналіз тональності тексту - автоматичне визначення емоційного забарвлення (позитив / негатив / нейтраль) за допомогою NLP-алгоритмів.
Viral Effect	Механізм швидкого та масового поширення контенту через соціальні мережі за принципом геометричної прогресії.
GDPR	General Data Protection Regulation - Загальний регламент захисту даних ЄС (2018). Основний міжнародний стандарт у сфері приватності.
Deepfake	Синтетичний медіаконтент (відео / аудіо), створений за допомогою AI (GAN) для переконливої імітації реальних людей.
API	Application Programming Interface - програмний інтерфейс для взаємодії між системами; основний спосіб отримання даних від соціальних платформ.
NLP	Natural Language Processing - обробка природної мови; галузь AI, що дозволяє комп'ютерам розуміти і аналізувати людський текст.
Bot / Botnet	Автоматизовані акаунти, що імітують поведінку людей; мережа ботів, що діє скоординовано для маніпуляцій або атак.
Compliance (Комплаєнс)	Відповідність діяльності організації вимогам законів, регуляцій та внутрішніх стандартів.
Dark Pattern	Маніпулятивний UI/UX-дизайн, що навмисно вводить користувача в оману або змушує його приймати небажані рішення.
Stream Processing	Обробка даних у режимі реального часу (потоків), без зупинки для накопичення партій. Критично важлива для ризик-моніторингу.
Filter Bubble	Ефект «фільтрової бульбашки» - персоналізований алгоритмічний контент, що ізолює користувача від альтернативних точок зору.

ВИСНОВКИ

Перша лекція заклала концептуальний фундамент дисципліни «Ризик-моніторинг у соціальних мережах». Ми побачили, що соціальні мережі пройшли

шлях від нішевих платформ для спілкування до глобальної інфраструктури, що охоплює понад 5 мільярдів людей і формує суспільну реальність. Цей масштаб породжує принципово нові ризики - репутаційні, кіберсек'юрити, правові, інформаційні, - для управління якими необхідна системна і технологічно зріла відповідь.

Ризик-моніторинг є не просто технічним інструментом, а цілісною управлінською практикою, що поєднує збір і аналіз даних, правову відповідність, комунікаційні стратегії і технічну безпеку. Для фахівця зі спеціальності 122 - Комп'ютерні науки (Консолідована інформація) ця дисципліна є прямим практичним застосуванням ключових компетентностей: роботи з API, обробки великих даних, застосування алгоритмів NLP та машинного навчання.

Ключові висновки з лекції: по-перше, соціальні мережі є критично важливим джерелом консолідованої інформації, яка вимагає системного підходу до збору, обробки та інтерпретації; по-друге, ефективний ризик-моніторинг будується на п'яти взаємопов'язаних компонентах - збір, зберігання, аналіз, візуалізація та реагування - кожен з яких використовує специфічний технологічний стек; по-третє, будь-яка робота з даними соціальних мереж здійснюється у строго визначеному правовому полі GDPR, CCPA, DSA та українського законодавства; по-четверте, технологічні тренди (AI-контент, децентралізація, відеодомінування) постійно змінюють ландшафт викликів і потребують безперервного оновлення знань.

Наступні лекції поглиблюють кожен із компонентів системи: детально розглянемо збір даних через API, алгоритми sentiment-аналізу, методи виявлення ботів, архітектуру real-time систем та побудову кризових комунікаційних стратегій.

КОНТРОЛЬНІ ПИТАННЯ ДЛЯ САМОПЕРЕВІРКИ

1. Яку роль відіграла теорія «шести рукоштовань» у виникненні першої соціальної мережі SixDegrees.com? Чи релевантна ця теорія для сучасних платформ?

2. Чим принципово відрізняється риск-моніторинг від звичайного моніторингу соціальних мереж? Назвіть не менше трьох відмінностей.
3. Уявіть, що ви - фахівець із риск-моніторингу банку. Опишіть, яким чином кожний із п'яти компонентів системи моніторингу використовуватиметься для захисту репутації фінансової установи.
4. Чому компанії поза межами Євросоюзу зобов'язані дотримуватись GDPR? Наведіть приклад з реального бізнесу.
5. У чому полягає принципова різниця між GDPR і DSA? Які конкретні обов'язки покладає DSA на великі платформи?
6. Поясніть, чому sentiment analysis погано справляється із сарказмом. Як технологія BERT вирішує цю проблему?
7. Проаналізуйте скандал Cambridge Analytica: які конкретні положення GDPR порушила ця компанія? Якими могли б бути штрафи за сучасним законодавством?
8. Ефект «фільтрової бульбашки» (filter bubble) - це технічна проблема, бізнес-модель чи соціальна небезпека? Аргументуйте свою відповідь.
9. Чому виявлення дипфейків є технічно складнішим завданням, ніж виявлення звичайних фейків? Які підходи використовуються для детекції?
10. Сформулюйте власний кейс: оберіть будь-яку відому компанію або організацію, що зазнала репутаційної кризи через соціальні мережі, та опишіть, як система риск-моніторингу могла б запобігти або пом'якшити наслідки цієї кризи.

Література

Офіційна документація та регуляторні органи

GDPR Official Site: <https://gdpr.eu>

European Data Protection Board: <https://edpb.europa.eu>

CCPA Official Information: <https://oag.ca.gov/privacy/ccpa>

Digital Services Act (EU): <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

Закон України про захист персональних даних:
<https://zakon.rada.gov.ua/laws/show/2297-17>

Інструменти ризик-моніторингу

Brandwatch: <https://www.brandwatch.com>

Brand24: <https://brand24.com>

Mention: <https://mention.com>

Sprout Social: <https://sproutsocial.com>

Hootsuite Insights: <https://www.hootsuite.com/products/insights>

Talkwalker: <https://www.talkwalker.com>

Кібербезпека та виявлення загроз

ZeroFOX: <https://www.zerofox.com>

RiskIQ (Microsoft): <https://www.riskiq.com>

Recorded Future: <https://www.recordedfuture.com>

Microsoft Video Authenticator (Deepfakes): <https://www.microsoft.com/en-us/research/project/video-authenticator>

Статистика та дослідження

DataReportal – Global Digital Reports: <https://datareportal.com>

Statista – Social Media Statistics: <https://www.statista.com/topics/1164/social-networks/>

Pew Research Center – Social Media: <https://www.pewresearch.org/internet/fact-sheet/social-media/>

IDC – Data & Analytics: <https://www.idc.com>

NLP та AI інструменти

Hugging Face – NLP Models: <https://huggingface.co/models>

spaCy – Industrial NLP: <https://spacy.io>

NLTK – Natural Language Toolkit: <https://www.nltk.org>

OpenAI Whisper: <https://openai.com/research/whisper>

GPTZero – AI Content Detection: <https://gptzero.me>

Факт-чекінг та верифікація

VoxUkraine – Ukrainian Fact-Checkers: <https://voxukraine.org>

StopFake Ukraine: <https://www.stopfake.org/uk>

IFCN – International Fact-Checking Network: <https://www.poynter.org/ifcn>

ЛЕКЦІЯ 2. РЕПУТАЦІЙНІ РИСКИ В СОЦІАЛЬНИХ МЕРЕЖАХ

ВСТУП

У сучасному цифровому середовищі репутація організації чи особи формується не лише завдяки реальним діям, а й через те, як ці дії сприймаються та інтерпретуються в онлайн-просторі. Соціальні мережі докорінно змінили правила гри: те, що раніше могло залишитись непоміченим або стати темою для обговорення у вузькому колі, сьогодні здатне за лічені години перетворитися на глобальний скандал.

Студентам, які вивчають ризик-моніторинг у соціальних мережах, важливо розуміти: репутаційні ризики - це не абстрактна загроза, а цілком конкретний явище, яке має свою природу, механізми поширення та інструменти управління. Ця лекція допоможе вам сформуванати системне уявлення про репутаційні ризики, навчитися їх класифікувати, вимірювати та відстежувати.

Вступне визначення: репутаційний ризик - це ймовірність виникнення ситуації, яка негативно впливає на сприйняття організації, бренду або особи з боку ключових аудиторій (клієнтів, партнерів, інвесторів, суспільства), і яка може призвести до фінансових або нефінансових втрат.

Чому ця тема особливо актуальна сьогодні? Причин декілька:

- Глобальна цифровізація: понад 5,4 млрд людей у світі користуються інтернетом (Statista, 2024), з яких понад 5 млрд є активними користувачами соціальних мереж.
- Швидкість поширення інформації: негативна новина може охопити мільйони людей за 15–30 хвилин завдяки механізмам репостів, хештегів та алгоритмів платформ.
- Необоротність наслідків: навіть після видалення контенту він зберігається в архівах, скріншотах та кешах пошукових систем.
- Зростання «ціни» репутації: за оцінками World Economic Forum (2023), понад 25% ринкової вартості компаній формується нематеріальними активами, серед яких репутація - один із ключових.

- Українська специфіка: в умовах воєнного часу та активної інформаційної боротьби репутаційні ризики набувають додаткового виміру - вони можуть бути інструментом ворожих впливових операцій.

ПЛАН ЛЕКЦІЇ

1. Вступ. Що таке репутаційний ризик та чому він набуває критичного значення в цифрову епоху.
2. Поняття, сутність та особливості репутаційних ризиків.
3. Класифікація репутаційних ризиків: типи, джерела, масштаби наслідків.
4. Механізм виникнення та поширення репутаційних криз у соціальних мережах.
5. Аналіз резонансних кейсів: українські та міжнародні приклади.
6. Метрики для вимірювання та оцінки репутаційних ризиків.
7. Інструменти моніторингу репутації в режимі реального часу.
8. Контрольні питання.
9. Список використаних джерел.

ПОНЯТТЯ, СУТНІСТЬ ТА ОСОБЛИВОСТІ РЕПУТАЦІЙНИХ РИСКІВ

Визначення репутаційного ризику

У науковій літературі репутаційний ризик визначається по-різному. Розглянемо кілька ключових підходів:

Підхід 1 - фінансовий: репутаційний ризик - це ризик виникнення збитків або недоотримання запланованих доходів внаслідок формування у суспільстві негативного уявлення про організацію (Базельський комітет з банківського нагляду, Principles for the Sound Management of Operational Risk, 2021).

Підхід 2 - комунікаційний: репутаційний ризик - це загроза розриву між очікуваннями стейкхолдерів (зацікавлених сторін) та фактичною поведінкою компанії, що стає публічно відомою (Doorley & Garcia, Reputation Management, 2020).

Підхід 3 - цифровий: в умовах соціальних мереж репутаційний ризик - це ризик виникнення вірусного поширення негативного контенту, що формує стійко

негативний образ бренду чи особи в цифровому середовищі (Aula, P., Reputation and Social Media, 2022).

Узагальнене визначення для цілей нашого курсу: 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, та може спричинити значні фінансові й нефінансові втрати в короткостроковій або довгостроковій перспективі.

Ключові характеристики репутаційних ризиків

Репутаційні ризики мають ряд особливостей, які відрізняють їх від інших видів ризиків:

- Асиметрія: репутацію будують роками, а зруйнувати можна за одну ніч. Негативні новини поширюються значно швидше, ніж позитивні (феномен «негативного упередження», або negativity bias).
- Каскадний ефект: репутаційна криза, як правило, тягне за собою інші ризики - фінансові (падіння акцій, відтік клієнтів), операційні (звільнення співробітників), юридичні (позови та штрафи).
- Невизначеність джерела: ризик може виникнути зсередини організації (дії співробітника) або зовні (атака конкурентів, дезінформація).
- Складність вимірювання: репутація - нематеріальний актив, тому її пошкодження важко виразити в точних цифрах на момент кризи.
- Глобальність: у цифровому середовищі репутаційна криза не знає кордонів - локальний скандал може стати міжнародним.

КЛАСИФІКАЦІЯ РЕПУТАЦІЙНИХ РИСКІВ

За джерелом виникнення

Репутаційні ризики можна поділити на внутрішні та зовнішні залежно від того, де виникає загроза.

Внутрішні ризики - це загрози, що виходять з самої організації:

- Неетична поведінка керівництва або співробітників (дискримінаційні висловлювання, сексуальні домагання, корупція).

- Якість продукту або послуги нижче задекларованого рівня (прихований брак, шкідливі компоненти).
- Провальні маркетингові та рекламні кампанії (образливий контент, неоднозначні меседжі).
- Витік конфіденційної інформації (персональні дані клієнтів, комерційна таємниця).
- Помилки в кризовому PR - неправильна або несвоєчасна реакція на скандал.

Зовнішні ризики - загрози, що надходять із зовнішнього середовища:

- Цілеспрямовані кампанії конкурентів або зловмисників (чорний PR, фальшиві відгуки, дезінформація).
- Дії активістів або незадоволених клієнтів (вірусні скарги, бойкоти, петиції).
- Негативне висвітлення в медіа та від інфлюєнсерів.
- Хакерські атаки та кіберінциденти з публічним розголосом.
- Загальносуспільні кризи (пандемія, військові дії), що змінюють контекст сприйняття.

За типом контенту

Якщо аналізувати репутаційні ризики крізь призму типу контенту, що генерує загрозу, виділяють:

Тип ризику	Опис	Приклад	Типові наслідки
Негативні відгуки та скарги клієнтів	Масове незадоволення продуктом/сервісом	Хвиля 1-зіркових відгуків після зміни рецептури продукту	Падіння продажів, відтік клієнтів
Viral-скандали	Миттєве вірусне поширення компрометуючого відео чи фото	Відео з некоректною поведінкою співробітника	Падіння акцій, потреба у публічних вибаченнях
Фейки та дезінформація	Поширення брехливих або спотворених новин	Фальшива новина про банкрутство компанії	Паніка серед клієнтів, судові позови
Скандали з персоналом	Публічне розкриття некоректної поведінки співробітників	Виявлення дискримінаційного корпоративного чату	Вимога звільнень, реструктуризація HR

Тип ризику	Опис	Приклад	Типові наслідки
Product fails	Публічні дефекти або небезпека продукції	Масове відкликання товару через несправність	Мільйонні збитки, регуляторні санкції
Атаки тролів та хейтерів	Організовані кампанії ненависті	Координоване нападання на сторінки бренду	Токсична репутація, відхід авторів контенту
Витік даних	Компрометація персональних даних клієнтів	Злам бази даних з оприлюдненням паролів	GDPR-штрафи, втрата довіри

За масштабом та географією

За масштабом поширення репутаційні ризики класифікують на:

- Локальні - зачіпають певний регіон чи громаду (скарги жителів конкретного міста на поведінку компанії).
- Національні - охоплюють всю країну (скандал з державною компанією в Україні, що стає темою №1 у новинах).
- Міжнародні - перетинають кордони (бойкоти міжнародних брендів у зв'язку з їхньою позицією щодо воєнних дій).
- Глобальні - миттєво стають відомими в усьому світі завдяки вірусному поширенню.

МЕХАНІЗМ ВИНИКНЕННЯ ТА ПОШИРЕННЯ РЕПУТАЦІЙНИХ КРИЗ

Стадії розвитку репутаційної кризи

Репутаційна криза рідко виникає миттєво - вона, як правило, проходить кілька стадій:

1. Передкризова стадія (latent stage): існують передумови для кризи (незадоволені клієнти, внутрішній конфлікт, проблема з якістю продукту), але вони ще не є публічними. На цьому етапі ризик можна виявити за допомогою моніторингу та вжити превентивних заходів.
2. Тригерна подія (trigger event): відбувається конкретна подія або публікується контент, який запускає кризу. Це може бути одне відео, одна новина або одна помилка співробітника.

3. Ескалація (escalation): контент починає поширюватися в соціальних мережах. Вступає в дію механізм вірусного поширення - репости, хештеги, коментарі, підхоплення медіа та інфлюєнсерами.

4. Пік кризи (peak): максимальний обсяг обговорення, максимальний негативний вплив. Саме на цій стадії найчастіше відбуваються найбільш відчутні фінансові втрати.

5. Затухання (declining): інтерес аудиторії знижується, обсяг згадок зменшується. Однак репутаційні «шрами» залишаються в пошукових системах та в пам'яті аудиторії.

6. Посткризовий стан (post-crisis): організація або відновлює довіру (якщо правильно відреагувала), або продовжує нести репутаційні втрати (якщо реакція була невдалою).

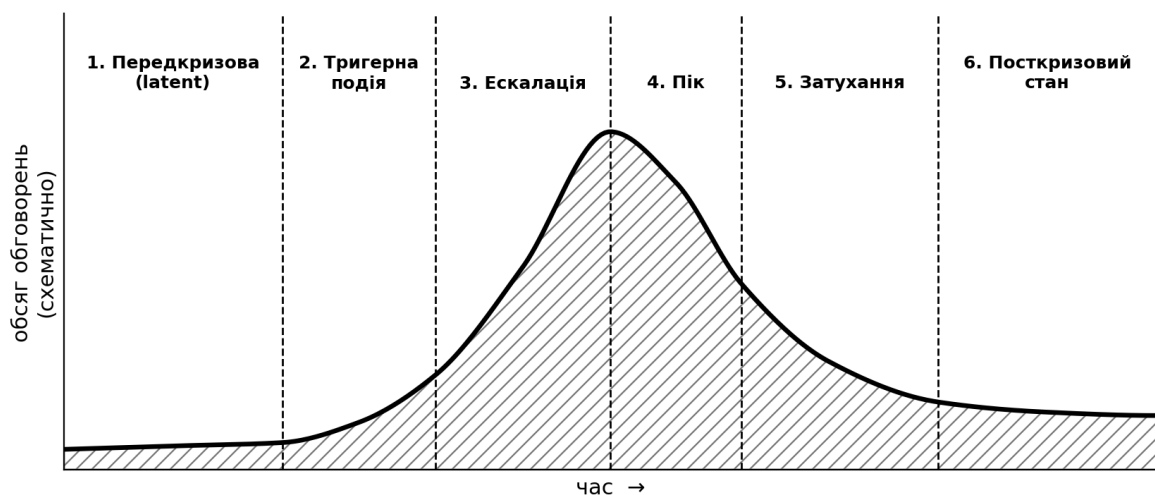


Рис. 2.1. Стадії розвитку репутаційної кризи (схематичний графік обсягу обговорень)

Роль алгоритмів соціальних мереж у поширенні ризиків

Важливо розуміти, що сучасні алгоритми соціальних мереж (Meta, TikTok, YouTube) побудовані на максимізації залученості (engagement). Контент, що викликає сильні емоції - особливо обурення, страх чи огиду - органічно отримує більше поширення. Це означає, що негативний контент про бренд чи особу поширюється значно швидше, ніж позитивний. Дослідження MIT (Vosoughi et al., 2018, журнал Science) показало, що брехня поширюється в 6 разів швидше, ніж правда у Twitter/X. Цей феномен безпосередньо впливає на динаміку репутаційних криз.

АНАЛІЗ РЕЗОНАНСНИХ КЕЙСІВ

Українські кейси

Кейс 1: ПриватБанк та зміна власника (2016–2017)

У грудні 2016 року ПриватБанк - найбільший приватний банк України - було націоналізовано. В соціальних мережах миттєво виникла хвиля паніки серед вкладників. Facebook, Instagram та Telegram переповнилися дописами про «крах банку», чергах до банкоматів та питаннями «чи повернуть вклади».

Ключові аспекти репутаційного ризику:

- Поширення неперевіреної інформації в Telegram-каналах спричинило масовий відтік коштів.
- Банк та НБУ були змушені в режимі реального часу спростовувати фейки через офіційні сторінки.
- Репутаційна криза банку частково пов'язана з інформаційними атаками ексвласників.
- Ситуація показала вразливість фінансового сектору до репутаційних ризиків у соціальних мережах.

Де дізнатися більше:

Економічна правда: Націоналізація ПриватБанку

Кейс 2: Rozetka та скарги на сервіс доставки (2020–2021)

Під час пандемії COVID-19 Rozetka - найбільший інтернет-ритейлер України - зіткнулась з різким зростанням замовлень та проблемами з доставкою. Соціальні мережі, особливо Facebook, заповнилися тисячами скарг про затримки, неповернення коштів та низьку якість підтримки.

Ключові аспекти:

- Хештег з критикою компанії потрапив у тренди українського Twitter.
- Блогери та інфлюєнсери почали публічно відмовлятися від послуг компанії.
- Компанія розгорнула масштабну кампанію з реагування на відгуки в соцмережах.
- Кейс показав, як операційні проблеми миттєво трансформуються в репутаційні ризики.

Де дізнатися більше:

AIN.UA: Проблеми Rozetka під час карантину

Кейс 3: Укрпошта та репутаційний моніторинг під час повномасштабного вторгнення (2022–2024)

З початком повномасштабного вторгнення у лютому 2022 року Укрпошта опинилась в центрі уваги як критична інфраструктура. З одного боку, організація набула позитивного розголосу завдяки маркам з лінкором «Москва» та героїчними меседжами. З іншого - зіткнулась з хвилями критики через затримки посилок, перебої в роботі та обвинувачення в неефективності.

Ключові аспекти:

- Приклад того, як правильна комунікаційна стратегія (патріотичний контент) може перекрити репутаційні ризики.
- Водночас, конкретні випадки втрат посилок отримували різкий резонанс у Facebook-групах.
- Компанія активно реагувала на скарги через офіційну сторінку у Facebook.
- Кейс демонструє складність управління репутацією в умовах воєнного часу.

Офіційні новини Укрпошти

Кейс 4: Інформаційні атаки на українські банки (2022 – дотепер)

Після 24 лютого 2022 року Служба безпеки України неодноразово фіксувала цілеспрямовані інформаційні атаки на банківський сектор - поширення фейків про «банкрутства» банків, закриття відділень, заморожування рахунків. Мета - спровокувати паніку серед населення та дестабілізувати фінансову систему.

Це принципово новий вид репутаційного ризику - репутаційна зброя як інструмент гібридної війни.

СБУ: блокування спецоперацій проти фінансової системи

5.2. Американські кейси

Кейс 5: United Airlines - «Dragging Incident» (2017)

Один з найгучніших репутаційних скандалів десятиліття. Пасажира Девіда Дао силоміць витягли з переповненого рейсу United Airlines у Чикаго. Очевидці зняли відео на смартфони та опублікували в Twitter і Facebook. За 24 години кількість переглядів перевищила 100 мільйонів, а хештег #BoycottUnitedAirlines став №1 у тренді.

Фінансові наслідки:

- Акції United Continental Holdings впали з \$71.97 до \$69.03 за добу (-4.0%).
- Ринкова капіталізація зменшилась приблизно на \$955 мільйонів.
- CEO Оскар Муньос спочатку виправдав дії співробітників - це поглибило кризу.
- Компанія врешті виплатила компенсацію та переглянула overbooking-політику.

Урок: першочергова реакція керівника (захист замість визнання помилки) посилила кризу в рази. Своєчасне і щире вибачення могло обмежити збитки.

The Guardian: United Airlines - повний аналіз кризи

Кейс 6: Facebook / Cambridge Analytica (2018)

У березні 2018 року розслідування The Guardian та New York Times виявили, що компанія Cambridge Analytica незаконно отримала дані 87 мільйонів користувачів Facebook для цільових політичних рекламних кампаній. Це спричинило один з найбільших репутаційних і регуляторних скандалів в історії технологічних компаній.

Ключові наслідки:

- Хештег #DeleteFacebook набрав мільйони публікацій. Навіть Елон Маск публічно видалив сторінки Tesla та SpaceX.
- Акції Facebook впали майже на 20% протягом кількох тижнів після публікації.
- Марк Цукерберг змушений був давати показання перед Конгресом США та Парламентом ЄС.
- FTC (Федеральна торгова комісія США) виписала штраф \$5 млрд - найбільший в історії технологічного регулювання на той момент.

– Введено GDPR в ЄС отримало новий імпульс для ефективного впровадження.

New York Times: Cambridge Analytica - детальний аналіз

5.3. Європейські кейси

Кейс 7: H&M - «Coolest Monkey in the Jungle» (2018, Швеція/Глобально)

H&M опублікували рекламне фото темношкірого хлопчика у толстовці з написом «Coolest Monkey in the Jungle» на своєму вебсайті та в соціальних мережах. Пост у Facebook та Instagram миттєво викликав шквал звинувачень у расизмі. Відомі виконавці, зокрема The Weeknd, публічно заявили про розрив партнерства з брендом.

Наслідки:

- Магазины H&M у Південній Африці були розгромлені протестувальниками.
- Продажі впали на 25% у перші тижні після скандалу.
- Компанія видалила фото, принесла публічні вибачення та звільнила відповідального за затвердження контенту.
- Введено обов'язкові тренінги з різноманіття та інклюзії для всього персоналу маркетингу.

Урок: перевірка контенту перед публікацією крізь призму різних культурних та соціальних груп - обов'язковий елемент риск-менеджменту в маркетингу.

BBC News: H&M скандал - повна хронологія

Кейс 8: Volkswagen - «Дизельгейт» (2015, Німеччина/Глобально)

У вересні 2015 року агентство EPA (США) оголосило, що Volkswagen свідомо встановлював програмне забезпечення для обману тестів на викиди. Скандал охопив 11 мільйонів автомобілів по всьому світу. Соціальні мережі і ЗМІ підхопили тему з виразом «Dieselgate», що стала синонімом корпоративного обману.

Наслідки:

- Акції VW впали більш ніж на 30% за два тижні (втрата понад €26 млрд ринкової капіталізації).
- CEO Мартін Вінтеркорн пішов у відставку через чотири дні після скандалу.
- Загальні штрафи та компенсації перевищили \$35 млрд у різних країнах.
- Бренд Volkswagen до сьогодні асоціюється з цим скандалом у контексті корпоративної чесності.

BBC News: Volkswagen Dieselgate - аналіз кризи

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке репутаційний ризик? Надайте визначення та поясніть його ключові характеристики.
2. Чим відрізняється репутаційний ризик від інших видів ризиків (фінансових, операційних)?
3. Назвіть та охарактеризуйте основні типи репутаційних ризиків за класифікацією з лекції.
4. Яка різниця між внутрішніми та зовнішніми репутаційними ризиками? Наведіть по 2 приклади кожного.
5. Опишіть стадії розвитку репутаційної кризи. На якій стадії найефективніше втрутитися?
6. Чому негативний контент поширюється швидше, ніж позитивний? Поясніть роль алгоритмів соціальних мереж.

Література

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-conjurers/>
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.

ЛЕКЦІЯ 3. КІЛЬКІСНІ МЕТОДИ ОЦІНКИ РЕПУТАЦІЙНИХ РИСКІВ У СОЦІАЛЬНИХ МЕРЕЖАХ

ВСТУП

Попередня лекція заклала теоретичне підґрунтя: ми розглянули природу репутаційних ризиків, їхні типи та джерела, механізми виникнення і поширення криз, а також проаналізували резонансні кейси з українського та міжнародного досвіду. Тепер, коли концептуальний апарат сформовано, логічним кроком є перехід від якісного опису до кількісного вимірювання.

Фахівець із ризик-моніторингу зобов'язаний не просто фіксувати факт наявності негативного контенту, а точно оцінювати його масштаб, динаміку та потенційну небезпеку. Саме для цього розроблені спеціалізовані метрики, які перетворюють розрізнені публікації у соціальних мережах на структуровані числові показники, придатні для управлінських рішень.

Ця лекція присвячена шести ключовим методикам кількісної оцінки репутаційних ризиків. Для кожної методики детально пояснено логіку побудови, наведено математичний апарат і розглянуто конкретні приклади розрахунків із поясненням висновків. Особливу увагу приділено порівнянню різних методик між собою: на практиці вони застосовуються не ізольовано, а як взаємодоповнюючий аналітичний інструментарій.

Опанування цих методик дозволить не лише виявляти загрози, а й обґрунтовувати управлінські рішення числовими аргументами, що є критично важливою навичкою в сучасному корпоративному середовищі.

ПЛАН ЛЕКЦІЇ

1. Вступ. Від якісного опису до кількісного вимірювання репутаційних ризиків.
2. Методика 1. Net Sentiment Score (NSS) - індекс тональності згадок: формула, розрахунок, інтерпретація.
3. Методика 2. Weighted Reputation Index (WRI) - зважений індекс репутації: логіка ваг, відмінність від NSS.

4. Методика 3. Crisis Probability Score (CPS) - оцінка ймовірності репутаційної кризи: компоненти, нормування, приклад.
5. Методика 4. Reputation Risk Matrix (RRM) - матриця репутаційних ризиків: побудова, шкала, практичне застосування.
6. Методика 5. Sentiment Trend Analysis (STA) - аналіз динаміки тональності: виявлення передкризових сигналів.
7. Методика 6. Channel Risk Distribution (CRD) - розподіл ризику за каналами: пріоритизація платформ.
8. Комплексне застосування методик та взаємозв'язок між ними.
9. Висновки та контрольні питання.

МЕТОДИКА 1. NET SENTIMENT SCORE (NSS) - ІНДЕКС ТОНАЛЬНОСТІ ЗГАДОК

Логіка та призначення методики

Net Sentiment Score (NSS) є базовою метрикою репутаційного моніторингу. Вона відповідає на найпростіше і найважливіше запитання: скільки людей говорять про бренд позитивно порівняно з тими, хто говорить негативно? Ця метрика аналогічна за своєю логікою показнику Net Promoter Score (NPS), широко відомому в маркетингу, але застосована не до опитувань клієнтів, а до публічного дискурсу в соціальних мережах.

Принципова ідея NSS полягає у тому, що нейтральні публікації не несуть репутаційного навантаження - вони не формують ні позитивного, ні негативного образу. Тому методика фокусується виключно на «полярних» повідомленнях: позитивних (висловлення задоволення, подяка, рекомендації, схвальні відгуки) та негативних (скарги, звинувачення, критика, іронічні або саркастичні коментарі).

Перед проведенням розрахунку кожна публікація у вибірці класифікується вручну або автоматично за допомогою NLP-інструментів (наприклад, VADER або BERT-based models) на три категорії: позитивна (P), нейтральна або негативна (N). Точність класифікації безпосередньо визначає точність кінцевого результату.

Формула розрахунку

NSS розраховується за такою формулою:

$$NSS = ((P - N) / T) \times 100\%$$

де: P - кількість позитивних публікацій у вибірці; N - кількість негативних публікацій; T - загальна кількість усіх публікацій (P + нейтральні + N). Результат виражається у відсотках і може набувати значень від –100% (усі публікації негативні) до +100% (усі публікації позитивні).

1.3. Шкала інтерпретації NSS

Значення NSS	Стан репутації	Рекомендована реакція
+50% та вище	Відмінний	Підтримувати поточну стратегію комунікації
+20% ... +49%	Добрий	Моніторинг, посилення позитивного контенту
0% ... +19%	Нейтральний	Активізація комунікації, збір зворотного зв'язку
–10% ... –1%	Тривожний	Аналіз причин, антикризова готовність
–30% ... –11%	Критичний	Негайне антикризове реагування
Нижче –30%	Катастрофічний	Повна антикризова мобілізація, залучення PR-спеціалістів

Приклад розрахунку та інтерпретація

Розглянемо умовний приклад для торгової мережі «Сільпо». Аналітик зібрав 60 публікацій у соціальних мережах за останній місяць і класифікував їх таким чином: 28 позитивних (коментарі про якість продуктів, швидке обслуговування, акції), 14 нейтральних (запитання, оголошення, репости новин), 18 негативних (скарги на ціни, чергу, відсутність товарів).

Підстановка у формулу:

$$NSS = ((28 - 18) / 60) \times 100\% = (10 / 60) \times 100\% = +16,7\%$$

Результат: $NSS = +16,7\%$ відповідає нейтральному стану репутації (діапазон $0\% - +19\%$). Попри те, що позитивних публікацій більше, ніж негативних, частка негативу (30% від усіх публікацій) є суттєвою. Це свідчить про те, що значна частина аудиторії незадоволена певними аспектами роботи мережі. Рекомендується активізувати зворотний зв'язок: відповідати на скарги публічно, виявляти системні проблеми та комунікувати про їх вирішення.

Важливі застереження щодо NSS: ця метрика враховує лише кількість публікацій, але не їхній охоплення чи вплив. Один вірусний негативний допис з 50 000 переглядами та одна нікому не відома скарга з двома лайками - рівноцінні в розрахунку NSS. Саме цей недолік усуває наступна методика.

МЕТОДИКА 2. WEIGHTED REPUTATION INDEX (WRI) - ЗВАЖЕНИЙ ІНДЕКС РЕПУТАЦІЇ

Логіка та призначення методики

Weighted Reputation Index (WRI) усуває ключовий недолік NSS - ігнорування реального впливу публікацій. В умовах соціальних мереж важливо не лише те, що написано, а й скільки людей це побачило та відреагувало. Публікація з 2 000 реакціями, 300 коментарями і 500 репостами здійснює на репутацію бренду незрівнянно більший вплив, ніж допис без жодної взаємодії.

WRI вводить концепцію зваженого підрахунку: кожна публікація множиться на свій показник залученості (engagement), який виступає як міра реального охоплення та впливу. Це наближає результат до реальної картини того, що аудиторія насправді бачить і з чим взаємодіє, а не просто до формального підрахунку кількості постів.

Показник залученості (Engagement, E_i) розраховується як сума трьох компонентів: кількість реакцій (лайків, серць тощо) + кількість коментарів + кількість репостів (поширень). Такий підрахунок враховує різні форми взаємодії аудиторії з контентом.

Формула розрахунку

WRI розраховується за такою формулою:

$$\text{WRI} = (\Sigma(P_i \times E_i) - \Sigma(N_i \times E_i)) / \Sigma(T_i \times E_i) \times 100\%$$

де: P_i - i -та позитивна публікація (значення 1 або 0); N_i - i -та негативна публікація; T_i - усі публікації; E_i - показник залученості i -ї публікації (реакції + коментарі + репости). У чисельнику - різниця між зваженою сумою позитивних і негативних публікацій. У знаменнику - зважена сума всіх публікацій (загальний «вагомий обсяг» дискурсу).

Приклад розрахунку та порівняння з NSS

Розглянемо ситуацію для бренду «Нова Пошта» на основі 6 публікацій. Важливо порівняти висновки NSS та WRI для одних і тих самих даних.

№	Тональність	Реакції	Коментарі	Репости	E_i	Зважений внесок
1	Позитивна	95	12	8	115	+115 (позит.)
2	Негативна	1 240	310	580	2 130	−2 130 (негат.)
3	Позитивна	67	9	4	80	+80 (позит.)
4	Нейтральна	23	3	1	27	0 (не враховується)
5	Негативна	340	95	130	565	−565 (негат.)
6	Позитивна	55	7	3	65	+65 (позит.)

Розрахунок NSS (без урахування залученості):

$$\text{NSS} = ((3 - 2) / 6) \times 100\% = +16,7\% - \text{нейтральний стан}$$

Розрахунок WRI (з урахуванням залученості):

$$\text{WRI} = (115 + 80 + 65 - 2\,130 - 565) / (115 + 2\,130 + 80 + 27 + 565 + 65) \times 100\%$$

$$\text{WRI} = (-2\,435) / 2\,982 \times 100\% = -81,7\%$$

Порівняння двох методик наочно демонструє принципову різницю у висновках. NSS = +16,7% говорить про «нейтральний стан» репутації, оскільки позитивних публікацій більше. Однак WRI = −81,7% (катастрофічний стан) виявляє реальну картину: два негативних дописи (публікації №2 і №5) набрали

2 695 одиниць залученості, тоді як три позитивних - лише 260. Аудиторія у 10,4 рази активніше реагувала на негативний контент.

Висновок: у ситуаціях, коли окремі негативні публікації є вірусними (мають аномально високий engagement), NSS може вводити в оману, формуючи хибне відчуття спокою. WRI є більш точним і практично значущим показником реального репутаційного стану. Рекомендується застосовувати обидві метрики паралельно і пояснювати їхні розбіжності.

МЕТОДИКА 3. CRISIS PROBABILITY SCORE (CPS) - ОЦІНКА ЙМОВІРНОСТІ РЕПУТАЦІЙНОЇ КРИЗИ

Логіка та призначення методики

Crisis Probability Score (CPS) відповідає на запитання якісно іншого рівня порівняно з NSS та WRI: не «яким є поточний стан репутації?», а «наскільки ймовірно, що поточна ситуація переросте у повноцінну репутаційну кризу?». Ця метрика є прогностичним інструментом, орієнтованим на майбутнє, а не лише на діагностику поточного стану.

Методика ґрунтується на Situational Crisis Communication Theory (SCCT) Тімоті Кумбса (2023) - одній із найбільш цитованих теорій кризової комунікації. SCCT постулює, що ймовірність і масштаб кризи залежать від кількох факторів одночасно: швидкості поширення негативу, його частки у загальному дискурсі, присутності впливових авторів та медіа. Саме ці фактори і покладені в основу CPS.

CPS поєднує чотири незалежних компоненти, кожен з яких нормується до шкали від 0 до 100, і зважено підсумовує їх. Зваження відображає відносний внесок кожного фактора у розвиток кризи: швидкість поширення є найбільш критичним фактором (35%), тоді як підхоплення медіа, хоч і важливе, має меншу вагу (15%) через те, що медіа є вторинним щодо соціальних мереж каналом.

Компоненти та формула розрахунку

Формула CPS виглядає так:

$$\text{CPS} = (\text{CV} \times 0,35) + (\text{NSS_neg} \times 0,30) + (\text{IR} \times 0,20) + (\text{MR} \times 0,15)$$

Позн.	Компонент	Як розрахувати (нормування до 0–100)	Вага
CV	Crisis Velocity - швидкість поширення негативу	Кількість нових негативних згадок за пікову годину. Нормування: 0 = 0 згадок; 100 = 1 000+ згадок/год. Формула: $CV = (\text{кількість} / 1000) \times 100$, максимум 100.	35%
NSS_neg	Частка негативних згадок у вибірці	$NSS_neg = (N / T) \times 100$. Значення вже знаходиться в шкалі 0–100 без додаткового нормування.	30%
IR	Influencer Reach - охоплення через інфлюєнсерів	Частка негативних публікацій від авторів з аудиторією 10K+ підписників від загальної кількості негативних $\times 100$.	20%
MR	Media Reach - підхоплення медіа	0 - жодного медіа; 50 - публікації в онлайн-виданнях; 100 - публікації в топових ЗМІ (ТСН, Укрінформ, Суспільне тощо).	15%

Шкала інтерпретації CPS

Значення CPS	Рівень загрози	Необхідні дії
0 – 20	Низький	Стандартний моніторинг
21 – 40	Помірний	Посилений моніторинг, підготовка антикризових заготовок
41 – 60	Підвищений	Активація антикризового плану, відповіді на згадки
61 – 80	Високий	Термінова реакція PR-команди, офіційна позиція
81 – 100	Критичний	Мобілізація всіх ресурсів, залучення топ-менеджменту

Приклад розрахунку та інтерпретація

Розглянемо реальну сценарну ситуацію: мережа супермаркетів «АТБ», вівторок, 16:00. У TikTok опубліковано відео, де покупець показує зіпсований товар із чинним терміном придатності. Відео розповсюджується.

Збираємо дані для розрахунку компонентів. За останню годину зафіксовано 120 нових негативних згадок у різних соціальних мережах ($CV = 120/1000 \times 100 = 12$). Із 50 зібраних публікацій 28 є негативними ($NSS_neg =$

$28/50 \times 100 = 56$). З 28 негативних публікацій 5 розміщено авторами з аудиторією понад 10 000 підписників ($IR = 5/28 \times 100 = 17,9$). Регіональне онлайн-видання опублікувало новину про інцидент ($MR = 50$).

Підстановка у формулу:

$$CPS = (12 \times 0,35) + (56 \times 0,30) + (17,9 \times 0,20) + (50 \times 0,15)$$

$$CPS = 4,20 + 16,80 + 3,58 + 7,50 = 32,1$$

Результат: $CPS = 32,1$ відповідає помірному рівню загрози. Криза ще не розгорнулася повною мірою, однак висока частка негативних публікацій (56%) є тривожним сигналом. Рекомендованими діями є посилений моніторинг, підготовка офіційного коментаря від представника компанії, а також проактивне реагування у TikTok із роз'ясненням ситуації. Якщо протягом наступних 2–3 годин ситуація не стабілізується і CV зросте вище 200 згадок/год, CPS перейде у зону підвищеного рівня загрози (41–60).

МЕТОДИКА 4. REPUTATION RISK MATRIX (RRM) - МАТРИЦЯ РЕПУТАЦІЙНИХ РИСКІВ

Логіка та призначення методики

Матриця репутаційних ризиків є адаптацією класичного інструменту ризик-менеджменту для специфічного контексту репутаційних загроз у соціальних мережах. Вона базується на стандарті ISO 31000:2018 «Менеджмент ризиків», де ризик оцінюється за двома незалежними вимірами: ймовірністю виникнення та потенційним масштабом впливу.

Ключова цінність матриці полягає у можливості одночасно відобразити та порівняти множину різних ризиків, визначити пріоритети для управлінської уваги і розподілити ресурси реагування залежно від ступеня загрози. Якщо NSS і WRI описують поточний стан, а CPS - ймовірність кризи, то RRM дає системний погляд на весь портфель ризиків організації.

Шкали оцінювання та формула

Кожен ідентифікований ризик оцінюється за двома параметрами у діапазоні від 1 до 5.

Бал	Ймовірність (Likelihood)	Вплив (Impact)
1	Майже неможливо (< 5% / рік)	Мінімальний: локальне обговорення, немає реальних збитків
2	Малоймовірно (5–20%)	Незначний: помітне зниження NSS, поодинокі скарги
3	Можливо (20–50%)	Помірний: медіа-публікації, відчутне зниження продажів
4	Ймовірно (50–80%)	Суттєвий: вірусне поширення, реакція регуляторів або партнерів
5	Майже неминуче (> 80%)	Критичний: глобальний скандал, судові позови, загроза існуванню бренду

Рівень ризику (Risk Level, RL) розраховується за формулою:

$$\text{Risk Level (RL)} = \text{Likelihood (L)} \times \text{Impact (I)}$$

Risk Level	Зона ризику	Дії
1 – 4	Прийнятна (зелена)	Стандартний моніторинг без активних заходів
5 – 9	Помірна (жовта)	Розробка плану реагування, підготовка шаблонів відповідей
10 – 14	Висока (помаранчева)	Активне управління, превентивні комунікаційні заходи
15 – 25	Критична (червона)	Негайне усунення ризику або розробка детального антикризового плану

Приклад побудови матриці для бренду «Укрзалізниця»

Наведемо умовний навчальний приклад побудови матриці репутаційних ризиків для «Укрзалізниці».

Риск	L (1–5)	I (1–5)	RL = L×I	Зона
Масові скарги на затримки потягів у соцмережах	5	3	15	Критична
Витік персональних даних пасажирів	2	5	10	Висока
Публічний конфлікт між пасажиром і провідником (відео)	4	4	16	Критична

Фейкові новини про скасування маршрутів	4	3	12	Висока
Критичні публікації відомого інфлюєнсера	3	4	12	Висока
Порівняльна кампанія від конкурентів (автобусні лінії)	3	2	6	Помірна
Незначні скарги на якість харчування у вагонах-ресторанах	4	1	4	Прийнятна

Інтерпретація матриці: два ризики потрапляють у критичну зону (RL = 15–16) - масові скарги на затримки та відео-конфлікти. Саме вони вимагають пріоритетної уваги та детально розроблених антикризових протоколів. Три ризики знаходяться у високій зоні та потребують активного управління. Сукупна картина дозволяє менеджменту правильно розподілити ресурси і не витратити зусилля на управління малоімовірними або малозначущими ризиками.

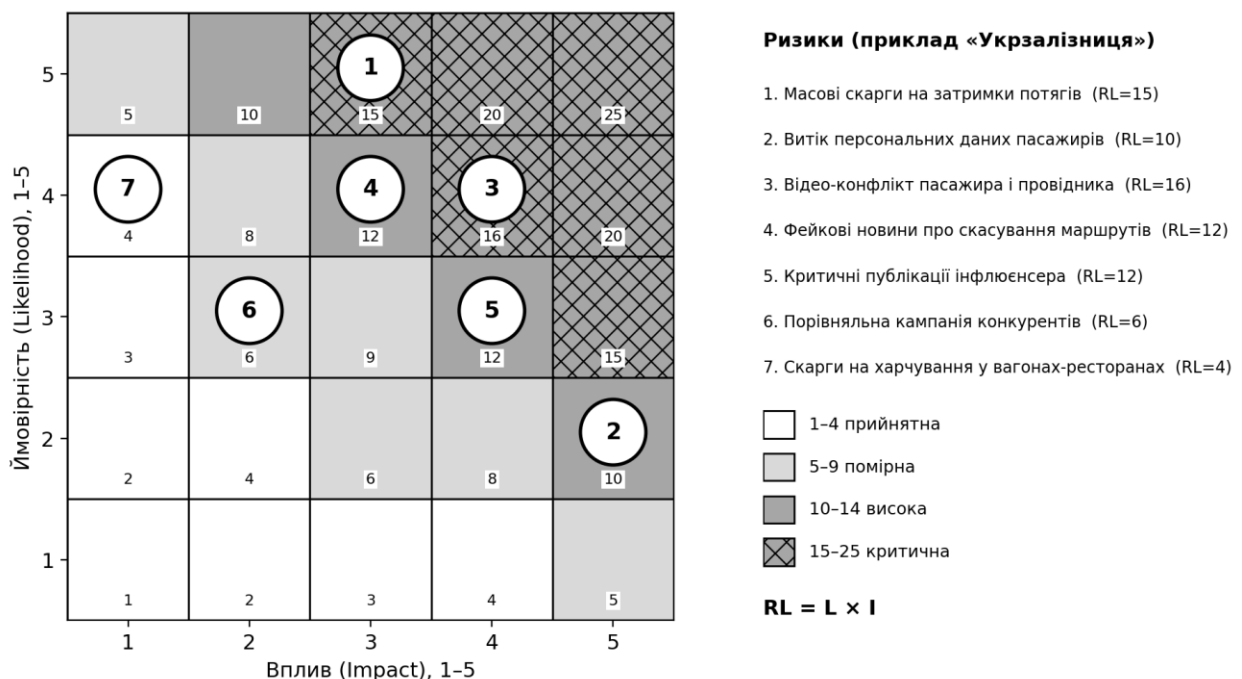


Рис. 3.1. Матриця репутаційних ризиків (RRM) на прикладі бренду «Укрзалізниця»

МЕТОДИКА 5. SENTIMENT TREND ANALYSIS (STA) - АНАЛІЗ ДИНАМІКИ ТОНАЛЬНОСТІ

Логіка та призначення методики

Sentiment Trend Analysis (STA) - це методика аналізу зміни NSS у часі. Якщо NSS показує статичну «фотографію» репутаційного стану на певний момент, то STA надає «відеозапис» - динаміку змін, яка дозволяє виявити тенденції погіршення задовго до того, як ситуація стане кризовою.

Ключова цінність STA полягає у виявленні передкризових сигналів. Репутаційна криза рідко виникає раптово: як правило, їй передують поступове погіршення тональності протягом кількох тижнів чи місяців. Якщо аналітик відстежує динаміку NSS регулярно (щотижня або щомісяця), він може помітити цю тенденцію заздалегідь і ініціювати превентивні заходи.

Крім самого значення NSS у кожному часовому інтервалі, STA розраховує показник ΔNSS - швидкість зміни тренду за одиницю часу (зазвичай тиждень або місяць). Різке падіння ΔNSS є тривожним сигналом, що вимагає негайної уваги.

Алгоритм проведення аналізу

1. Розбити зібрані публікації на рівні часові інтервали (тижні або місяці залежно від загального обсягу вибірки та досліджуваного періоду).
2. Для кожного інтервалу підрахувати кількість позитивних (P), нейтральних та негативних (N) публікацій, а також загальну кількість (T).
3. Розрахувати NSS для кожного інтервалу за формулою Методики 1.
4. Розрахувати ΔNSS для кожного наступного інтервалу: $\Delta NSS = NSS(\text{поточний}) - NSS(\text{попередній})$.
5. Визначити загальний тренд: позитивний (NSS зростає), негативний (NSS знижується) або нейтральний (коливається без явного напрямку).
6. Якщо $\Delta NSS < -10\%$ за один тижневий інтервал - ситуація потребує посиленої уваги. Якщо $\Delta NSS < -20\%$ - негайна реакція.

Приклад розрахунку та інтерпретація

Розглянемо приклад для інтернет-магазину «Rozetka». Аналітик зібрав публікації за чотири тижні поспіль і отримав такі дані:

Тиждень	Позитив (P)	Нейтрал	Негатив (N)	Всього (T)	NSS (%)	Δ NSS
Тиждень 1	14	6	5	25	+36,0%	-
Тиждень 2	12	5	8	25	+16,0%	-20,0%
Тиждень 3	9	4	12	25	-12,0%	-28,0%
Тиждень 4	6	3	16	25	-40,0%	-28,0%

Інтерпретація результатів. За чотири тижні NSS знизився від +36,0% (добрий стан) до -40,0% (критичний стан). Перший тривожний сигнал з'явився на другому тижні: Δ NSS = -20,0%, що перевищило порогове значення -10% і мало б ініціювати посилений моніторинг та аналіз причин. На третьому тижні Δ NSS = -28,0% (критичне значення), і NSS перейшов у негативну зону - це був останній момент для превентивного антикризового реагування. На четвертому тижні стан вже є критичним: частка негативних публікацій (64%) значно перевищує позитивні (24%).

Практичний висновок: якби аналітик виявив стрімке падіння Δ NSS на другому тижні, компанія мала б у запасі мінімум один-два тижні для діагностики причин і підготовки комунікаційної відповіді. Реактивне реагування на четвертому тижні вже потребуватиме значно більших ресурсів.

МЕТОДИКА 6. CHANNEL RISK DISTRIBUTION (CRD) - РОЗПОДІЛ РИСКУ ЗА КАНАЛАМИ

Логіка та призначення методики

Channel Risk Distribution (CRD) вирішує стратегічне питання розподілу ресурсів моніторингу: де саме зосередити аналітичні зусилля? Різні платформи мають принципово різні характеристики поширення контенту: те, що «вибухає» в TikTok, може залишатися майже непоміченим у LinkedIn, і навпаки.

Методика складається з двох взаємодоповнюючих розрахунків. Перший - CRD - визначає частку негативних згадок на кожній платформі від їхньої загальної кількості. Це показник кількісного внеску платформи в репутаційний ризик. Другий - середній показник залученості негативних публікацій (Avg_E) на

кожній платформі - відображає, наскільки «гучним» є негатив на конкретному каналі.

Поєднання двох показників дозволяє виявити не лише «де найбільше негативу», а й «де негатив найнебезпечніший». Платформа з невеликою кількістю негативних публікацій, але з надзвичайно високим Avg_E, може становити більшу загрозу, ніж платформа з великою кількістю малопомітних скарг.

Формули розрахунку

Частка негативних згадок по каналу:

$$\text{CRD(канал)} = (\text{Кількість негативних згадок на каналі} / \text{Загальна кількість негативних згадок}) \times 100\%$$

Середня залученість негативного контенту на каналі:

$$\text{Avg_E(канал)} = \Sigma \text{Engagement негативних публікацій на каналі} / \text{Кількість негативних публікацій на каналі}$$

Приклад розрахунку та інтерпретація

Розглянемо приклад для телеком-оператора «Vodafone Україна». Аналітик зібрав 55 негативних публікацій за місяць і розподілив їх за платформами:

Платформа	Негатив. згадок	CRD (%)	Σ Engagement	Avg_E	Пріоритет
Facebook	22	40,0%	18 500	841	Високий
Telegram	16	29,1%	24 800	1 550	Дуже висок.
Instagram	7	12,7%	5 600	800	Середній
TikTok	4	7,3%	86 000	21 500	Критичний
Twitter/X	4	7,3%	2 200	550	Низький
Google Reviews	2	3,6%	0	0	Мінімальний

Аналіз результатів демонструє парадоксальну ситуацію. Facebook є лідером за кількістю негативних публікацій (40% від усього негативу), однак за реальним впливом це не найнебезпечніша платформа. TikTok, де знаходиться лише 7,3% негативних публікацій, має Avg_E = 21 500, що у 25,6 рази перевищує показник Facebook. Це означає, що кожен негативний допис у TikTok охоплює аудиторію, порівнянну з 25 публікаціями у Facebook.

Практичний висновок: розподіл ресурсів моніторингу має бути не пропорційним кількості публікацій, а зваженим за реальним впливом. Рекомендується виділяти окремого спеціаліста для моніторингу TikTok та Telegram, незважаючи на їхню нижчу кількісну присутність.

КОМПЛЕКСНЕ ЗАСТОСУВАННЯ МЕТОДИК ТА ВЗАЄМОЗВ'ЯЗОК МІЖ НИМИ

Обмеження окремих методик та синергетичний ефект їх комбінування

Жодна з шести розглянутих методик не є універсальним інструментом, достатнім для повноцінної оцінки репутаційних ризиків. Кожна з них вирішує певну аналітичну задачу, але має власні обмеження. NSS простий і швидкий у розрахунку, але ігнорує вагу публікацій. WRI усуває цей недолік, але не дає прогнозу. CPS є прогностичним, але не описує поточний стан. RRM охоплює весь портфель ризиків, але є статичним. STA відображає динаміку, але не враховує залученість. CRD розкриває каналну специфіку, але не інтегрує часовий вимір.

Ефективна система ризик-моніторингу використовує всі методики в комплексі, де кожна доповнює інші. Нижче наведено рекомендовану послідовність застосування методик як частини щотижневого або щомісячного аналітичного циклу.

Рекомендований аналітичний цикл

Крок	Методика	Що дає на цьому кроці
1	CRD	Визначити, на яких платформах сконцентрований негатив. Встановити пріоритети збору даних.

2	NSS	Отримати базовий «знімок» поточного репутаційного стану. Швидка первинна діагностика.
3	WRI	Уточнити реальну картину з урахуванням залученості. Порівняти з NSS - виявити потенційно вірусний негатив.
4	CPS	Оцінити ймовірність переростання ситуації у кризу. Визначити рівень тривоги для PR-команди.
5	STA	Порівняти поточний NSS з попередніми періодами. Виявити тренд та передкризові сигнали.
6	RRM	Оновити матрицю ризиків з урахуванням нових даних. Переглянути пріоритети управлінської уваги.

Кейс комплексного застосування: телекомунікаційна компанія під час масового збою мережі

Уявімо таку ситуацію: у неділю, 13:00, у регіональній мережі мобільного оператора стався масовий збій. Сотні тисяч абонентів втратили зв'язок на 3 години. Розглянемо, як всі шість методик працюють у комплексі для управління ситуацією.

Крок 1 (CRD). Первинний аналіз показує: 52% негативного контенту сформовано у Twitter/X (Avg_E = 2 400), 28% - у Telegram (Avg_E = 3 100), 20% - у Facebook (Avg_E = 680). Висновок: зусилля реагування слід сконцентрувати у Twitter/X та Telegram.

Крок 2 (NSS). Зі 120 зібраних публікацій за останню годину: 8 позитивних, 14 нейтральних, 98 негативних. $NSS = ((8-98)/120) \times 100\% = -75\%$. Катастрофічний стан.

Крок 3 (WRI). З урахуванням залученості $WRI = -88,4\%$, що підтверджує катастрофічний стан і вказує на надзвичайно широке охоплення негативного контенту.

Крок 4 (CPS). CV = 450 негативних згадок за останню годину (CV = 45); $NSS_{neg} = 81,7 (98/120 \times 100)$; IR = 35 (7 акаунтів 10K+ з 20 негативних); MR = 100 (головні телеканали вже повідомляють про збій). $CPS = (45 \times 0,35) + (81,7 \times 0,30) + (35 \times 0,20) + (100 \times 0,15) = 15,75 + 24,51 + 7 + 15 = 62,3$. Рівень загрози: Високий - криза активно розгортається.

Кроки 5–6 (STA та RRM). STA підтверджує стрімке падіння Δ NSS порівняно з попереднім тижнем. RRM фіксує, що ризик «масового технічного збою» переходить із зони «Висока» у зону «Критична».

Комплексний висновок: системний аналіз усіх методик вимагає негайного публічного визнання проблеми від офіційного акаунту компанії у Twitter/X і Telegram (де сконцентовано найбільш вірусний негатив), повідомлення про причини збою і очікуваний час відновлення, а також готовності CEO до публічного коментаря для медіа. Стратегія мовчання чи затримки у цьому випадку є неприйнятною.

ВИСНОВКИ

Лекція ознайомила з шістьма ключовими методиками кількісної оцінки репутаційних ризиків у соціальних мережах, кожна з яких відповідає на власне аналітичне запитання. Net Sentiment Score надає базовий «знімок» тональності. Weighted Reputation Index коригує його з урахуванням реального охоплення публікацій. Crisis Probability Score дозволяє прогнозувати ймовірність розгортання кризи. Reputation Risk Matrix систематизує весь портфель ризиків організації. Sentiment Trend Analysis виявляє передкризові тенденції у динаміці. Channel Risk Distribution визначає найнебезпечніші платформи для концентрації моніторингових зусиль.

Важливим висновком є те, що жодна методика не є достатньою сама по собі. NSS може демонструвати «нейтральний стан», тоді як WRI одночасно фіксує «катастрофічний» через один вірусний негативний допис - і обидва результати є правильними у своєму контексті. CRD може показати, що 80% негативу зосереджено у Facebook, однак TikTok з 5% негативних публікацій може становити більшу реальну загрозу через на порядки вищий показник залученості. Саме такі несподівані розбіжності між методиками є найціннішими аналітичними знахідками.

Розрахунки метрик є не самоціллю, а інструментом обґрунтування управлінських рішень. Цифри мають сенс лише тоді, коли вони правильно інтерпретуються і транслуються у конкретні дії: зміну комунікаційної стратегії,

перерозподіл ресурсів моніторингу, активацію антикризових протоколів або превентивні заходи з управління ризиками.

Фахівець зі спеціальності «Комп'ютерні науки (Консолідована інформація)» повинен опанувати як математичний апарат цих методик, так і управлінський контекст їхнього застосування. Технічна точність розрахунків і здатність зрозуміло донести їхнє значення до команди та керівництва є рівнозначно важливими компетентностями.

КОНТРОЛЬНІ ПИТАННЯ

1. Чому NSS та WRI для однієї і тієї самої вибірки публікацій можуть давати принципово різні висновки? Наведіть конкретний числовий приклад, що демонструє цю ситуацію.
2. Поясніть логіку нормування компонента CV у формулі CPS. Чому саме значення 1 000 згадок/год прийнято за верхню межу шкали?
3. Що таке Risk Level у матриці репутаційних ризиків? Поясніть, чому ризик з $L=5$, $I=2$ може потребувати більш термінового реагування, ніж ризик з $L=2$, $I=4$, попри однаковий $RL=10$.
4. Аналітик отримав такий ряд NSS за 5 тижнів: +42%, +38%, +19%, -8%, -25%. Розрахуйте ΔNSS для кожного тижня та визначте, на якому тижні мали б бути активовані антикризові заходи і чому.
5. Компанія фіксує: у Facebook 60% всіх негативних публікацій ($Avg_E = 200$), у TikTok - 10% ($Avg_E = 18\,000$). Розрахуйте сумарний Engagement негативного контенту на кожній платформі (за умови 50 негативних публікацій загалом) та поясніть, яка платформа є пріоритетною для реагування і чому.
6. Чому аналітичний цикл рекомендується розпочинати з CRD, а не з NSS? Яку управлінську перевагу дає такий порядок?
7. Порівняйте методики NSS та CPS: яку аналітичну задачу вирішує кожна? Чи можливе таке поєднання: $NSS = +40\%$ і $CPS = 75$? Якщо так - за яких умов?

Література

1. VADER Sentiment Analysis: <https://github.com/cjhutto/vaderSentiment>
2. Brandwatch Consumer Research:
<https://www.brandwatch.com/blog/reputation-management/>
3. DataReportal Global Digital Reports: <https://datareportal.com>

ЛЕКЦІЯ 4. МЕРЕЖНИЙ АНАЛІЗ У РИСК-МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ

ВСТУП

Соціальні мережі сьогодні є не лише майданчиком для спілкування, вони стали складними інформаційними системами, де щосекунди формуються, трансформуються та поширюються мільйони одиниць контенту. За даними дослідження компанії DataReportal (2024), щомісяця у світі активно використовують соціальні мережі понад 5 мільярдів людей. Це означає, що будь-яка подія – запуск нового продукту, скандал навколо бренду, політична заява чи навіть чутка – може в лічені години охопити мільйони людей і спричинити непередбачувані наслідки.

Студенти спеціальності 122 «Комп'ютерні науки» – це майбутні інженери-розробники, аналітики даних та архітектори інформаційних систем. Їхня роль у сучасних організаціях не обмежується написанням коду: вони проєктують системи, які автоматично відстежують, аналізують і реагують на процеси в цифровому просторі. Риск-моніторинг соціальних мереж є саме таким завданням технічно складним, соціально важливим і комерційно затребуваним.

Мережний аналіз (Network Analysis) – це один з ключових інструментів у цій галузі. Він дозволяє не просто читати публікації та підраховувати кількість згадок бренду, а розуміти структуру інформаційних потоків: хто є реальним центром впливу, як саме поширюється контент, де зосереджені найбільш активні спільноти та які зв'язки між ними існують. Це знання має безпосередню практичну цінність.

Розглянемо конкретну ситуацію. Уявіть, що ви розробник системи риск-моніторингу для великої української ритейлера (наприклад, Rozetka або Comfy). Негативна публікація з'являється у Facebook: незадоволений клієнт скаржиться на неякісний товар. Без мережного аналізу ви бачите лише один пост з певною кількістю лайків. Але якщо застосувати інструменти аналізу мереж, картина докорінно змінюється: ви можете побачити, що цей конкретний користувач має 50 000 підписників і є ключовим вузлом у спільноті споживчих правозахисників, що його публікація вже ретвітнута трьома журналістами з охопленням по 100 000 людей кожен, і що в мережі сформувалася координована

група з 40 акаунтів, які активно поширюють цей контент. Таке розуміння дозволяє вчасно ескалювати ситуацію та запобігти репутаційній кризі.

Саме тому мережний аналіз займає центральне місце в дисципліні «Риск-моніторинг у соціальних мережах». Він є точкою перетину математики (теорія графів), програмування (Python, алгоритми на графах), соціології (структура спільнот) та прикладної аналітики (підтримка управлінських рішень).

ПЛАН ЛЕКЦІЇ

1. Мережний аналіз (Network Analysis)
2. Основні поняття теорії графів для аналізу соціальних мереж
3. Метрики центральності та їх практичне значення
4. Виявлення спільнот (Community Detection)
5. Реалізація мережного аналізу в Python: NetworkX
6. Інструменти візуалізації мереж
7. Виявлення ботів та координованих мереж
8. Реальні кейси застосування мережного аналізу

Де саме використовується мережний аналіз: конкретні сфери застосування Корпоративний ризик-моніторинг і репутаційний менеджмент

Найочевидніша і найпоширеніша сфера застосування моніторинг репутації брендів та компаній. Компанії по всьому світу витрачають значні ресурси на відстеження того, що про них говорять у соціальних мережах. Але просте підрахування кількості згадок це лише перший крок. Значно важливіше розуміти структуру цих розмов.

Практичний приклад: у листопаді 2021 року українська авіакомпанія отримала хвилю негативу у Twitter після масового скасування рейсів через погодні умови. Служба моніторингу компанії зафіксувала стрибок негативних згадок, але завдяки мережному аналізу вдалося виявити додаткову критичну деталь: серед авторів негативних публікацій був акаунт відомого туристичного блогера з аудиторією 300 000 підписників, який, крім того, мав численні зв'язки з іншими туристичними лідерами думок. Саме цей вузол мережі ставав «підсилювачем» негативу. Компанія оперативно зв'язалася з блогером, вирішила

його особисту проблему і він опублікував позитивне оновлення що миттєво змінило настрої у мережі.

Аналогічний підхід використовують провідні платформи управління репутацією: Brandwatch, Mention, Sprout Social, YouScan (українська платформа). Всі вони інтегрують елементи мережного аналізу для ідентифікації ключових акаунтів впливу.

Виявлення дезінформації та координованих маніпулятивних кампаній

Дезінформація є однією з найсерйозніших загроз інформаційної безпеки сучасності. В умовах збройного конфлікту в Україні ця проблема набуває особливої гостроти. Мережний аналіз є одним з ключових інструментів виявлення скоординованих кампаній з поширення фейків.

Принцип виявлення наступний: якщо група акаунтів публікує однаковий або дуже схожий контент у короткий проміжок часу, поводить ся аномально синхронно (наприклад, всі одночасно ретвітять одне й те саме), або якщо в мережі поширення контенту виявляються незвично щільні кластери нових акаунтів це ознаки координованої неавтентичної поведінки (Coordinated Inauthentic Behavior, CIB). Саме такі патерни виявляє мережний аналіз.

Конкретний приклад: дослідницька організація EU DisinfoLab у 2023 році виявила мережу з понад 180 підроблених новинних сайтів та акаунтів у соціальних мережах, які координовано поширювали антиукраїнські наративи в Європі. Виявлення цієї мережі стало можливим саме завдяки аналізу структури зв'язків між акаунтами та патернів поширення контенту тобто через мережний аналіз.

Центр протидії дезінформації при РНБО України також використовує подібні методи для моніторингу інформаційних операцій проти України.

Аналіз виборчих кампаній та політичних комунікацій

Під час виборів соціальні мережі стають полем битви за суспільну думку. Мережний аналіз дозволяє штабам кандидатів, журналістам та незалежним дослідникам розуміти структуру підтримки та опозиції в цифровому просторі.

Під час виборчих кампаній у Верховну Раду в Україні аналітики відстежують мережі підтримки різних партій у Facebook та Telegram. Алгоритми виявлення спільнот (Community Detection) дозволяють ідентифікувати, які групи населення підтримують ту чи іншу силу, якими є зв'язки між різними ідеологічними спільнотами, де є можливості для переконання «коливних» виборців. Це інформація, яка безпосередньо впливає на стратегію кампанії.

Академічні дослідники також активно вивчають ці процеси. Дослідники Стенфордського інституту Інтернету (Stanford Internet Observatory) у 2023 році опублікували дослідження, в якому за допомогою мережного аналізу виявили понад 70 000 акаунтів з аномальною поведінкою під час виборів у різних країнах.

Кризовий менеджмент у реальному часі

Кризова комунікація це ще одна галузь, де мережний аналіз має безпосереднє прикладне значення. Коли компанія опиняється в центрі скандалу, першочерговим завданням антикризового менеджера є розуміння динаміки кризи: звідки вона почалася, хто її підсилює, куди вона поширюється.

Показовим є кейс H&M 2018 року. Після публікації рекламної кампанії, яка була сприйнята як расистська, у соціальних мережах спалахнув потужний скандал. Ретроспективний аналіз показав: мережа поширення негативу мала чітку структуру кілька ключових акаунтів з великою аудиторією були «мостами» між різними спільнотами (BLM-активісти, fashion-блогери, споживчі захисники). Якби компанія мала систему моніторингу на основі мережного аналізу, вона могла б ідентифікувати цих ключових вузлів на ранній стадії і вибудувати цільову комунікацію саме з ними.

Кібербезпека та захист від соціальної інженерії

Мережний аналіз використовується також у сфері кібербезпеки зокрема, для виявлення фішингових мереж та кампаній соціальної інженерії. Шахраї та кіберзлочинці часто будують мережі підроблених акаунтів для поширення шкідливих посилань або формування хибної довіри.

Служби безпеки банків та фінансових установ в Україні (зокрема, Приватбанк, monobank) активно моніторять соціальні мережі на предмет

підроблених акаунтів, що видають себе за офіційні сторінки банку. Мережний аналіз допомагає виявляти координовані групи таких акаунтів, які часто мають характерну структуру взаємних зв'язків.

Маркетинг та аналіз споживчої поведінки

З позитивного боку, мережний аналіз є потужним інструментом маркетингу впливу (influencer marketing). Розуміння структури мережі дозволяє ідентифікувати не лише найбільших за кількістю підписників блогерів, а й тих, хто є реальним авторитетом у конкретній спільноті – так звані мікроінфлюенсери з лояльною аудиторією.

Наприклад, для просування нової лінійки косметики в Україні компанія може провести мережний аналіз beauty-спільноти в Instagram та TikTok, щоб виявити не просто акаунти з найбільшою аудиторією, а тих, чії публікації найактивніше поширюються всередині цільової спільноти (висока betweenness centrality). Такий підхід значно ефективніший і часто дешевший, ніж просто закупівля реклами у «зіркових» блогерів.

Компетентності, які формує вивчення мережного аналізу

Вивчення мережного аналізу в контексті дисципліни «Риск-моніторинг у соціальних мережах» формує у студентів спеціальності 122 комплекс взаємопов'язаних компетентностей.

Математичні компетентності: студенти опановують теорію графів на прикладному рівні розуміють, що таке вузли (nodes) та ребра (edges), навчаються рахувати метрики центральності, розуміють принципи алгоритмів пошуку спільнот. Це не абстрактна математика – це математика, яка безпосередньо застосовується для вирішення реальних задач аналізу соціальних мереж.

Програмувальні компетентності: студенти навчаються працювати з провідними Python-бібліотеками для роботи з графами (NetworkX, igraph), опановують методи імпорту та обробки реальних даних про соціальні зв'язки, вчать будувати аналітичні пайплайни від збору даних до отримання інсайтів.

Аналітичні компетентності: важлива навичка інтерпретація результатів мережного аналізу. Виявити, що певний вузол має PageRank 0.0045, це технічне завдання. Але зрозуміти, що це означає в контексті репутаційного ризику для компанії, і запропонувати конкретну дію це аналітична компетентність, яка відрізняє хорошого фахівця від посереднього.

Міждисциплінарне мислення: мережний аналіз вимагає розуміти соціальний контекст даних. Студенти вчаться поєднувати технічний аналіз з розумінням соціальних процесів, що відображаються в структурі мереж.

МЕРЕЖНИЙ АНАЛІЗ (NETWORK ANALYSIS)

Основні поняття теорії графів для аналізу соціальних мереж

Перш ніж переходити до практичних інструментів, необхідно розібратися з математичним фундаментом мережного аналізу. Теорія графів це розділ математики, що вивчає об'єкти, які складаються з вузлів (vertices або nodes) та ребер (edges) між ними. Соціальна мережа в математичному розумінні є саме графом: кожен акаунт це вузол, а зв'язки між акаунтами (підписки, ретвіти, відповіді, лайки) це ребра.

Для роботи зі соціальними мережами ключовим є поняття орієнтованого графа (directed graph, digraph). На відміну від неорієнтованого графа, де ребра двосторонні (якщо А пов'язаний з Б, то й Б пов'язаний з А), в орієнтованому графі ребра мають напрям. Це критично важливо для аналізу соціальних мереж: якщо користувач А підписаний на користувача Б, це не означає, що Б підписаний на А. Ретвіт також є спрямованою дією: А ретвітнув Б це конкретний напрям потоку інформації.

Зважений граф (weighted graph) додає ще один вимір: кожне ребро має числову вагу. У контексті аналізу соціальних мереж вагою ребра може бути кількість взаємодій між двома акаунтами, частота ретвітів, кількість спільних публікацій або будь-яка інша метрика інтенсивності зв'язку. Зважені графи дозволяють розрізняти «слабкі» та «сильні» зв'язки в мережі.

Ще одне важливе поняття дводольний граф (bipartite graph). У дослідженнях соціальних мереж дводольні графи використовуються, коли є два типи вузлів, і зв'язки існують лише між вузлами різних типів. Наприклад:

акаунти користувачів та хештеги якщо акаунт А публікує хештег #Rozetka, між ними виникає ребро. Аналіз таких структур дозволяє виявляти тематичні кластери та ком'юніті.

Для роботи з реальними мережевими даними важливо розуміти кілька базових структурних властивостей графів. Щільність мережі (network density) показує, яка частка можливих зв'язків між вузлами реально існує. У соціальних мережах щільність, як правило, дуже низька більшість користувачів не пов'язані один з одним безпосередньо. Діаметр мережі (network diameter) це максимальна відстань між будь-якими двома вузлами, тобто найдовший найкоротший шлях. Відомий феномен «шести рукостискань» (six degrees of separation) саме про це: у більшості соціальних мереж діаметр відносно невеликий попри величезну кількість вузлів. Компонента зв'язності (connected component) це підграф, всередині якого існує шлях між будь-якими двома вузлами. В аналізі соціальних мереж зазвичай є одна велика компонента (giant component) та безліч дрібних ізольованих кластерів.

Поняття	Визначення	Приклад у соціальній мережі
Вузол (Node)	Окремий елемент мережі	Акаунт користувача, сторінка бренду
Ребро (Edge)	Зв'язок між двома вузлами	Підписка, ретвіт, відповідь на коментар
Орієнтований граф	Ребра мають напрям	А підписаний на Б (але не навпаки)
Зважений граф	Ребра мають числову вагу	Кількість взаємодій між двома акаунтами
Щільність мережі	Частка реалізованих зв'язків від можливих	0.001–0.05 для великих соціальних мереж
Giant Component	Найбільший зв'язний підграф	Основна маса активних користувачів

Метрики центральності та їх практичне значення

Центральність (centrality) це клас метрик, що вимірюють «важливість» або «впливовість» вузла в мережі. Різні метрики центральності вимірюють різні аспекти важливості і дають різну інформацію для аналізу ризиків. Розуміння відмінностей між ними є критично важливим для правильної інтерпретації результатів.

Degree Centrality (ступінь центральності)

Найпростіша метрика: кількість прямих зв'язків вузла, нормована на максимально можливу кількість зв'язків. Для орієнтованих графів розрізняють in-degree (кількість вхідних зв'язків) та out-degree (кількість вихідних зв'язків).

Практичне застосування: high in-degree акаунт, на який часто посилаються або якого ретвітять це потенційний лідер думок. High out-degree акаунт, який сам активно поширює контент може бути ботом або «підсилювачем». Аномально висок out-degree у поєднанні з низьким in-degree є класичною ознакою бот-акаунту: він активно поширює контент, але майже ніхто не відповідає йому у відповідь.

Конкретний приклад: під час аналізу мережі поширення фейку про «обстріл дитячої лікарні» (вигаданий приклад) аналітики виявляють акаунт з out-degree = 850 за 24 години. Це означає, що один акаунт зробив 850 ретвітів або публікацій за один день що технічно неможливо для живої людини і свідчить про автоматизовану поведінку.

Betweenness Centrality (посередницька центральність)

Betweenness centrality вимірює, наскільки часто певний вузол знаходиться на найкоротшому шляху між іншими парами вузлів у мережі. Формально: це частка найкоротших шляхів між усіма парами вузлів, що проходять через даний вузол.

Практичне значення цієї метрики надзвичайно велике для риск-моніторингу. Вузол з високою betweenness centrality є «мостом» або «воротарем» між різними частинами мережі. Він контролює потік інформації між спільнотами. Якщо такий вузол починає поширювати негативну інформацію про бренд ця інформація може дуже швидко перетекти з однієї спільноти в іншу.

Показовий приклад із практики: у дослідженні мережі поширення скандалу навколо United Airlines після інциденту з пасажиром у 2017 році було встановлено, що три акаунти мали betweenness centrality у 8–12 разів вищу за середній показник. Саме ці акаунти були «містками» між авіаційною

спільнотою, активістами споживчих прав та загальноновинними акаунтами. Без них криза навряд чи вийшла б за межі авіаційних форумів.

PageRank

PageRank алгоритм, спочатку розроблений засновниками Google Ларрі Пейджем та Сергієм Бріном для ранжування веб-сторінок. Його основна ідея: важливість вузла визначається не просто кількістю посилань на нього, а якістю цих посилань. Якщо на вузол А посилається вузол Б з дуже високим PageRank це дає вузлу А більше «авторитету», ніж якби на нього посилалися сто маловідомих вузлів.

В аналізі соціальних мереж PageRank це найточніша метрика реального впливу акаунту. Вона не піддається легкій маніпуляції (на відміну від кількості підписників, яку можна накрутити), оскільки враховує якість зв'язків. Акаунт з 10 000 підписників, серед яких є 50 відомих журналістів та лідерів думок, матиме значно вищий PageRank, ніж акаунт з 100 000 підписників-ботів.

Closeness Centrality (близькість)

Closeness centrality це обернена величина до середньої відстані від даного вузла до всіх інших вузлів у мережі. Вузол з високою closeness centrality може «дотягнутися» до всіх інших вузлів за мінімальну кількість кроків.

Практичне значення: closeness centrality показує, наскільки швидко вузол може поширити інформацію по всій мережі. Акаунт з високою closeness centrality це ідеальний «посланець»: будь-яка інформація, яку він публікує, дуже швидко досягає всіх куточків мережі. Для риск-моніторингу це означає, що такі акаунти потребують особливої уваги: негативний контент від них поширюється максимально ефективно.

Метрика	Що вимірює	Практичне застосування в риск-моніторингу
Degree Centrality	Кількість прямих зв'язків	Виявлення активних акаунтів; висок out-degree = підозра на бот

Метрика	Що вимірює	Практичне застосування в ризик-моніторингу
In-degree	Кількість вхідних зв'язків	Ідентифікація лідерів думок та популярних акаунтів
Out-degree	Кількість вихідних зв'язків	Виявлення «підсилювачів» та потенційних ботів
Betweenness Centrality	Частка шляхів, що проходять через вузол	Знаходження «мостів» між спільнотами ключових посередників
PageRank	Авторитетність за якістю зв'язків	Точна оцінка реального впливу акаунту
Closeness Centrality	Швидкість досягнення всіх вузлів	Виявлення акаунтів, які найшвидше поширюють інформацію
Clustering Coefficient	Щільність зв'язків між сусідами вузла	Виявлення тісно згуртованих груп, координуваних акаунтів

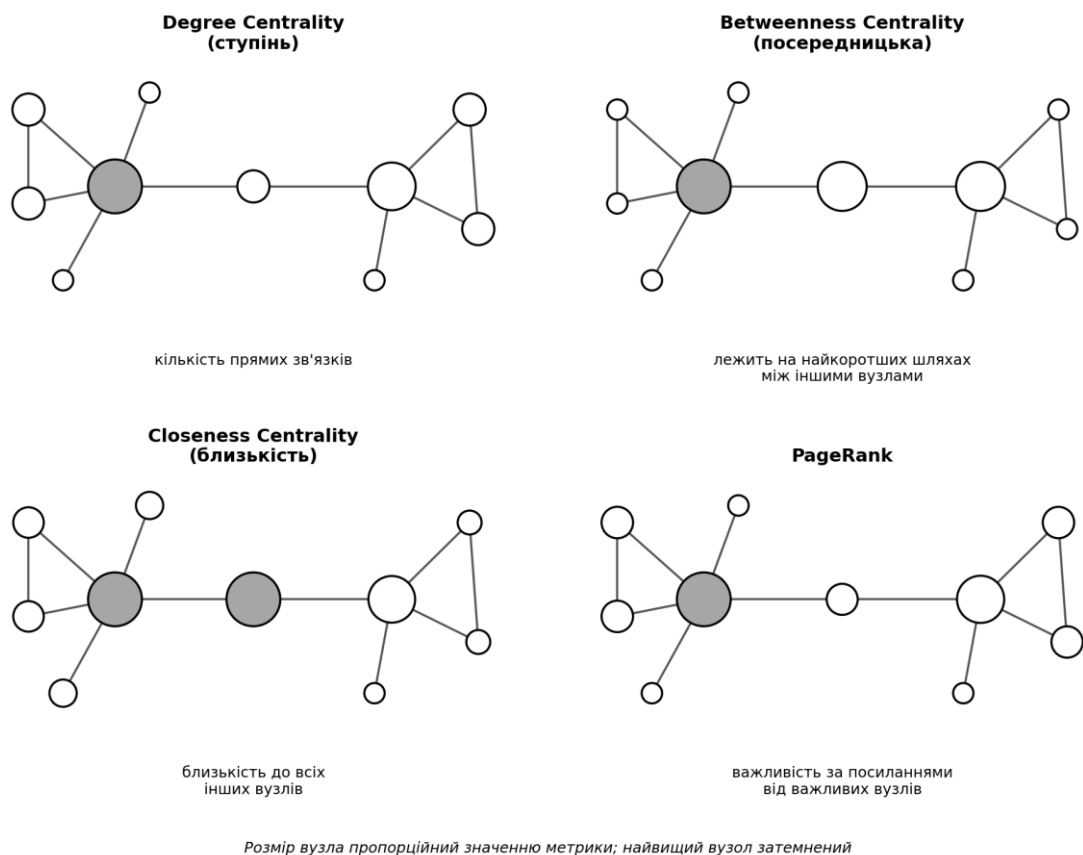


Рис. 4.1. Метрики центральності на одному й тому самому графі

Виявлення спільнот (Community Detection)

Community Detection це одна з найважливіших задач мережного аналізу. Вона полягає в автоматичному виявленні груп (кластерів, спільнот) вузлів, які мають більше зв'язків між собою, ніж з рештою мережі. Інтуїтивно: це ті групи людей у соціальній мережі, які «спілкуються» переважно між собою.

Для оцінки якості виявлених спільнот використовується метрика модульності (modularity), яка вимірює, наскільки виявлені кластери відрізняються від випадкового розподілу зв'язків. Значення модульності від 0.3 до 0.7 вважається хорошим результатом для реальних соціальних мереж.

Алгоритм Louvain

Алгоритм Louvain (Blondel et al., 2008) є найпопулярнішим алгоритмом виявлення спільнот для великих мереж. Він оптимізує модульність за допомогою жадібного підходу: спочатку кожен вузол є окремою спільнотою, потім ітеративно об'єднуються вузли, об'єднання яких максимально збільшує модульність.

Головна перевага алгоритму Louvain його швидкість: часова складність $O(n \log n)$, що дозволяє обробляти мережі з мільйонами вузлів. Саме тому він є стандартним інструментом для аналізу великих соціальних мереж.

Практичний приклад застосування: уявімо, що ми аналізуємо мережу з 500 000 акаунтів, які публікували контент з хештегом #Ukraine протягом тижня. Алгоритм Louvain виявляє в цій мережі 12 основних спільнот. Подальший аналіз показує: спільнота 1 переважно українськомовні акаунти, що поширюють офіційні новини; спільнота 2 міжнародні медіа та журналісти; спільнота 3 проросійські акаунти з аномальною поведінкою; спільнота 4–7 географічно зосереджені групи (польська, британська, американська діаспора). Кожна з цих спільнот вимагає окремої стратегії комунікації.

Алгоритм Girvan-Newman

Алгоритм Girvan-Newman використовує інший підхід: він ітеративно видаляє ребра з найвищою betweenness centrality. Логіка така: ребра, що з'єднують різні спільноти, мають вищу betweenness centrality, ніж ребра всередині спільнот. Видаляючи їх послідовно, алгоритм «розрізає» мережу на все дрібніші кластери.

Недолік алгоритму висока обчислювальна складність ($O(n^3)$ для ненаправлених графів), що робить його непридатним для великих мереж. Проте

для малих і середніх мереж (до 10 000 вузлів) він дає якісні та добре інтерпретовані результати з чіткою ієрархічною структурою спільнот.

Label Propagation та Infomap

Алгоритм Label Propagation (поширення міток) є найшвидшим алгоритмом виявлення спільнот з лінійною складністю $O(n)$. Він працює так: кожному вузлу присвоюється мітка (ідентифікатор спільноти), а потім кожен вузол ітеративно приймає мітку, що є найпоширенішою серед його сусідів. Алгоритм швидкий, але дає нестабільні результати різні запуски можуть давати різні спільноти.

Infomap алгоритм, що базується на мінімізації довжини опису потоків інформації в мережі (принцип мінімальної довжини опису, MDL). Він особливо підходить для аналізу спрямованих графів і добре відображає реальні потоки інформації в соціальних мережах. Дослідники часто використовують Infomap для аналізу мереж поширення контенту (ретвіти, репости).

Алгоритм	Складність	Оптимальний розмір мережі	Коли використовувати
Louvain	$O(n \log n)$	Будь-який (до десятків млн)	Стандартний вибір для великих мереж соціальних медіа
Girvan-Newman	$O(n^3)$	До 10 000 вузлів	Малі мережі, коли важлива ієрархічна структура
Label Propagation	$O(n)$	Дуже великі мережі	Швидкий попередній аналіз, орієнтовний результат
Infomap	$O(n \log n)$	Середні та великі мережі	Аналіз спрямованих потоків інформації
Spectral Clustering	$O(n^2 - n^3)$	Малі та середні мережі	Мережі з чіткою блочною структурою

Реалізація мережного аналізу в Python: NetworkX

NetworkX це провідна Python-бібліотека для створення, аналізу та маніпуляції з графами. Вона надає зручний API для роботи з графами різних типів і реалізує сотні алгоритмів теорії графів. NetworkX є стандартом де-факто для академічних досліджень та прикладного аналізу мереж у Python.

Встановлення бібліотеки відбувається командою: `pip install networkx`. Основний робочий процес складається з трьох кроків: створення (або завантаження) графа, обчислення метрик, інтерпретація та візуалізація результатів.

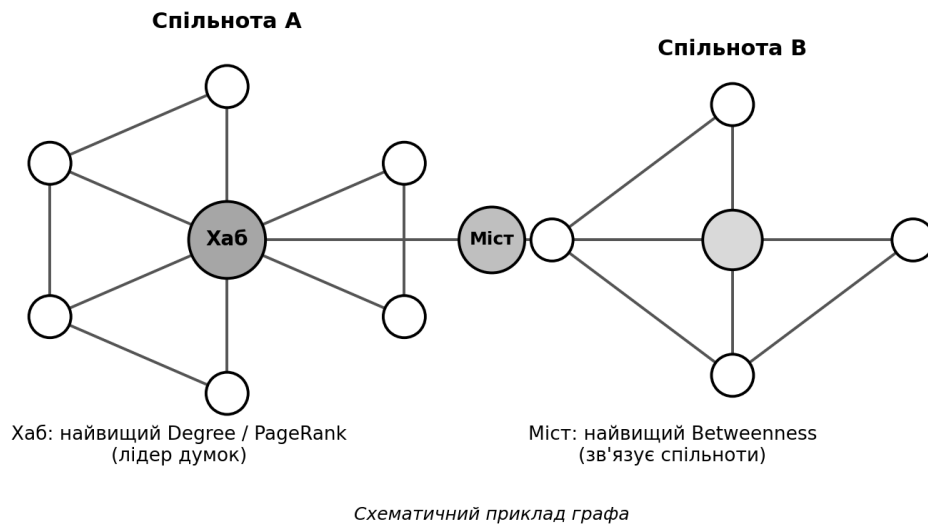


Рис. 4.2. Схематичний приклад мережі: хаб і міст між двома спільнотами

Базова робота з графами

Для початку роботи необхідно створити граф та наповнити його даними. У контексті аналізу Twitter/X це може бути мережа ретвітів: вузли це акаунти користувачів, ребра це дії ретвіту (хто кого ретвітнув). Нижче наведено базову структуру коду для роботи з NetworkX:

```
import networkx as nx
import matplotlib.pyplot as plt

# Створення орієнтованого зваженого графа
G = nx.DiGraph()

# Завантаження даних ретвітів
retweet_data = [
    ('user_A', 'influencer_X', 5),
    ('user_B', 'influencer_X', 12),
    ('user_C', 'user_A', 3),
] # (хто ретвітнув, чий твіт, скільки разів)

for source, target, weight in retweet_data:
    G.add_edge(source, target, weight=weight)
```

Після наповнення графа даними можна обчислювати метрики. Метрики PageRank, betweenness centrality та in-degree дають різні кути зору на важливість вузлів у мережі. Результати зазвичай сортуються за спаданням для ідентифікації топ-N найважливіших вузлів:

```
# Обчислення метрик центральності  
pagerank = nx.pagerank(G, alpha=0.85)  
betweenness = nx.betweenness_centrality(G)  
in_degree = dict(G.in_degree())
```

Community Detection у NetworkX та python-louvain

NetworkX сам по собі не включає алгоритм Louvain, але є окрема бібліотека python-louvain (pip install python-louvain), яка чудово інтегрується з NetworkX. Для роботи алгоритму Louvain граф повинен бути неорієнтованим (undirected), тому при аналізі мереж ретвітів зазвичай конвертують орієнтований граф або використовують окремий неорієнтований граф взаємодій:

```
import community as community_louvain  
  
# Конвертуємо орієнтований граф у неорієнтований  
G_undirected = G.to_undirected()  
  
# Застосовуємо алгоритм Louvain  
partition = community_louvain.best_partition(G_undirected)  
  
# Кількість знайдених спільнот  
num_communities = max(partition.values()) + 1  
print(f'Знайдено спільнот: {num_communities}')
```

Результатом є словник, де кожному вузлу (акаунту) присвоєний номер спільноти. Подальший аналіз полягає у вивченні характеристик кожної спільноти: якою мовою говорять її члени, які теми обговорюють, яку активність демонструють.

Інструменти візуалізації мереж

Результати мережного аналізу важко інтерпретувати без якісної візуалізації. Числові значення метрик центральності стають значно зрозумілішими, коли їх можна побачити на графі. Водночас великі мережі (сотні тисяч вузлів) вимагають спеціалізованих інструментів звичайні бібліотеки для малювання графів не можуть їх опрацювати.

Gephi стандарт для дослідників

Gephi це відкритий настільний застосунок для інтерактивної візуалізації та аналізу мереж. Він розроблений у 2006 році і є стандартним інструментом у академічних дослідженнях соціальних мереж. Gephi підтримує граф до 10 мільйонів вузлів завдяки апаратному прискоренню на GPU.

Gephi надає кілька алгоритмів макету для розташування вузлів у просторі. Найпопулярнішим є ForceAtlas2 силовий алгоритм, що «відштовхує» несхожі вузли та «притягує» зв'язані вузли один до одного. В результаті спільноти візуально виокремлюються у просторі щільні кластери пов'язаних акаунтів чітко видно. Алгоритм Yifan Hu краще підходить для дуже великих мереж (понад 100 000 вузлів). Circular Layout корисний для порівняльного аналізу невеликих мереж.

Gephi підтримує кілька форматів імпорту: GEXF (рекомендований, підтримує динамічні мережі), GraphML (XML-формат), CSV (списки ребер), GDF та JSON. Для експорту результатів мережного аналізу з NetworkX в Gephi зазвичай використовують формат GEXF:

```
# Експорт графа з NetworkX у GEXF для Gephi  
nx.write_gexf(G, 'retweet_network.gexf')  
# Далі відкриваємо файл у Gephi
```

igraph для масштабних обчислень

igraph бібліотека з інтерфейсами для Python, R та C, спеціально розроблена для роботи з великими мережами. Вона реалізована на C і є значно швидшою за NetworkX для обчислення метрик на великих графах. igraph є стандартним вибором, коли потрібно аналізувати мережі з сотнями тисяч і мільйонами вузлів.

Бібліотека включає всі основні алгоритми мережного аналізу: метрики центральності, кілька алгоритмів Community Detection (Louvain, Infomap, Label Propagation, Fastgreedy), засоби для роботи з підграфами та компонентами зв'язності, а також базові можливості візуалізації.

D3.js та Sigma.js інтерактивні веб-візуалізації

D3.js (Data-Driven Documents) JavaScript-бібліотека для побудови інтерактивних веб-візуалізацій. Вона дозволяє створювати повністю кастомізовані інтерактивні графи мереж, які можна вбудовувати у веб-застосунки та дашборди.

Sigma.js спеціалізована JavaScript-бібліотека для рендерингу графів у браузері з використанням WebGL. Вона оптимізована для роботи з великими графами (до 100 000 вузлів у браузері) та підтримує інтерактивні функції: масштабування, фільтрування, пошук за вузлами.

Для побудови системи риск-моніторингу, що включає веб-інтерфейс для аналітиків, поєднання Python (NetworkX/igraph) на бекенді та Sigma.js або D3.js на фронтенді є стандартним архітектурним рішенням.

ВИЯВЛЕННЯ БОТІВ ТА КООРДИНОВАНИХ МЕРЕЖ

Одним з найважливіших практичних застосувань мережного аналізу в контексті риск-моніторингу є виявлення ботів (автоматизованих акаунтів) та координованих мереж акаунтів, що діють не як незалежні особи, а як організована система.

Ознаки бот-акаунтів у мережній структурі

Боти та координовані акаунти мають характерні патерни в мережній структурі, що відрізняються від поведінки реальних людей. Аномально високий out-degree є першою ознакою: людина фізично не може ретвітнути 500 публікацій за годину, але бот може. Низьке значення clustering coefficient за умови високого degree ще одна ознака: реальні люди зазвичай взаємодіють зі своїми «знайомими», тоді як боти взаємодіють хаотично з різними акаунтами.

Зіркова топологія (star topology) є класичною структурою для ботнету: один центральний «командний» акаунт, навколо якого групуються десятки або сотні «виконавчих» акаунтів. Всі виконавчі акаунти ретвітять або дублюють контент командного акаунту. Така структура легко виявляється при аналізі in-degree та out-degree: командний акаунт матиме дуже високий in-degree від акаунтів ботнету.

Ще одна важлива ознака хронологічна синхронність. Якщо велика кількість акаунтів публікує однаковий або дуже схожий контент в один і той самий проміжок часу (наприклад, з різницею в секунди або кілька хвилин), це вказує на координовану автоматизовану поведінку. Для виявлення таких патернів мережний аналіз поєднується з часовим аналізом публікацій.

Алгоритмічне виявлення координованих мереж

Академічна спільнота розробила кілька методологій для виявлення Coordinated Inauthentic Behavior (CIB). Найбільш поширеною є методологія на основі аналізу коматриці URL-поширення: якщо два акаунти регулярно поширюють одні й ті самі URL в близький за часом момент, між ними додається «ребро координації». Мережа таких ребер координації потім аналізується на предмет кластерів.

Дослідники з Університету Кальярі (Nizzoli et al., 2021) запропонували метрику Coordinated Sharing Score (CSS), яка вимірює ступінь координованості пари акаунтів на основі порівняння часових рядів їхніх публікацій. Пари з високим CSS утворюють мережу координованої поведінки, яка потім аналізується за допомогою Community Detection.

У контексті українського інформаційного простору подібні методи використовує Центр стратегічних комунікацій та інформаційної безпеки (StratCom) при Міністерстві культури та інформаційної політики для виявлення та документування проявів інформаційних операцій.

Реальні кейси застосування мережного аналізу

Кейс 1: Виявлення координованої дезінформаційної кампанії EU DisinfoLab (2023)

У 2023 році організація EU DisinfoLab опублікувала дослідження, в якому задокументувала мережу з 750+ координованих акаунтів у Twitter/X та Facebook, що поширювали антиукраїнські наративи в Євросоюзі. Методологія дослідження базувалася на мережному аналізі: збирались дані про ретвіти та посилання на спільні джерела, будувалась мережа «координованого поширення», після чого алгоритмом Louvain виявлялись кластери акаунтів з

аномально схожою поведінкою. Ключові висновки дослідження: 80% акаунтів у виявленій мережі були створені протягом 3-місячного вікна, всі вони активно посилались на одні й ті самі 15 псевдоновинних сайтів, а хронологічний аналіз показав ідентичні патерни публікацій з точністю до хвилин.

Кейс 2: Аналіз скандалу H&M структура поширення кризи (2018)

Скандал навколо рекламної кампанії H&M у лютому 2018 став одним з найбільш задокументованих кейсів кризової комунікації в соціальних мережах. Ретроспективний мережний аналіз публікацій показав: протягом перших 48 годин у Twitter утворилось 7 чітко виражених спільнот навколо цієї теми. Community Detection виявив 3 акаунти з betweenness centrality вище 0.15 вони були «містками» між спільнотами. Серед цих містків акаунт музиканта The Weeknd, який публічно відмовився від співпраці з брендом та «активував» свою аудиторію. PageRank аналіз показав, що публікація The Weeknd мала в 45 разів більший реальний вплив, ніж його кількість підписників могла б свідчити. Висновок для риск-моніторингу: автоматизована система, що аналізує betweenness centrality в режимі реального часу, могла б ідентифікувати The Weeknd як ключовий вузол ще до того, як його публікація набрала масштабу.

Кейс 3: Моніторинг репутації українського бренду в умовах кризи

Платформа YouScan (українська система моніторингу соціальних мереж) в одному зі своїх публічних кейсів описала аналіз репутаційної кризи великого українського ритейлера (ідентифікація не розкривається) під час пікового сезону розпродажів. Система виявила різке збільшення негативних згадок і застосувала мережний аналіз для ідентифікації джерела: виявилось, що 67% негативного контенту поширювалося через один інформаційний хаб популярну групу споживчих відгуків у Facebook з 250 000 членів. Адміністрація групи сама публікувала негативні пости, що мали дуже високий in-degree (тисячі ретвітів та поширень). Завдяки мережному аналізу вдалося точно ідентифікувати «епіцентр» проблеми та вибудувати цільову комунікацію з адміністрацією групи.

Кейс 4: Виявлення ботів під час виборів Stanford Internet Observatory

Дослідники Стенфордського Internet Observatory у серії публікацій 2022–2023 років описали методологію виявлення автоматизованих акаунтів під час виборчих кампаній. Використовуючи комбінацію метрик out-degree аномалій, кластеризаційного коефіцієнта та аналізу часових патернів публікацій, дослідники ідентифікували понад 70 000 акаунтів з ознаками автоматизованої поведінки. Важливим висновком є те, що прості порогові значення (наприклад, «більше 500 публікацій на день = бот») дають багато помилкових спрацьовувань. Значно ефективнішим є аналіз структурних патернів у мережі: реальні люди, навіть дуже активні, мають інші мережеві характеристики, ніж автоматизовані акаунти.

ВИСНОВКИ

Мережний аналіз (Network Analysis) є фундаментальним інструментом сучасного риск-моніторингу соціальних мереж, що перетворює розрізнені публікації та взаємодії в зрозумілу структуру інформаційних потоків і соціальних зв'язків.

Перший ключовий висновок: розуміння математичних основ теорії графів є необхідною умовою для роботи зі структурованими даними соціальних мереж. Поняття вузлів та ребер, орієнтованих та зважених графів, щільності мережі та компонент зв'язності це базовий словник, без якого неможливо ані правильно сформулювати задачу аналізу, ані коректно інтерпретувати її результати.

Другий ключовий висновок: метрики центральності дозволяють ідентифікувати ключових акторів у мережі тих, чиї дії мають непропорційно великий вплив на поширення інформації. Degree centrality виявляє активні вузли, betweenness centrality ідентифікує «містки» між спільнотами, PageRank вимірює реальний вплив, а clustering coefficient допомагає виявити координовані групи акаунтів.

Третій ключовий висновок: алгоритми виявлення спільнот (Community Detection) є потужним інструментом для розуміння структури аудиторії та

виявлення координованих кампаній. Алгоритм Louvain є стандартним вибором для великих мереж завдяки поєднанню швидкості та якості результатів.

Четвертий ключовий висновок: практичний стек технологій для мережного аналізу соціальних мереж включає NetworkX та igraph для обчислень, Gephi для інтерактивної візуалізації та дослідження, Sigma.js та D3.js для інтеграції у веб-застосунки. Всі ці інструменти є відкритими та безкоштовними, що робить їх доступними для навчання та реальних проєктів.

П'ятий ключовий висновок: реальні кейси від виявлення дезінформаційних мереж EU DisinfoLab до аналізу репутаційних криз Н&М та українських брендів демонструють, що мережний аналіз є не теоретичним академічним інструментом, а практичним методом вирішення конкретних проблем інформаційної безпеки та репутаційного менеджменту.

Для студентів спеціальності 122 «Комп'ютерні науки» освоєння мережного аналізу відкриває широкі кар'єрні можливості: від розробника систем риск-моніторингу та аналітика кібербезпеки до дослідника соціальних мереж та спеціаліста з антикризових комунікацій. Попит на фахівців, що поєднують технічні навички програмування з розумінням соціальних процесів у цифровому середовищі, стабільно зростає як в Україні, так і на міжнародному ринку праці.

КОНТРОЛЬНІ ПИТАННЯ

1. Що таке мережний аналіз (Network Analysis) і чому він є ключовим інструментом риск-моніторингу соціальних мереж? Наведіть конкретний приклад його практичного застосування.
2. Поясніть різницю між орієнтованим та неорієнтованим графом. Наведіть приклад кожного з типів у контексті аналізу соціальних мереж.
3. Що вимірює Betweenness Centrality і чому ця метрика має особливе значення для риск-моніторингу? Наведіть приклад з реального кейсу, описаного в лекції.
4. Чим відрізняється PageRank від Degree Centrality як метрики оцінки впливу акаунту? Чому PageRank вважається більш точним показником реального впливу?

5. Що таке Community Detection і яку задачу вона вирішує? Опишіть принцип роботи алгоритму Louvain та вкажіть його переваги порівняно з алгоритмом Girvan-Newman.
6. Що таке модульність (modularity) і як вона використовується для оцінки якості виявлених спільнот? Які значення модульності вважаються прийнятними для реальних соціальних мереж?
7. Які мережеві ознаки свідчать про те, що акаунт є ботом або частиною координованої мережі? Опишіть щонайменше три характерні патерни.
8. Що таке Coordinated Inauthentic Behavior (CIB) і яким чином мережний аналіз допомагає його виявляти? Наведіть приклад із кейсу EU DisinfoLab (2023).
9. Опишіть основні можливості бібліотеки NetworkX для роботи з графами в Python. Яка різниця між NetworkX та igraph з точки зору продуктивності та сфери застосування?
10. Для яких задач використовується інструмент Gephi? Опишіть алгоритм ForceAtlas2 та поясніть, чому він є популярним для візуалізації спільнот у соціальних мережах.
11. Що таке зважений граф (weighted graph) і яку додаткову інформацію він надає порівняно із звичайним графом? Наведіть приклад застосування зваженого графа в аналізі соціальних мереж.
12. Проаналізуйте кейс H&M (2018) з позиції мережного аналізу. Яку роль відіграли акаунти з високою Betweenness Centrality у поширенні кризи та які висновки можна зробити для побудови систем ризик-моніторингу?
13. Поясніть поняття “giant component” та “щільність мережі”. Яке типове значення щільності для великих соціальних мереж і чим воно пояснюється?
14. Яку архітектуру системи ризик-моніторингу з веб-інтерфейсом ви б запропонували, спираючись на інструменти, описані в лекції? Обґрунтуйте вибір технологій для бекенду та фронтенду.
15. Як мережний аналіз застосовується в маркетингу впливу (influencer marketing)? Яку метрику центральності доцільно використовувати для пошуку ефективних мікроінфлюенсерів і чому?

Література

1. NetworkX Documentation (2024). NetworkX: Network Analysis in Python. <https://networkx.org/documentation/stable/>
2. EU DisinfoLab (2023). Report on Coordinated Inauthentic Behavior targeting Ukrainian narratives. <https://www.disinfo.eu/>
3. Stanford Internet Observatory (2023). Research on coordinated inauthentic behavior. <https://io.stanford.edu/>
4. YouScan (2024). Social Media Monitoring Case Studies for Ukrainian Brands. <https://youscan.io/>

ЛЕКЦІЯ 5. ІНСТРУМЕНТИ МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ

ВСТУП.

Соціальні мережі давно перестали бути просто майданчиком для спілкування. Сьогодні вони є головним середовищем, де формується громадська думка, народжуються репутаційні кризи та поширюється дезінформація. За даними дослідницької компанії DataReportal, станом на 2024 рік понад 5 мільярдів людей у світі щодня користуються соціальними мережами, генеруючи сотні мільйонів публікацій на добу. В цьому потоці даних приховані як можливості, так і загрози - для брендів, організацій, держав і окремих осіб.

Риск-моніторинг у соціальних мережах - це системна діяльність з відстеження, фільтрації та аналізу публічного контенту з метою раннього виявлення загроз репутації, кризових ситуацій, фейків і деструктивних інформаційних кампаній. Але аналіз неможливий без інструментів збору та обробки даних. Саме тому четверта лекція присвячена практичному фундаменту всієї дисципліни - інструментам моніторингу.

Для майбутнього фахівця зі спеціальності «Консолідована інформація» розуміння інструментарію моніторингу є критично важливим з кількох причин.

По-перше, жодна аналітична модель не має практичної цінності без даних. Фахівець, який знає лише теорію, але не вміє налаштувати систему отримання інформації, подібний до лікаря, що вміє ставити діагнози, але не вміє провести обстеження пацієнта.

По-друге, ринок інструментів моніторингу є надзвичайно різноманітним: від повністю безкоштовних рішень до корпоративних платформ вартістю десятки тисяч доларів на рік. Вміння обирати правильний інструмент під конкретне завдання і бюджет - окрема фахова компетенція. Ця лекція охоплює весь спектр: від Google Alerts, який не коштує нічого, до enterprise-рішень на кшталт Brandwatch.

По-третє, в умовах інформаційної війни, яку Україна веде з 2014 року і яка набула повномасштабного характеру з лютого 2022 року, питання оперативного моніторингу наративів і дезінформації у соціальних мережах вийшло далеко за

межі бізнес-завдань. Це питання національної безпеки, і фахівці зі спеціальності 122 мають бути готові вирішувати задачі такого рівня.

Четверта тема логічно продовжує попередні лекції: від теоретичних основ риск-моніторингу та методів аналізу тональності ми переходимо до практичної інфраструктури - конкретних платформ і бібліотек, завдяки яким ці методи реалізуються в реальному часі.

ПЛАН ЛЕКЦІЇ

1. Безкоштовні інструменти моніторингу - з чого почати
2. Комерційні платформи моніторингу: огляд, порівняння, вибір
3. Open-Source інструменти: Tweepy, Instaloader, PRAW, Telethon
4. Побудова власної системи моніторингу: архітектура та технологічний стек

Безкоштовні інструменти моніторингу - з чого почати

Перш ніж говорити про дорогі комерційні платформи і технічні бібліотеки, зупинимося на тому, що доступне кожному прямо зараз, без реєстрації картки і без витрат жодної гривні. Це принципово важливо: значна частина реальних задач риск-моніторингу вирішується безкоштовними інструментами, якщо грамотно їх комбінувати. Саме ці інструменти студенти використовуватимуть у лабораторно-практичних роботах. Безкоштовні інструменти умовно поділяються на дві категорії. Перша - це веб-сервіси з графічним інтерфейсом: не потребують програмування, запускаються в браузері, доступні кожному. Друга - Python-бібліотеки з відкритим кодом: потребують базових навичок програмування, але дають повну свободу в роботі з даними.

Google Alerts - найпростіший старт

Google Alerts (alerts.google.com) - безкоштовний сервіс від Google, що дозволяє відстежувати появу будь-якого ключового слова або фрази в публічному інтернеті: новинних сайтах, блогах, форумах. Щойно Google індексує нову сторінку з вашим запитом, ви отримуєте листа на email.

Налаштування займає буквально три хвилини. Достатньо зайти на alerts.google.com, ввести назву бренду, компанії або персони, обрати мову,

країну і частоту сповіщень - і система починає працювати. Нульові технічні знання, нульова оплата.

Практичний приклад: студент виконує завдання з моніторингу репутації «Нової пошти». Він налаштовує три окремі алерти: «Нова Пошта», «Nova Poshta» і «НоваПошта» (для варіантів написання). Протягом тижня він отримує на email усі новини і публікації, де згадується компанія, і може аналізувати тональність вручну або зберегти у таблицю. Головні обмеження Google Alerts: сервіс охоплює лише індексовані Google сторінки - соціальні мережі (Facebook, Instagram, Telegram) він не моніторить. Окрім того, сповіщення можуть надходити із затримкою до кількох годин. Для базового моніторингу новинного фону це чудовий старт, але для повноцінного риск-аналізу його потрібно доповнювати іншими інструментами.

Hootsuite Free - безкоштовний план для 3 профілів

Hootsuite - одна з найвідоміших у світі платформ управління соціальними мережами. Більшість її функцій платна, але є безкоштовний план, що включає підключення до трьох соціальних профілів і базовий моніторинг стрічки.

Для студентських і навчальних цілей безкоштовний план Hootsuite дозволяє відстежувати публікації за ключовими словами в підключених соціальних мережах, планувати публікації і отримувати базову статистику охоплення. Реєстрація проходить на hootsuite.com без прив'язки платіжної картки. Важливе застереження: безкоштовний план Hootsuite суттєво обмежений у функціях моніторингу порівняно з платними тарифами. Він підходить для знайомства з платформою і виконання базових навчальних завдань, але не замінює повноцінний social listening.

Mention - 14 днів безкоштовного trial з повним функціоналом

Mention (mention.com) - спеціалізована платформа медіамоніторингу, що відстежує понад мільярд джерел і надсилає алерти протягом п'яти хвилин після появи нової публікації. Платформа пропонує безкоштовний пробний період тривалістю 14 днів з повним доступом до всіх функцій - без обмежень.

14 днів цілком достатньо для виконання лабораторно-практичної роботи. За цей час студент може налаштувати моніторинг обраного бренду або персони, зібрати дані про згадки в соціальних мережах і ЗМІ, проаналізувати динаміку тональності і підготувати звіт. Реєстрація безкоштовна на mention.com, платіжна картка для trial не обов'язкова.

Після закінчення trial Mention пропонує платні тарифи від 49 доларів на місяць. Для навчальних цілей безкоштовного періоду більш ніж достатньо.

Brand24 - 14 днів trial з підтримкою української мови

Brand24 (brand24.com) - польська платформа моніторингу, що особливо добре підходить для роботи з україномовним контентом. Вона підтримує аналіз тональності для 108 мов, включно з українською, і має унікальну функцію Anomaly Detection - автоматичне виявлення аномальних стрибків у кількості згадок. Brand24 також надає 14-денний безкоштовний trial з повним функціоналом. Реєстрація на brand24.com займає кілька хвилин. Після введення ключового слова платформа одразу починає збирати згадки і показує їх на зрозумілому дашборді з графіком динаміки, картою джерел і аналізом тональності.

Для студентів зі спеціальності «Консолідована інформація» Brand24 є найрекомендованішою платформою для лабораторних робіт: інтуїтивний інтерфейс, підтримка української мови, широке охоплення джерел і функціональний безкоштовний trial.

Open-Source Python-бібліотеки - безкоштовні назавжди

Python-бібліотеки з відкритим кодом - це інструменти, що встановлюються однією командою (pip install назва_бібліотеки) і надають повний програмний доступ до даних соціальних мереж. На відміну від веб-сервісів, вони потребують базових навичок Python, але натомість дають повну свободу: ви самі визначаєте, які дані збирати, як їх обробляти і де зберігати. Жодних місячних лімітів, жодної оплати.

Детальний огляд кожної бібліотеки наведено у розділі 4.3. Тут перелічимо основні інструменти, доступні студентам для практичної роботи.

- **Tweepy (Twitter/X)** - найпопулярніша бібліотека для роботи з Twitter/X API. Дозволяє шукати твіти за ключовими словами і хештегами. Важливий нюанс: безкоштовний рівень API Twitter після змін 2023 року суттєво обмежений за кількістю запитів. Для навчальних завдань цього достатньо, але промисловий моніторинг потребує платного доступу. Документація: <https://docs.tweepy.org>
- **PRAW (Reddit)** - офіційна бібліотека Reddit API. Повністю безкоштовна без жодних реальних обмежень для навчальних задач. Reddit API досі залишається щедрим і зручним для роботи. Документація: <https://praw.readthedocs.io>
- **Instaloader (Instagram)** - бібліотека для збору публічних публікацій і коментарів з Instagram без офіційного API. Повністю безкоштовна. Слід пам'ятати про дотримання rate limits Instagram. Документація: <https://instaloader.github.io>
- **Telethon (Telegram)** - бібліотека для роботи з MTProto API Telegram. Повністю безкоштовна і є найціннішим інструментом для моніторингу в Україні, де Telegram є домінуючим медіасередовищем. Документація: <https://docs.telethon.dev>

Практичний висновок: що обрати для лабораторної роботи

Для виконання лабораторно-практичних робіт з дисципліни «Риск-моніторинг у соціальних мережах» пропонується наступна стратегія вибору інструменту.

Якщо завдання стосується моніторингу новинного фону і не потребує охоплення соціальних мереж - використовуйте Google Alerts. Налаштування займає 5 хвилин, результат отримаєте вже наступного дня.

Якщо завдання потребує аналізу згадок у соціальних мережах через зрозумілий графічний інтерфейс - зареєструйтесь на trial Brand24 або Mention. Обидві платформи дають 14 днів повного безкоштовного доступу, що перекидає тривалість будь-якої лабораторної роботи.

Якщо завдання має технічний характер і передбачає програмування - використовуйте PRAW для Reddit або Telethon для Telegram. Обидві бібліотеки повністю безкоштовні і мають чудову документацію.

Комбінація Google Alerts + Brand24 trial + PRAW або Telethon покриває більшість навчальних задач з риск-моніторингу без будь-яких витрат.

Комерційні платформи моніторингу

Комерційні платформи моніторингу - це готові SaaS-рішення (Software as a Service), що надають повний набір інструментів у єдиному інтерфейсі: збір даних з тисяч джерел, автоматичний аналіз тональності, налаштування алертів та формування звітів. Вони позбавляють аналітика необхідності програмувати і дозволяють зосередитись безпосередньо на роботі з даними. Проте за зручність доводиться платити - і буквально, і в сенсі залежності від постачальника.

Знати комерційні платформи необхідно навіть тим, хто ніколи не буде їх купувати. Причина проста: у реальній роботі аналітик отримуватиме завдання від замовників, які вже використовують ці системи. Вміти читати їхні звіти, розуміти їхні метрики і критично оцінювати їхні обмеження - обов'язкова компетенція.

Brandwatch - Enterprise Social Intelligence (від 1 000 \$/міс)

Brandwatch - один із найпотужніших інструментів на ринку, орієнтований насамперед на великі корпорації та PR-агенції. Платформа моніторить понад 100 мільйонів онлайн-джерел і зберігає архів публікацій глибиною 27 років, що дозволяє проводити ретроспективний аналіз і порівнювати поточну ситуацію з минулими кризами.

Ключовою перевагою Brandwatch є точність sentiment analysis на рівні близько 90%, що досягається завдяки власним моделям машинного навчання. Крім того, платформа вміє аналізувати зображення - автоматично розпізнавати логотипи брендів на фотографіях навіть без текстових згадок.

Реальний кейс: під час кризи Samsung Galaxy Note 7 у 2016 році, коли смартфони починали загорятися, Samsung використовував Brandwatch для відстеження реакції аудиторії у 28 країнах одночасно. Система аналізувала

понад 500 000 публікацій на добу, а PR-команда отримувала сповіщення про нові хвилі негативу протягом трьох хвилин після їх появи. Це дозволило координувати антикризові кампанії у різних часових поясах паралельно.

Вартість від 1 000 доларів на місяць робить Brandwatch недоступним для освітніх установ, але знання про його можливості є частиною фахової підготовки.

Sprout Social - SMM та аналітика в одному рішенні (від 249 \$/міс)

Sprout Social поєднує управління публікаціями в соціальних мережах з функціями моніторингу та аналітики. Це робить її привабливою для агенцій і брендів, яким потрібен єдиний інструмент для роботи з контентом і відстеження реакції аудиторії. Платформа підтримує TikTok, LinkedIn, Pinterest. Вбудована CRM-функціональність дозволяє відстежувати комунікацію з конкретними клієнтами безпосередньо в інтерфейсі платформи.

Приклад: компанія Evernote використовує Sprout Social для моніторингу відгуків у Twitter та Facebook, автоматично призначаючи скарги відповідним менеджерам підтримки. Це скоротило середній час відповіді клієнтам з кількох годин до 20–30 хвилин.

Brand24 - рекомендована платформа для українського ринку (від 79 \$/міс, є trial)

Brand24 - польська платформа, що стала особливо популярною серед українських брендів, агенцій та університетів. Унікальна функція Anomaly Detection автоматично виявляє аномальні стрибки у кількості згадок: якщо звичайна добова кількість публікацій про бренд становить 50, а раптом за годину їх з'являється 300 - система миттєво надсилає сповіщення. Саме так виявляються початкові стадії репутаційних криз, коли ще є час на превентивне реагування.

Як зазначалося у розділі 4.1, Brand24 пропонує 14-денний безкоштовний trial. Після завершення trial вартість платних тарифів стартує від 79 доларів на місяць. Для академічних установ є спеціальні знижки.

Meltwater - найкращий вибір для PR-команд (від 5 000 \$/рік)

Meltwater орієнтований на PR-команди великих корпорацій. Головна особливість - власна база даних більше мільйона журналістів і медіа-редакцій у всьому світі, що дозволяє не лише моніторити ЗМІ, але й планувати PR-кампанії, орієнтовані на конкретних журналістів і видання. Платформа відстежує понад 400 000 медіа-джерел і готує автоматичні PR-звіти. Ціна від 5 000 доларів на рік робить Meltwater вибором виключно для великих корпорацій.

ЯК ОБИРАТИ КОМЕРЦІЙНУ ПЛАТФОРМУ

Вибір платформи завжди залежить від бюджету, масштабу задач і технічних компетенцій команди. Стартап або агенція з обмеженим бюджетом обере Brand24 або Mention. SMM-агенція, що обслуговує кількох клієнтів, виграє від Sprout Social, який об'єднує управління публікаціями і аналітику. Великий бренд з ризиком репутаційних криз на мільйони доларів може виправдати витрати на Brandwatch. PR-відділ корпорації, що активно працює зі ЗМІ, оцінить унікальну базу журналістів Meltwater.

Open-Source інструменти

Open-source інструменти - це бібліотеки з відкритим вихідним кодом, безкоштовні назавжди. На противагу комерційним платформам, вони не мають зручного графічного інтерфейсу - потребують навичок програмування на Python. Проте вони дають те, чого не дасть жодна комерційна платформа: повний контроль над даними, необмежені обсяги збору і можливість моніторити будь-які джерела, включно з Telegram-каналами.

Чому риск-аналітик повинен знати open-source інструменти? Перша причина - гнучкість: ви збираєте рівно ті дані, що потрібні, без обмежень постачальника. Друга - вартість: при великих обсягах аналізу ліміти комерційних платформ вичерпуються швидко, а дані по тарифах коштують дорого. Третя - унікальні джерела: Telegram в Україні є критично важливим медіасередовищем, але жодна комерційна платформа не моніторить його повноцінно.

Tweepy - моніторинг Twitter/X

Tweepy - найпопулярніша Python-бібліотека для роботи з Twitter/X API. Вона дозволяє шукати твіти за ключовими словами, відстежувати хештеги у реальному часі та аналізувати активність конкретних акаунтів.

Практичний приклад: уявіть, що ви аналітик для великої української логістичної компанії. Клієнт пише скаргу в Twitter з хештегом #НоваПошта. Якщо компанія використовує Tweepy у поєднанні з sentiment classifier, цей твіт може бути визначений як негативний і переданий команді підтримки протягом хвилини після публікації - задовго до того, як SMM-менеджер перевірить стрічку.

Важлива технічна особливість: після змін у квітні 2023 року безкоштовний рівень Twitter API v2 суттєво обмежений - лише 500 000 твітів на місяць і 1 запит на 15 хвилин для деяких ендпоінтів. Для навчальних задач цього достатньо, але для промислового моніторингу потрібен платний Basic або Pro доступ. Офіційна документація: <https://docs.tweepy.org/en/stable/>

4.3.2. PRAW - моніторинг Reddit

PRAW (Python Reddit API Wrapper) - офіційна бібліотека для роботи з Reddit API. Reddit є надзвичайно цінним джерелом для моніторингу міжнародної репутації компаній. Його аудиторія схильна до розгорнутих, аргументованих коментарів, тому репутаційні кризи часто зароджуються саме там і лише потім потрапляють в основні ЗМІ.

Практичний приклад: кейс United Airlines у 2017 році, коли пасажира силоміць зняли з рейсу. Відео стало вірусним спочатку на Reddit (сабредит r/videos), і лише через кілька годин потрапило на CNN та BBC. Компанія втратила 1,4 мільярда доларів капіталізації за один день. Система моніторингу на PRAW могла б виявити ситуацію ще на початковій стадії.

PRAW є повністю безкоштовним без суттєвих обмежень для навчальних задач. Реєстрація застосунку на reddit.com/prefs/apps займає кілька хвилин. Офіційна документація: <https://praw.readthedocs.io/>

Instaloader - аналіз публічного контенту Instagram

Instaloader - Python-бібліотека, що дозволяє збирати публічні публікації, коментарі та метадані профілів з Instagram без офіційного Instagram Graph API, доступ до якого суттєво обмежений.

Практичний кейс: компанія «Епіцентр К» під час репутаційної кризи 2022 року могла б використати Instaloader для збору та аналізу коментарів під своїми публікаціями та публікаціями медіа з хештегом #епіцентр. Аналіз тисяч коментарів за допомогою NLP-інструментів дав би кількісну картину настроїв аудиторії і допоміг розставити пріоритети в антикризовій комунікації.

Важливе застереження: між запитами необхідно робити паузи, щоб не перевищити rate limits Instagram. При надмірно інтенсивному зборі акаунт може бути тимчасово заблокований. Офіційна документація: <https://instaloader.github.io/>

Telethon - моніторинг Telegram (критично для України)

Telethon - Python-бібліотека для роботи з MTProto API Telegram. Для українського ринку вона є, мабуть, найважливішим open-source інструментом моніторингу. Telegram в Україні - це не лише месенджер: тисячі новинних каналів, анонімних каналів із «зливами» інформації, груп громадського обговорення утворюють потужне медіасередовище, яке жодна комерційна платформа не охоплює повноцінно.

За допомогою Telethon можна підписатись на будь-який публічний Telegram-канал і отримувати всі нові повідомлення в режимі реального часу, зберігаючи їх у базу даних для подальшого аналізу. Бібліотека повністю безкоштовна. Офіційна документація: <https://docs.telethon.dev/>

Social-Analyzer - кроссплатформений аналіз профілів

Social-Analyzer - відкрита бібліотека для пошуку профілів однієї особи або бренду одночасно на більш ніж 300 платформах. Вона корисна в задачах конкурентної розвідки та відстеження поведінки конкретних акторів у різних соціальних мережах. GitHub: <https://github.com/qeeqbox/social-analyzer>

ПОБУДОВА ВЛАСНОЇ СИСТЕМИ МОНІТОРИНГУ

Власна система моніторингу - це рішення, яке організація розробляє самостійно, поєднуючи open-source бібліотеки, хмарні сервіси та власну бізнес-логіку. Для технічних команд або організацій зі специфічними вимогами власна система часто виявляється ефективнішою за комерційні альтернативи.

Власна система виправдана в кількох ситуаціях: бюджетні обмеження (при п'яти брендах для аналізу власна розробка дешевша за комерційну підписку вже через рік), вимоги до конфіденційності даних (державні і фінансові установи не можуть передавати дані стороннім SaaS-провайдерам), унікальні джерела (специфічні галузеві форуми або локальні сайти, яких немає в комерційних платформах).

П'ятишарова архітектура системи моніторингу

Будь-яка система моніторингу соціальних мереж, незалежно від масштабу, складається з п'яти функціональних шарів. Це не просто технічна деталь - це ментальна модель, що допомагає критично оцінювати будь-які інструменти: за кожним інтерфейсом комерційної платформи стоять ці ж самі п'ять шарів.

Перший шар - збір даних (Data Collection). Відповідає за отримання сирих даних з різних джерел. Twitter/X опрацьовується через Tweepy у режимі реального часу. Instagram - через Instaloader з інтервалом раз на годину-шість. Reddit - через PRAW кожні 30 хвилин. Новинні сайти - через web-scraping бібліотеками Scrapy і BeautifulSoup кожні 15 хвилин. Telegram-канали - через Telethon у реальному часі. Для моніторингу в Україні критично важливо охоплювати специфічні локальні джерела: Telegram-канали, бізнес-видання Delo.ua, Mind.ua, Е правда, IT-спільноту DOU.ua, відгуки на OLX та Rozetka.

Другий шар - зберігання даних (Storage). Дані з соціальних мереж є гетерогенними - твіт, відгук на OLX і стаття в ЗМІ мають абсолютно різні структури. Тому реальні системи використовують декілька баз даних паралельно. MongoDB (документна NoSQL) найкраще підходить для сирих постів з різних платформ. PostgreSQL - для структурованих аналітичних запитів. Elasticsearch забезпечує швидкий повнотекстовий пошук по великому архіву.

Redis застосовується для кешування і черг у реальному часі. ClickHouse - для агрегаційних запитів на мільярдах рядків.

Третій шар - обробка даних (Processing). Сирі дані непридатні для аналізу: вони містять URL-адреси, HTML-теги, повтори і спам. Базовий ETL-пайплайн включає видалення URL та HTML-тегів, збереження емодзі (вони несуть важливу емоційну інформацію), нормалізацію пробілів, визначення мови. Для великих обсягів використовують Apache Kafka (черга повідомлень) і Apache Spark Streaming (паралельна обробка). Для менших обсягів достатньо Celery з Redis.

Четвертий шар - аналітика (Analytics). Тут відбувається перетворення очищених текстів на змістовні сигнали. Для класифікації тональності використовуються BERT-подібні моделі або VADER. Topic modeling (BERTopic, LDA) автоматично кластеризує публікації за темами. Anomaly detection (Z-score, Isolation Forest) виявляє аномальні стрибки обсягу згадок. Named Entity Recognition у бібліотеці spaCy з моделлю uk_core_news забезпечує виявлення імен, організацій і географічних об'єктів в українському тексті.

П'ятий шар - візуалізація (Visualization). Найкраща аналітична модель марна без зрозумілого представлення результатів. Grafana - безкоштовний інструмент для real-time дашбордів. Kibana - вбудований інтерфейс Elasticsearch. Tableau і Power BI - комерційні рішення для бізнес-аналітики. Для студентських проектів найкраще підходить Streamlit - Python-бібліотека, що перетворює скрипт на веб-дашборд за 10–30 рядків коду.



Рис. 5.1. П'ятишарова архітектура системи моніторингу соціальних мереж

Мінімальна власна система: MVP за тиждень

Розглянемо покроковий план побудови мінімальної системи моніторингу для студентського проекту. Такий MVP (Minimum Viable Product) не замінить Brandwatch, але демонструє повний цикл від збору даних до звіту і є цінним проектом для портфолію.

Перший і другий дні - збір даних. Налаштовується Google Alerts для новинних сайтів і PRAW або Telethon для соціальних мереж. Дані зберігаються у CSV-файл.

Третій день - зберігання. CSV замінюється базою даних SQLite (вбудована SQL-база, не потребує сервера) або безкоштовним хмарним рівнем MongoDB Atlas.

Четвертий день - аналіз. До кожного запису додається оцінка тональності за допомогою VADER, розраховуються щоденний Net Sentiment Score та Crisis Velocity (швидкість зростання негативу).

П'ятий і шостий дні - візуалізація. На Streamlit будується простий дашборд з графіком динаміки NSS, хмарою слів і таблицею останніх негативних публікацій.

Сьомий день - алертинг. Додається Telegram-бот (бібліотека python-telegram-bot), що надсилає повідомлення в робочий чат при падінні NSS нижче заданого порогу.

Реальний кейс: Укрпошта та гібридна система моніторингу

Укрпошта у 2022–2023 роках значно посилила систему моніторингу репутації, зіткнувшись з масовим потоком скарг через зростання навантаження на логістику під час повномасштабного вторгнення. Компанія обрала гібридний підхід: на комерційному рівні використовувала Brand24 для базового моніторингу та звітності, на власному рівні - Python-скрипти на Telethon для моніторингу Telegram-каналів. Результат: час виявлення репутаційних проблем скоротився з 24 годин до 2–3 годин. Скарги, виявлені в соцмережах, автоматично перетворювались на тикети в CRM-системі.

Цей кейс ілюструє ключовий принцип: найкраще рішення рідко є виключно комерційним або виключно open-source. Найефективніша стратегія - комбінація безкоштовних інструментів для рутинного моніторингу, trial-доступу до комерційних платформ для разових проєктів і власних Python-скриптів для специфічних джерел.

ВИСНОВКИ

Тема четвертої лекції є центральною в практичному вимірі дисципліни «Риск-моніторинг у соціальних мережах». Розглянутий матеріал дозволяє сформулювати кілька ключових висновків.

Перший висновок: якісний риск-моніторинг можна організувати без жодних фінансових витрат. Google Alerts, безкоштовні trial-версії Brand24 і Mention, а також Python-бібліотеки PRAW і Telethon забезпечують повноцінний цикл збору та аналізу даних. Студенти і початківці-аналітики мають усе необхідне для практичної роботи вже сьогодні.

Другий висновок: не існує універсально найкращого інструменту. Вибір завжди залежить від конкретного поєднання факторів: бюджету, технічних компетенцій, мовних вимог, специфіки джерел і рівня кризових ризиків. Розуміння всього спектру - від Google Alerts до Brandwatch - дозволяє приймати обґрунтовані рішення.

Третій висновок: для України Telegram є критично важливим джерелом інформації, якого жодна комерційна платформа не охоплює повноцінно.

Навичка роботи з бібліотекою Telethon є практичною необхідністю для вітчизняного риск-аналітика.

Четвертий висновок: фундаментальне розуміння п'ятишарової архітектури систем моніторингу (збір - зберігання - обробка - аналітика - візуалізація) є інваріантним знанням, що залишається актуальним незалежно від того, які конкретні інструменти використовуються. Ринок змінюється: платформи з'являються і зникають, але архітектурні принципи залишаються.

П'ятий висновок: практичні навички набуваються лише через практику. Виконання лабораторно-практичних робіт з використанням безкоштовних інструментів, описаних у цій лекції, є ефективним способом закріплення матеріалу і одночасно формування портфоліо.

Контрольні питання

1. Назвіть чотири повністю безкоштовні інструменти моніторингу. Які задачі вирішує кожен з них?
2. Що таке Google Alerts і яке його головне обмеження з точки зору риск-моніторингу?
3. Чим відрізняється безкоштовний trial Brand24 від безкоштовного плану Hootsuite? Який з них ефективніший для навчальних задач?
4. Назвіть три ключові відмінності між Brandwatch та Brand24. Для яких типів організацій підходить кожна з платформ?
5. Коли варто обирати open-source рішення замість комерційної платформи? Наведіть три аргументи.
6. Чому Telethon є критично важливою бібліотекою для риск-моніторингу в Україні?
7. Опишіть п'ятишарову архітектуру власної системи моніторингу. Яке призначення кожного шару?
8. Запропонуйте оптимальний набір безкоштовних інструментів для студентського проекту з моніторингу репутації українського бренду. Обґрунтуйте.

Література

1. Google Alerts: офіційний сервіс. URL: <https://alerts.google.com>
2. Hootsuite: безкоштовний план. URL: <https://hootsuite.com>
3. Mention: безкоштовний trial 14 днів. URL: <https://mention.com>
4. Brand24: безкоштовний trial 14 днів. URL: <https://brand24.com> (дата звернення: 2024).
5. Tweepy: офіційна документація. URL: <https://docs.tweepy.org/en/stable/>
6. PRAW - Python Reddit API Wrapper: документація. URL: <https://praw.readthedocs.io/>
7. Instaloader: офіційна документація. URL: <https://instaloader.github.io/>
8. Telethon - Python Telegram MTProto API: документація. URL: <https://docs.telethon.dev/>
9. Social-Analyzer: GitHub. URL: <https://github.com/qeeqbox/social-analyzer>
10. Apache Kafka: офіційна документація. URL: <https://kafka.apache.org/documentation/>
11. Elasticsearch / Kibana: офіційна документація. URL: <https://www.elastic.co/guide/>
12. Grafana: офіційна документація. URL: <https://grafana.com/docs/>
13. Streamlit: офіційна документація. URL: <https://docs.streamlit.io/>
14. DataReportal - Global Digital Overview 2024. URL: <https://datareportal.com/global-digital-overview>

Лекція 6. КРИЗОВИЙ МЕНЕДЖМЕНТ ТА АНТИКРИЗОВА КОМУНІКАЦІЯ В СОЦІАЛЬНИХ МЕРЕЖАХ

ВСТУП.

Попередні лекції сформували фундамент: ми з'ясували, що таке ризик-моніторинг і навіщо він потрібний, вивчили типологію ризиків у соціальних мережах, опанували методи збору та аналізу даних, а також розглянули весь спектр інструментів - від безкоштовних до enterprise-рішень. Однак усі ці знання набувають практичного сенсу лише тоді, коли ми вміємо відповідати на питання: що робити, коли криза вже розгорілася?

Дана лекція присвячена саме цьому - кризовому менеджменту та антикризовій комунікації в соціальних мережах. Це не лише теорія: за даними PwC Global Crisis Survey 2023, 95% керівників великих компаній вважають кризовий менеджмент одним із трьох найважливіших операційних пріоритетів, а 70% визнають, що їхні організації були б серйозно пошкоджені без підготовленого плану реагування.

Посилання: <https://www.pwc.com/gx/en/issues/crisis-and-resilience/global-crisis-survey.html>

Для майбутнього фахівця зі спеціальності «Консолідована інформація» розуміння кризового менеджменту є критично важливим з кількох причин.

По-перше, у цифровому середовищі криза розвивається в десятки разів швидше, ніж у традиційних медіа. Дослідження Edelman Trust Barometer 2024 показало: 72% споживачів формують остаточну думку про бренд у кризовій ситуації протягом першої години після появи негативної публікації. Це означає, що аналітик, який вміє лише збирати дані, але не знає, як на них реагувати, має половину необхідних компетенцій.

Посилання: <https://www.edelman.com/trust/2024/trust-barometer>

По-друге, антикризова комунікація в соціальних мережах принципово відрізняється від традиційного PR. Тут немає можливості відредагувати матеріал після публікації, аудиторія отримує інформацію не з одного джерела, а з тисяч, і кожен коментар компанії - чи то правильний, чи то помилковий - стає самостійним об'єктом аналізу та поширення. Студент, який розуміє ці механізми, здатний запобігати збиткам, а не лише констатувати їх.

По-третє, в умовах, коли Україна веде інформаційну війну з 2014 року і повномасштабну з лютого 2022 року, кризовий менеджмент став питанням не лише корпоративного, а й державного та суспільного значення. Відповідальна антикризова комунікація захищає не лише бізнес - вона захищає суспільну довіру, яка є одним з ключових ресурсів в умовах гібридної війни.

ПЛАН ЛЕКЦІЇ

1. Анатомія репутаційної кризи в соціальних мережах: стадії, механізми поширення та типові тригери
2. Превентивний кризовий менеджмент: Crisis Playbook та передкризова підготовка
3. Стратегії та тактики антикризової комунікації: від першої реакції до відновлення репутації
4. Особливості кризової комунікації для різних типів криз та різних аудиторій
5. Відновлення репутації після кризи: довгострокові стратегії та вимірювання результатів
6. Реальні кейси: аналіз успіхів і невдач антикризової комунікації

АНАТОМІЯ РЕПУТАЦІЙНОЇ КРИЗИ В СОЦІАЛЬНИХ МЕРЕЖАХ **Поняття репутаційної кризи та її специфіка в цифровому середовищі**

Репутаційна криза - це ситуація, за якої публічне сприйняття організації, бренду або особи різко погіршується внаслідок конкретної події або серії подій, що набули широкого розголосу. Ключова відмінність кризи в соціальних мережах від традиційної медіакризи полягає в трьох характеристиках: швидкості поширення, масштабі охоплення та складності контролю над наративом.

Швидкість поширення є принципово іншою, ніж у класичних медіа. Журналіст традиційного видання пише матеріал кілька годин, редактор його перевіряє, матеріал публікується до певного часу. У соціальних мережах відео може бути знято, опубліковане та переглянуте мільйоном людей ще до того, як перший журналіст отримає повідомлення про інцидент. Дослідження MIT (Vosoughi et al., 2018) показало, що неправдива інформація у Twitter поширюється в 6 разів швидше за правдиву та охоплює в 10 разів більшу

аудиторію.

Посилання

на

дослідження:

<https://science.sciencemag.org/content/359/6380/1146>

Масштаб охоплення у цифровому середовищі не має географічних або мовних обмежень. Локальний інцидент може стати міжнародним за лічені години. Класичним прикладом є скандал з United Airlines у квітні 2017 року: силове видалення пасажирів Девіда Дао зафільмували інші пасажирів, відео опинилось у Twitter, і вже за 24 години кількість переглядів перевищила 100 мільйонів. Капіталізація компанії скоротилась приблизно на 955 мільйонів доларів. Джерело: <https://www.theguardian.com/business/2017/apr/11/united-airlines-boss-deeply-apologises>

Завдання кризового менеджменту в соціальних мережах - не ліквідувати чужі голоси (це неможливо), а запропонувати настільки переконливий власний наратив, щоб він домінував у публічному дискурсі.!!!!

СТАДІЇ РОЗВИТКУ КРИЗИ

Стадія 1. Передкризова (Latent Stage). Існують передумови для кризи, але вони ще не стали публічними. Це можуть бути накопичені скарги клієнтів у закритих каналах, внутрішній конфлікт, технічна вразливість або повільно наростаючий негатив на маловідомих форумах. Саме на цій стадії системи моніторингу, описані в попередніх лекціях, здатні виявити проблему і дати час на превентивне реагування. Приклад: до публічного скандалу з тарганами в одній із мереж швидкого харчування в Україні (2021) відповідні публікації з'являлись у місцевих Facebook-групах протягом кількох тижнів.

Стадія 2. Тригерна подія (Trigger Event). Конкретна публікація, відео, стаття або заява запускає кризу. Тригером може бути не нова подія - часто це давно відома проблема, яку один вірусний пост виносить на масове обговорення. Тут рахунок іде на хвилини: перші 60 хвилин після тригерної події визначають, чи залишиться криза локальною, чи вибухне.

Стадія 3. Ескалація (Escalation). Контент починає поширюватись через репости, коментарі, хештеги та підхоплення ЗМІ. На цій стадії системи виявлення аномалій (Anomaly Detection) фіксують різкий стрибок Crisis Velocity.

Ключова небезпека: медіа підсилюють і деформують початковий меседж - кожне нове переповідання додає емоційне забарвлення та спотворення.

Стадія 4. Пік (Peak). Максимальний обсяг обговорення, залучення ЗМІ, запити від журналістів, реакції конкурентів та лідерів думок. Саме на цій стадії відбуваються найбільші фінансові збитки: падіння акцій, відтік клієнтів, відмова партнерів від співпраці.

Стадія 5. Затухання (Declining). Інтерес аудиторії знижується. Але криза не зникає безслідно: публікації залишаються в пошукових системах, алгоритми рекомендацій продовжують показувати їх новим користувачам. Репутаційні “шрами” можуть залишатись активними роками.

Стадія 6. Посткризовий стан (Post-Crisis). Організація або відновлює репутацію (якщо правильно реагувала на кожній стадії), або входить у тривалий стан підвищеного негативного фону. Дослідження Deloitte Global Crisis Survey показало: компанії, що мали підготовлений crisis playbook, відновлювали докризовий рівень Net Sentiment Score у середньому за 4 місяці, тоді як непередготовлені - за 14 місяців. Посилання: <https://www2.deloitte.com/global/en/pages/risk/articles/crisis-survey.html>

Типологія кризових тригерів

На основі аналізу понад 500 корпоративних криз у соціальних мережах дослідники виокремлюють шість основних типів тригерів, кожен з яких вимагає окремої стратегії реагування.

Операційний збій - технічний або сервісний інцидент, що безпосередньо вплинув на клієнтів: відключення сервісу, затримка доставки, масовий дефект продукту. Типовий приклад - кібератака на Kyivstar у грудні 2023 року, яка залишила без зв'язку понад 24 мільйони абонентів. За перші 6 годин кількість згадок у соцмережах перевищила 180 тисяч. Джерело: <https://nv.ua/ukr/techno/gadgets/kyivstar-zboy-shcho-vidomo-50384942.html>

Скандал з персоналом або керівництвом - публічне розкриття неетичної поведінки, дискримінаційних висловлювань або незаконних дій. Приклад: у 2023 році генеральний директор однієї з провідних американських технологічних компаній потрапив під удар після публікації у LinkedIn внутрішніх листів, в яких

він зневажливо відгукувався про жінок-інженерів. Кампанія з хештегом #ToxicLeadership зібрала 2,3 мільйона публікацій за 48 годин.

Дезінформаційна атака - цілеспрямоване поширення неправдивої або спотвореної інформації про організацію. Особливо актуально для України: у 2016 році масштабна кампанія у Facebook поширювала фейки про банкрутство ПриватБанку після його націоналізації. Сотні тисяч людей стояли в чергах до банкоматів, а НБУ та банк були змушені цілодобово спростовувати фейки. Джерело: <https://www.epravda.com.ua/news/2016/12/19/614700/>

Соціальний конфлікт або бойкот - організована кампанія незадоволення, пов'язана з ціннісними питаннями: дискримінацією, екологічними проблемами, підтримкою або несхваленням певних соціальних позицій. У 2017 році кампанія #DeleteUber зібрала понад 200 тисяч видалень застосунку за один тиждень після того, як Uber продовжував роботу під час страйку таксистів проти антиімміграційного указу Трампа. Джерело: <https://www.theguardian.com/technology/2017/jan/29/uber-delete-campaign-donald-trump>

Вірусний скандал (Viral Scandal) - несподіване поширення одного відео, фотографії або висловлювання, що викликає масове обурення. Відрізняється від інших тригерів надзвичайною швидкістю: від публікації до глобального поширення може минути менше двох годин.

Регуляторний або правовий інцидент - рішення суду, штраф регулятора, початок розслідування, що стає публічним. Приклад: рішення ірландського регулятора DPC у травні 2023 року оштрафувати Meta на 1,2 мільярда євро за порушення GDPR миттєво породило хвилю публікацій про безпеку персональних даних. Джерело: <https://www.irishexaminer.com/business/arid-41126014.html>

ПРЕВЕНТИВНИЙ КРИЗОВИЙ МЕНЕДЖМЕНТ

Концепція превентивного менеджменту

Традиційне уявлення про кризовий менеджмент зводиться до реагування після того, як криза вже сталася. Сучасна парадигма принципово інша: найкраща криза - та, якої вдалось уникнути або яку було погашено до вибуху.

Превентивний кризовий менеджмент - це сукупність заходів, що знижують ймовірність виникнення кризи та мінімізують її наслідки ще до того, як вона стала публічною.

За оцінкою консалтингової компанії Burson (2023), вкладення 1 долара в превентивний моніторинг та підготовку дає економію в середньому 6 доларів на антикризових витратах. Посилання: <https://burson.com/perspectives/crisis-preparedness-report-2023>

Crisis Playbook: що це і чому він необхідний

Crisis Playbook - це детальний операційний документ, що описує алгоритми дій команди у різних кризових сценаріях. Він розробляється заздалегідь, тестується, затверджується і зберігається у місці, доступному всій кризовій команді. Його наявність - різниця між хаосом та координованою відповіддю.

Структура повноцінного Crisis Playbook включає декілька ключових компонентів. По-перше, реєстр потенційних криз з описом сценарію, ймовірності та потенційного масштабу для кожного типу. По-друге, матрицю відповідальності (RACI): хто відповідає за прийняття рішень (Responsible), хто дає дозвіл (Accountable), хто консультує (Consulted), хто інформується (Informed). По-третє, контактний список кризової команди з ролями, номерами телефонів та протоколом ескалації. По-четверте, готові шаблони першої реакції (Response Templates) для кожного типу кризи - тексти для соцмереж, прес-релізів, email-розсилок. По-п'яте, процедуру моніторингу та пороги активації (Alert Thresholds).

Реальний приклад добре розробленого playbook демонструє авіакомпанія Ryanair. У 2023 році вони опублікували спрощену версію свого кризового протоколу, де розписано 14 типів криз від технічного збою до авіакатастрофи із зазначенням відповідальних осіб та часових стандартів реакції. Після гучного скандалу 2018 року з расистською поведінкою пасажирів, якого відзняли на відео, компанія суттєво вдосконалила свій playbook та зменшила час першої реакції з 4 годин до 25 хвилин. Джерело: <https://www.ryanair.com/ie/en/newsroom/>

2.3. Аналіз вразливостей (Vulnerability Audit)

Перед розробкою Crisis Playbook необхідно провести аналіз вразливостей - систематичну оцінку потенційних джерел кризи для конкретної організації. Методологічно це схоже на SWOT-аналіз, але зосереджений виключно на ризиках репутаційного характеру.

Аналіз вразливостей охоплює кілька вимірів. У вимірі продукту або послуги оцінюються: чи існують відомі дефекти або ризики для безпеки, чи є скарги, що системно ігноруються, чи є прогалини у контролі якості. У вимірі персоналу: чи є публічні особи серед керівництва зі скандальними висловлюваннями в минулому, чи є проблеми корпоративної культури, які можуть стати публічними. У вимірі партнерів та постачальників: чи пов'язані ваші партнери з конкретними ризиками. У вимірі технологій: чи є вразливості в кібербезпеці, які можуть призвести до витоку даних.

Для кожної виявленої вразливості у Crisis Playbook розробляється відповідний сценарій реагування. Наприклад, Nova Poshta, знаючи про потенційні ризики затримок у пікові сезони (передноворічний, 8 березня), заздалегідь готує шаблони відповідей та збільшує ресурси команди моніторингу саме в ці періоди. Джерело: <https://novaposhta.ua/about/press-center>

2.4. Alert System: система сповіщень для кризової команди

Система раннього оповіщення - технічний міст між моніторинговою платформою та кризовою командою. Її завдання - автоматично повідомляти потрібних людей у потрібний момент, щоб не гаяти критично важливий час.

Рівень один, зелений, є нормальним станом, коли кількість згадок знаходиться в межах базового рівня. Він не потребує спеціальних дій. Рівень два, жовтий, фіксується тоді, коли кількість згадок перевищує дворазовий базовий рівень або NSS падає нижче мінус 15 відсотків. Відповідні дії: повідомлення SMM-менеджеру, підвищена частота перевірки до 30 хвилин. Рівень три, помаранчевий, відповідає перевищенню трикратного базового рівня або NSS нижче мінус 25 відсотків. Дії: повідомлення PR-директору, підготовка шаблону відповіді, готовність до публікації. Рівень чотири, червоний, означає кризу:

перевищення п'ятикратного базового рівня, вірусне поширення або загроза здоров'ю. Дії: активація Crisis Playbook, залучення CEO, прес-конференція.

Тригер		Дії
Рівень 1	у межах базового рівня згадок	без спеціальних дій
Рівень 2	згадок > 2х базового або NSS нижче –15%	повідомлення SMM-менеджеру; перевірка кожні 30 хв
Рівень 3	згадок > 3х базового або NSS нижче –25%	повідомлення PR-директору; шаблон відповіді, готовність до публікації
Рівень 4 (криза)	згадок > 5х базового, вірусне поширення або загроза здоров'ю	активація Crisis Playbook; CEO, прес-конференція

Рис. 6.1. Рівні системи сповіщень для кризової команди

Технічно система сповіщень може бути реалізована за допомогою інтеграцій між платформою моніторингу (Brand24, Brandwatch) та Slack, Telegram або SMS. Наприклад, Brand24 дозволяє налаштувати Webhook для автоматичного надсилання сповіщення у корпоративний Telegram-канал кризової команди при досягненні будь-якого порогового значення. Документація Brand24 Webhooks: <https://brand24.com/developers/>

СТРАТЕГІЇ АНТИКРИЗОВОЇ КОМУНІКАЦІЇ

Протокол кризового реагування: від виявлення до вирішення

Незалежно від типу кризи та її масштабу, ефективне реагування будується на єдиній логічній послідовності дій, яку у фаховій літературі позначають як MARC-L: Monitor (Моніторинг), Assess (Оцінка), Respond (Реагування), Correct (Виправлення), Learn (Навчання). Ця послідовність не є механічною - на практиці кроки можуть перекриватись, але їхня внутрішня логіка залишається незмінною.

Крок 1. Monitor - Моніторинг та виявлення (0–15 хвилин)

На цьому кроці завдання - якомога швидше виявити кризу і зрозуміти її початкові контури. Конкретні дії включають перевірку сповіщень системи моніторингу та оцінку Crisis Velocity; визначення джерела (звідки пішов тригерний контент), ключових акторів (хто поширює, хто коментує) та платформ, де розгортається криза; фіксацію початкових даних: час, кількість згадок, перші реакції. Інструменти: Brand24, Brandwatch, Mention, Telegram-моніторинг через Telethon. Усе це має бути виконано за 15 хвилин.

Крок 2. Assess - Оцінка масштабу (15–30 хвилин)

Після виявлення необхідно швидко відповісти на питання: це дійсно криза, чи управоване незадоволення? Оцінюються рівень охоплення (локальне, регіональне, національне, глобальне), швидкість поширення (повільна, швидка, вірусна), тип ризику (репутаційний, правовий, фінансовий), наявність залучення ЗМІ, а також потенційні наслідки для ключових стейкхолдерів: клієнтів, партнерів, інвесторів, регуляторів. На основі оцінки визначається рівень кризи та список осіб, яких необхідно залучити до реагування.

Крок 3. Respond - Реагування (до 60 хвилин від початку кризи)

Перша публічна відповідь є найважливішим елементом кризової комунікації. Дослідження Institute for Crisis Management показало: бренди, що відповіли протягом першої години, у середньому мали на 57% меншу кількість негативних публікацій наступного дня порівняно з тими, хто мовчав довше. Посилання: <https://crisisconsultant.com/icm-reports/>

Перша відповідь не обов'язково має містити всі деталі та рішення - їх часто просто ще немає. Вона має виконати три функції: підтвердити, що організація в курсі ситуації; показати, що нею займаються; дати аудиторії орієнтир, коли очікувати детальнішої інформації. Приклад правильної першої відповіді: «Нам відомо про ситуацію, що виникла з [коротко про подію]. Ми негайно розпочали розслідування та вжиємо всіх необхідних заходів. Детальна інформація буде опублікована протягом [час]. Дякуємо за терпіння та розуміння».

Канали комунікації обираються залежно від платформи, де почалась криза, та аудиторії. Якщо криза почалась у Facebook - першу відповідь публікують там. Якщо це корпоративний інцидент з діловою аудиторією - прес-реліз та LinkedIn.

Якщо криза охопила ЗМІ - офіційний сайт та прес-конференція. На практиці великі компанії реагують одночасно в кількох каналах, але з адаптованими меседжами для кожного.

Крок 4. Correct - Виправлення та вирішення

Цей крок - найтриваліший і найважчий: усунення причини кризи та відновлення довіри. Він включає проведення внутрішнього розслідування та публічне оголошення його результатів (навіть якщо вони не вигідні компанії); запровадження конкретних виправних заходів з чіткими строками та відповідальними; компенсацію постраждалим; регулярні оновлення аудиторії (кожні 2–6 годин в активній фазі). Важливий принцип: повідомляйте про зміни конкретно, а не загально. «Ми збільшили штат служби підтримки на 40 осіб та скоротили час відповіді з 3 годин до 45 хвилин» значно переконливіше, ніж «Ми вживаємо заходів для покращення якості обслуговування».

Крок 5. Learn - Post-crisis аналіз та вдосконалення

Через 2–4 тижні після завершення кризи обов'язково проводиться post-crisis аналіз. Він документує хронологію подій, оцінює ефективність прийнятих рішень, виявляє прогалини в Crisis Playbook та визначає конкретні зміни в процесах. Результат - оновлений Crisis Playbook та підвищена готовність до наступного інциденту. Компанії, що системно проводять post-crisis аналіз, мають у середньому на 40% коротший час реагування при наступній кризі, ніж ті, хто цього не робить.

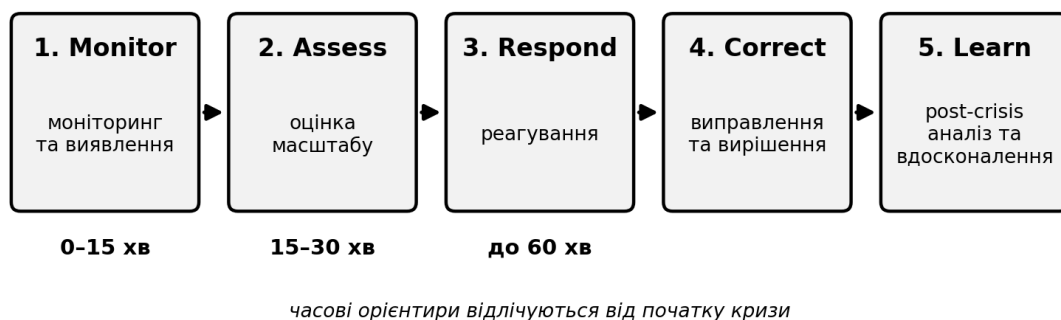


Рис. 6.2. Протокол антикризової комунікації: Monitor – Assess – Respond – Correct – Learn

Tone of Voice під час кризи

Тон комунікації під час кризи є не менш важливим, ніж зміст повідомлення. Три ключові принципи антикризового Tone of Voice - емпатія, прозорість та орієнтація на дію - є практично незмінними незалежно від типу кризи.

Емпатія означає визнання болю та незручностей постраждалих. Перш за все - людське ставлення, а вже потім пояснення та виправдання. Порівняймо дві відповіді: «Ми приносимо вибачення за незручності, що могли виникнути» - холодна, безособова, мінімізує проблему. «Ми розуміємо, наскільки це розчарувало вас, і нам справді шкода» - тепла, визнає реальний досвід клієнта. Нейролінгвістичні дослідження (Simons et al., 2023) показують: аудиторія в 3,4 рази більш схильна простити бренд, якщо перша реакція містила слова, що визнають емоційний стан постраждалих.

Прозорість означає готовність чесно повідомити про те, що сталося, навіть якщо ця правда не вигідна. Аудиторія в епоху соціальних мереж виявляє приховування набагато швидше, ніж корпоративний юрист встигає написати заяву-відмовку. Туманна відповідь без конкретики, як правило, посилює підозри та продовжує кризу. Приклад прозорості комунікації: Kyivstar після кібератаки у грудні 2023 року опублікував детальний технічний звіт про масштаб атаки, уражені системи та вжиті заходи - незважаючи на те, що це розкривало вразливості. Результат: NSS повернувся до докризового рівня протягом 10 днів. Джерело: <https://kyivstar.ua/uk/mm/news/zayava-schodo-kiberataky>

Орієнтація на дію означає, що кожне комунікаційне повідомлення під час кризи повинне містити конкретні дії, строки та відповідальних осіб. Вибачення без плану дій - це слова без зобов'язань. «До 1 лютого ми запровадимо нову систему верифікації замовлень та повністю відшкодуємо витрати всіх постраждалих клієнтів» набагато ефективніше, ніж «Ми вжиємо всіх необхідних заходів».

Чого абсолютно не можна робити під час кризи

Існує низка помилок у кризовій комунікації, які стабільно погіршують ситуацію і про які свідчить практика десятків кейсів.

Мовчання та затримка є першою і найчастішою помилкою. Інформаційний вакуум аудиторія та журналісти заповнюють самостійно - як правило, найгіршими припущеннями. Кожна додаткова година мовчання в активній фазі кризи збільшує кількість негативних публікацій у середньому на 23%, згідно з дослідженням Reputation Institute (2022). Посилання: <https://www.reputationinstitute.com/research>

Заперечення очевидного - друга критична помилка. Якщо факт підтверджений відео або скріншотами, будь-яке заперечення лише підсилює обурення. Найгучніший приклад - перша реакція CEO United Airlines Оскара Муньоса у 2017 році, який написав внутрішній лист у підтримку дій співробітників, не визнаючи нічого неприйнятнього. Коли цей лист витік у пресу, він спровокував другу хвилю скандалу.

Видалення негативних коментарів без пояснення сприймається аудиторією як цензура та приховування. Це неодмінно породжує скріншоти з коментарем “компанія ховає правду” - і публікації з цими скріншотами набирають більше взаємодій, ніж оригінальні.

Звинувачення клієнтів або «третіх осіб» є особливо руйнівним для репутації. Аудиторія завжди на боці постраждалого клієнта. Навіть якщо клієнт частково неправий, публічне звинувачення на адресу постраждалих викликає ефект бумерангу. Дослідження Nielsen (2023) підтверджує: 84% споживачів перестають довіряти бренду, якщо він публічно звинувачує власних клієнтів.

Один пост і тиша - одна з типових помилок середніх компаній. Опублікувавши одну заяву, вони вважають, що цього достатньо. Але аудиторія очікує регулярних оновлень. Відсутність нових повідомлень інтерпретується як байдужість або як те, що ситуація погіршилась.

ОСОБЛИВОСТІ КРИЗОВОЇ КОМУНІКАЦІЇ ДЛЯ РІЗНИХ ТИПІВ КРИЗ ТА АУДИТОРІЙ

Операційні та технічні кризи

Операційна криза - збій сервісу, технічна проблема, затримка доставки - має свою специфіку: аудиторія реально постраждала і очікує насамперед компенсації та відновлення сервісу, а не красивих слів. Комунікаційна стратегія

будується навколо трьох елементів: визнання факту (підтверджуємо, що відбувся збій), статус вирішення у реальному часі (оновлення кожні 1–2 години: що вже зроблено, коли очікується відновлення), конкретна компенсація.

Приклад ефективної комунікації при операційній кризі - Meta під час великого збою у жовтні 2021 року, що залишив Facebook, Instagram та WhatsApp недоступними протягом 6+ годин. Компанія публікувала оновлення на офіційному сайті та через Twitter щогодини, чітко повідомляла про прогрес і вибачилася особисто від CEO. Незважаючи на масштаб збою, NSS відновився протягом 5 днів. Джерело: <https://engineering.fb.com/2021/10/05/networking-traffic/outage-details/>

Скандали з персоналом або керівництвом

Скандали, пов'язані з людьми - найважчі для управління, бо зачіпають цінності, а не лише функціональні очікування. Аудиторія хоче знати не лише «що відбулось», але й «хто несе відповідальність». Стратегія реагування включає швидке дистанціювання компанії від неприйнятної поведінки, конкретні дисциплінарні або кадрові рішення, а в серйозних випадках - публічні зміни в корпоративній культурі чи кодексі поведінки.

Приклад правильної реакції: коли у 2018 році стало відомо про расистський пост менеджера мережі Starbucks у Філадельфії, CEO компанії Кевін Джонсон особисто зустрівся з постраждалими, публічно вибачився та оголосив закриття 8000 кафе на один день для обов'язкового навчання персоналу з расового упередження. Захід охопив 175 000 співробітників і коштував близько 12 мільйонів доларів. NSS повернувся до позитивних значень через 3 тижні. Джерело: <https://www.bbc.com/news/business-43742266>

Дезінформаційні атаки

Реагування на дезінформацію має власну логіку, що відрізняється від інших типів криз. По-перше, категорично не рекомендується повторювати фейк у офіційній заяві навіть для його спростування - це підсилює поширення неправдивої інформації (ефект inoculation за теорією Vaccinationi проти

дезінформації, Lewandowsky & Ecker, 2021). Посилання: <https://doi.org/10.1093/oxfordhb/9780190900809.013.6>

Правильна тактика включає: пряме твердження правди без посилання на фейк («Правда про ситуацію така: [факти з посиланням на джерела]»), мобілізацію надійних третіх сторін - галузевих асоціацій, незалежних експертів, регуляторів, - які підтверджують позицію компанії, а також системне відстеження поширення фейку з метою виявлення його джерела та вжиття юридичних або технічних заходів.

Актуальний приклад з України: після появи в Telegram-каналах фейків про "банкрутство" великого фінтех-стартапу у 2023 році компанія діяла за класичною антидезінформаційною стратегією: опублікувала офіційну фінансову звітність з посиланням на відкриті реєстри, отримала публічне підтвердження від НБУ, залучила фінансових журналістів для незалежного коментаря. Фейк було нейтралізовано за 8 годин.

Комунікація для різних аудиторій під час кризи

Під час кризи одне повідомлення ніколи не підходить для всіх аудиторій. Кожна стейкхолдерська група має власні очікування, канали комунікації та пріоритети.

Клієнти та кінцеві споживачі очікують: чи вирішена проблема, чи отримають вони компенсацію і коли. Канали: соціальні мережі (Instagram/Facebook), push-сповіщення в застосунку, email.

Ділові партнери та постачальники хочуть знати: чи вплине криза на виконання контрактних зобов'язань і якщо так - як саме. Канали: персональні листи від керівництва, телефонні дзвінки ключовим партнерам.

Інвестори та акціонери потребують фінансового виміру: які прямі та опосередковані фінансові наслідки, що робить компанія для мінімізації збитків. Канали: IR-сайт, прес-реліз на фінансових платформах, конференц-дзвінок для аналітиків.

Журналісти та ЗМІ хочуть факти, цифри та доступ до відповідальних осіб. Канали: прес-реліз, прес-конференція, персональні коментарі від PR-директора

або CEO. Важливо: надати журналістам офіційний коментар до публікації їхнього матеріалу, інакше він виходить без позиції компанії.

Регулятори та державні органи очікують повного і своєчасного розкриття інформації відповідно до законодавчих вимог - особливо у сферах фінансів, охорони здоров'я та персональних даних. Канали: офіційні листи, звіти в регуляторні органи.

ВІДНОВЛЕННЯ РЕПУТАЦІЇ ПІСЛЯ КРИЗИ

Чому відновлення репутації є окремою стратегічною задачею

Завершення активної фази кризи не означає відновлення репутації. Дослідження YouGov BrandIndex (2024) фіксує: після кризи, навіть добре управленої, репутаційний індекс бренду залишається нижчим за докризовий рівень у середньому від 6 до 18 місяців. Пошукові системи зберігають негативні публікації роками. Алгоритми рекомендацій продовжують показувати матеріали про кризу новим користувачам. Тому відновлення репутації є окремим проектом з власними цілями, стратегіями та метриками.

Стратегії відновлення репутації

Стратегія 1. Content Rehabilitation. Системне заміщення негативного контенту в пошукових системах і соціальних мережах позитивним або нейтральним. Це не маніпуляція - це правомірне просування якісного контенту про продукти, досягнення, кейси та корпоративну культуру. SEO-оптимізація нових позитивних матеріалів поступово витісняє кризові публікації зі сторінок видачі. Термін: від 3 до 12 місяців залежно від масштабу кризи.

Стратегія 2. Third-Party Validation. Залучення незалежних сторін - галузевих асоціацій, незалежних аудиторів, задоволених клієнтів, авторитетних лідерів думок, журналістів - для підтвердження того, що компанія змінилась. Власні заяви компанії в посткризовий період сприймаються з підвищеним скептицизмом. Слово незалежного експерта або клієнта важить набагато більше.

Стратегія 3. Proof of Change. Публічна демонстрація конкретних системних змін, впроваджених після кризи. Це найпереконливіший аргумент для аудиторії: не слова, а факти. Приклад - Samsung після скандалу з Galaxy Note 7 у 2016 році впровадив нову 8-рівневу систему перевірки безпеки батарей та

опублікував детальний технічний звіт. Прозорий процес відновлення довіри дав змогу компанії повернути лідерство на ринку вже наступного року. Джерело: <https://news.samsung.com/global/samsung-details-galaxy-note7-investigation-results>

Стратегія 4. Community Engagement. Активна взаємодія з аудиторією у соціальних мережах, відповідь на коментарі, участь у діалозі - навіть у складних або критичних темах. Компанія, що продовжує комунікацію після кризи і не закривається у собі, демонструє впевненість та відповідальність.

5.3. Вимірювання відновлення репутації

Відновлення репутації вимірюється за тими самими метриками, що використовувались для оцінки кризи. Серед ключових показників виокремлюють Net Sentiment Score - ціль повернутись до докризового рівня та зафіксувати його стабільність протягом 4+ тижнів. Share of Voice у порівнянні з конкурентами використовується для виявлення частки позитивних згадок серед загального обсягу. Engagement Rate на посткризових публікаціях свідчить про те, чи залучається аудиторія до позитивного контенту. Органічний пошук відображає місця кризових публікацій на сторінках пошукової видачі. Brand Health Score є комплексним індексом, що надають платформи Brand24 та Brandwatch.

Важливо: відновлення вважається досягнутим не тоді, коли NSS повернувся до позитивних значень одного разу, а коли він залишається стабільно позитивним протягом щонайменше 4 послідовних тижнів. Поодинокий позитивний сплеск може бути результатом акції або промо-кампанії, а не реального відновлення репутації.

РЕАЛЬНІ КЕЙСИ: АНАЛІЗ УСПІХІВ І НЕВДАЧ

Кейс успіху: Kyivstar та кібератака (грудень 2023)

У грудні 2023 року Kyivstar зазнав масштабної кібератаки, що залишила без зв'язку понад 24 мільйони абонентів - найбільший збій в Україні з 1991 року. З точки зору антикризової комунікації цей кейс є одним з найкращих прикладів в українській практиці.

Перша реакція вийшла через 45 хвилин після початку масових скарг у соцмережах. Вона підтвердила факт збою та пообіцяла оновлення. Протягом

перших 12 годин Kyivstar публікував оновлення кожні 1–2 години у Twitter/X та Facebook. CEO Олег Кут особисто брав участь у прес-конференції. Kyivstar перший у своїй галузі опублікував детальний технічний звіт про атаку та її наслідки. Компанія оголосила конкретну компенсацію - один день безкоштовного зв'язку для всіх абонентів. NSS повернувся з мінус 65 відсотків (у перші 24 години) до мінус 5 відсотків - майже докризового рівня - за 10 днів. Джерело: <https://kyivstar.ua/uk/mm/news/zayava-schodo-kiberataky>

Кейс невдачі: Pepsi та реклама з Кендалл Дженнер (2017)

У квітні 2017 року Pepsi випустила рекламний ролик, де модель Кендалл Дженнер підходить до поліцейського на протестній акції та подає йому банку Pepsi - після чого всі посміхаються і напруга зникає. Ролик сприйняли як тривіалізацію протестів руху Black Lives Matter та нечутливе використання соціальної напруги у рекламних цілях.

Спочатку Pepsi захищала ролик, стверджуючи, що він «відображає дух єднання». Але реакція аудиторії була однозначною: ролик зібрав 1,6 мільйона негативних коментарів за 48 годин. Хештег #PepsiAd став глобальним трендом з переважно критичним контентом. Після 24 годин захисних заяв Pepsi видалила ролик та вибачилась. Але запізнїла реакція та початковий захист вже завдали репутаційного збитку: NSS Pepsi впав на 27 відсоткових пунктів і залишався негативним протягом трьох місяців. Джерело: <https://www.bbc.com/news/business-39523243>

Ключові уроки кейсу: по-перше, обов'язкова перевірка рекламного контенту на культурну чутливість до публікації - особливо якщо він стосується соціально резонансних тем; по-друге, захист очевидно хибного рішення лише поглиблює кризу і відкладає неминуче вибачення; по-третє, соціальні мережі є не лише каналом кризи, а й каналом попередньої перевірки: тестові фокус-групи в соцмережах могли виявити проблему до публікації.

Кейс з українського контексту: Nova Poshta та затримки під час пандемії (2020)

У 2020 році, під час першого локдауну, Nova Poshta зіткнулась з хвилею скарг у Facebook та Google Maps через різке збільшення часу доставки. Кількість негативних відгуків зросла в 8 разів порівняно з докризовим рівнем. Компанія відреагувала швидко: публічно визнала проблему, пояснила причини (безпрецедентне зростання обсягу відправлень на тлі обмеження персоналу), оперативно відкрила додаткові відділення та запустила систему онлайн-відстеження статусів. NSS стабілізувався протягом двох тижнів. Джерело: <https://novaposhta.ua/about/press-center>

Важливий аспект цього кейсу: компанія не намагалась ні мінімізувати проблему, ні звинувачувати зовнішні обставини - хоча вони справді мали місце. Визнання реального досвіду клієнтів та конкретні операційні рішення виявились ефективнішими, ніж будь-які PR-маневри.

КОНТРОЛЬНІ ПИТАННЯ

1. Назвіть шість стадій розвитку репутаційної кризи в соціальних мережах. Яка з них є найважливішою для своєчасного втручання і чому?
2. У чому полягає концепція превентивного кризового менеджменту? Які три компоненти є обов'язковими у Crisis Playbook?
3. Що таке Vulnerability Audit і для чого він проводиться перед розробкою Crisis Playbook? Наведіть приклад вразливості для конкретного типу організації.
4. Опишіть протокол реагування MARC-L. Який крок є найважливішим та чому?
5. Які три принципи визначають правильний Tone of Voice під час кризи? Для кожного принципу наведіть приклад правильного та неправильного формулювання.
6. Чому видалення негативних коментарів під час кризи є помилкою? Яка стратегія є правильною альтернативою?
7. Чим відрізняється стратегія реагування на дезінформаційну атаку від реагування на операційний збій? Назвіть два ключові відмінності.
8. Що таке Content Rehabilitation і Third-Party Validation як стратегії посткризового відновлення? Наведіть приклад застосування кожної з них.

9. Порівняйте кейси Kyivstar (2023) та Pepsi (2017). Що спільного і що відмінного в їхніх помилках і правильних рішеннях?
10. Як правильно вимірювати відновлення репутації після кризи? Яка метрика є основною і яке значення вважається критерієм успішного відновлення?

ВИСНОВКИ

Перший висновок. Кризовий менеджмент у соціальних мережах - це не реакція на непередбачуване, а системна дисципліна з чіткими алгоритмами, інструментами і стандартами. Організація, що має підготовлений Crisis Playbook і налагоджену систему моніторингу, виходить з кризи в середньому з меншими збитками у 2–3 рази, ніж непередбачена. Перша година після тригерної події вирішує більшість результату: 72% споживачів формують остаточну думку про бренд саме в цей проміжок.

Другий висновок. Три принципи антикризового Tone of Voice - емпатія, прозорість та орієнтація на дію - є незмінними незалежно від типу кризи, галузі та аудиторії. Порушення будь-якого з них - мовчання, заперечення очевидного або загальні обіцянки без конкретики - стабільно погіршує ситуацію. Це підтверджено аналізом сотень кризових кейсів.

Третій висновок. Відновлення репутації після кризи є окремим стратегічним проектом, який триває від 4 до 18 місяців і потребує комплексного підходу: Content Rehabilitation, Third-Party Validation, Proof of Change та Community Engagement. Без активного управління цим процесом репутаційний збиток зберігається роками.

Четвертий висновок. Особливістю кризового менеджменту в Україні є необхідність враховувати специфіку Telegram-каналів як основного майданчика поширення інформаційних криз - особливо в умовах воєнного часу. Жодна комерційна платформа моніторингу не охоплює цей сегмент повноцінно, що робить навичку роботи з open-source інструментами (Telethon) практичною необхідністю.

П'ятий висновок. Матеріал цієї лекції є безпосередньою теоретичною основою для двох лабораторно-практичних робіт: розробки Crisis Playbook для реального або модельного бренду та симуляції антикризового реагування в

реальному часі. Системне розуміння алгоритмів та принципів, викладених у лекції, є обов'язковою умовою їх успішного виконання.

Література

1. 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./ Упоряд.: 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
2. Українські медіа, ставлення та довіра у 2023 р. URL: <https://internews.in.ua/wp-content/uploads/2023/10/Ukrainski-media-stavlennia-ta-dovira-2023r.pdf>
3. Мудрак Л. Комунікація і криза: як громадам протистояти викликам і успішно діяти в період кризи: Посібник <https://cutt.ly/1w0pla9I> (дата звернення: 30.04.2025).
4. Павловський М. Світ і Україна на порозі XXI століття. URL: <https://universum.lviv.ua/magazines/universum/2001/1/dobr.html> (дата звернення: 30.04.2025).
5. 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
6. Мудрак Л. 8 правил кризових комунікацій – поради для місцевого самоврядування. Портал «Децентралізація». URL: <https://decentralization.ua/news/12353>
7. 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>
8. Онлайн-курс Із кризових комунікацій. Освітній портал «Європейський простір». URL: <https://euprostitir.org.ua/courses/149183>

9. Що таке комунікаційна стратегія та як її побудувати? Школа Бізнесу.
URL: <https://online.novaposhta.education/blog/shho-take-komunikacijna-stratehiya-ta-yak-ii-pobuduvati>

10. Сучасні комунікаційні стратегії. Європейська Бізнес Асоціація (European Business Association). URL: <https://eba.com.ua/suchasni-komunikatsijni-strategiyi-shho-novogo/>

11. Демченко О. П'ять помилок, що провокують неякісну комунікацію в бізнесі. Освітній портал Education.ua. URL: <https://www.education.ua/blog/47410/>

12. Коник Д. Кризові комунікації органів місцевого самоврядування : практичний посібник. URL: <https://auc.org.ua/sites/default/files/library/crisis-communications-guide.pdf>

13. 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>

14. 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>

15. Почепцов Г. Сучасні інформаційні війни. Всеукраїнська експертна мережа. URL: http://www.experts.in.ua/baza/analitic/index.php?ELEMENT_ID=112800

16. Кембриджський словник (Cambridge Dictionary). URL: <https://dictionary.cambridge.org/dictionary/english/disinformation>

Лекція 7. ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ МОНІТОРИНГУ СОЦІАЛЬНИХ МЕРЕЖ

ВСТУП.

Попередні лекції заклали комплексний фундамент: ми вивчили природу ризиків у соціальних мережах, опанували методи збору та аналізу даних, інструменти моніторингу - від безкоштовних до enterprise-рішень - та кризовий менеджмент. Однак за кожним запитом до API, кожним зібраним профілем або проаналізованим повідомленням стоять реальні люди - з їхніми правами, очікуваннями на приватність і правовим захистом.

Дана лекція розглядає питання, яке часто залишається поза увагою технічних фахівців: що дозволено і що заборонено робити з даними соціальних мереж? Де закінчується законний моніторинг і починається незаконне стеження? Яка різниця між технічно можливим і етично прийнятним? За даними GDPR Enforcement Tracker (2024), сума штрафів за порушення регуляторних вимог щодо обробки персональних даних у ЄС перевищила 4,5 мільярда євро - і значна частина цих порушень пов'язана саме з некоректним моніторингом онлайн-активності. Посилання: <https://www.enforcementtracker.com/>

Для майбутнього фахівця зі спеціальності «Консолідована інформація» розуміння правових та етичних основ моніторингу є критично важливим з кількох причин.

По-перше, знання правового поля захищає фахівця особисто. Незнання закону не звільняє від відповідальності: аналітик, що збирає дані без підстав або порушує умови використання платформ, несе юридичні ризики нарівні з організацією, яка його найняла.

По-друге, це питання репутації та довіри. Компанії, що використовують методи «harvesting» (масового збору даних) без згоди користувачів, регулярно стають об'єктами скандалів, які ми самі аналізували в попередній лекції. Cambridge Analytica, Clearview AI, численні менші компанії - всі вони технічно «могли» робити те, що робили. Але це не зробило їхні дії законними або прийнятними.

По-третє, в умовах євроінтеграції України та поступового впровадження стандартів GDPR в українське законодавство (через Закон України «Про захист персональних даних»), ця компетентність стає практичною необхідністю для будь-якого фахівця, що працює з даними.

По-четверте, за цією лекцією слідуватиме лабораторна робота, яка передбачає аудит правомірності конкретного сценарію моніторингу та розробку етичного кодексу для системи моніторингу. Без розуміння теоретичних основ, викладених у цій лекції, виконання завдань буде неможливим.

ПЛАН ЛЕКЦІЇ

1. Правове регулювання збору та обробки даних соціальних мереж: міжнародний і національний контекст
2. GDPR та його вплив на моніторинг соціальних мереж: що дозволено, що заборонено, що вимагає згоди
3. Умови використання платформ (ToS): юридичне значення та обмеження для моніторингових систем
4. Етичні основи моніторингу: приватність, пропорційність, прозорість
5. Практичні кейси: правові та етичні порушення у моніторингу соціальних мереж
6. Побудова відповідального моніторингу: Privacy by Design та Ethical AI Framework

ПРАВОВЕ РЕГУЛЮВАННЯ ЗБОРУ ТА ОБРОБКИ ДАНИХ СОЦІАЛЬНИХ МЕРЕЖ

Ландшафт правового регулювання: три рівні

Правове регулювання у сфері обробки даних соціальних мереж функціонує на трьох взаємопов'язаних рівнях: міжнародному, регіональному (насамперед ЄС) та національному. Для фахівця з моніторингу соціальних мереж в Україні актуальними є всі три рівні, оскільки значна частина платформ і даних підпадає під юрисдикцію ЄС, а українське законодавство поступово адаптується до його стандартів.

На міжнародному рівні відправним документом є Конвенція Ради Європи «108+» (Конвенція про захист осіб у зв'язку з автоматизованою обробкою

персональних даних, оновлена редакція 2018 року), яку Україна ратифікувала. Конвенція встановлює базові принципи: законність обробки, цілеспрямованість, пропорційність, безпеку та права суб'єктів даних. Посилання: <https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1>

На рівні ЄС основним інструментом є Загальний регламент про захист даних (GDPR, Regulation (EU) 2016/679), що набрав чинності у травні 2018 року. Попри те, що GDPR є нормативним актом ЄС, його екстериторіальна дія охоплює будь-яку організацію у світі, яка обробляє дані громадян ЄС або надає їм послуги. Це означає, що українська компанія, яка аналізує публікації користувачів з Польщі, Німеччини або Франції, підпадає під вимоги GDPR незалежно від свого місцезнаходження.

На національному рівні в Україні діє Закон «Про захист персональних даних» (2010, з наступними змінами), який встановлює вимоги до обробки персональних даних для організацій та осіб, що здійснюють свою діяльність на території України. Регулятором є Уповноважений Верховної Ради з прав людини. У контексті євроінтеграції Закон поступово гармонізується з GDPR, хоча повна відповідність ще не досягнута. Посилання: <https://zakon.rada.gov.ua/laws/show/2297-17>

Ключові правові поняття для аналітика соціальних мереж

Правильне застосування законодавства про захист даних неможливе без чіткого розуміння базових термінів, які мають конкретне правове значення.

Персональні дані - будь-яка інформація, що стосується ідентифікованої або ідентифікованої фізичної особи. У контексті соціальних мереж це охоплює значно більше, ніж ім'я та email: username, публічна публікація з геолокацією, фотографія, IP-адреса, поведінкові патерни, навіть комбінація непрямих ознак, що дозволяє ідентифікувати особу. Ключова концепція - «можливість ідентифікації»: якщо за допомогою розумних зусиль можна встановити особу, до якої відносяться дані, вони є персональними.

Обробка даних - будь-яка дія або набір дій із персональними даними: збір, реєстрація, організація, структурування, зберігання, адаптація, витяг,

консультування, використання, розкриття, поширення, вирівнювання, комбінування, обмеження, стирання або знищення. Важливо, що пасивний «перегляд» публікацій за допомогою автоматизованих інструментів уже є обробкою, навіть якщо дані не зберігаються.

Підстави для обробки (Legal Basis) - одна з шести підстав, що роблять обробку законною: згода суб'єкта, виконання договору, виконання юридичного зобов'язання, захист життєвих інтересів, виконання завдання в публічних інтересах або законний інтерес контролера (Legitimate Interest). Для комерційного моніторингу соціальних мереж найбільш релевантна підстава - законний інтерес, але він вимагає окремої оцінки та не є «автоматичною» підставою.

Спеціальні категорії даних (раніше «чутливі дані») - інформація про расове або етнічне походження, політичні погляди, релігійні або філософські переконання, профспілкове членство, генетичні, біометричні дані, стан здоров'я, сексуальну орієнтацію. Обробка таких даних заборонена як виняток, якщо немає окремої правової підстави. Аналіз тональності публікацій у поєднанні з ідентифікацією особи може ненавмисно породжувати профілі, що містять спеціальні категорії.

Правовий статус публічних даних у соціальних мережах

Найпоширеніша хибна думка серед аналітиків соціальних мереж: «якщо дані публічні, значить, їх можна використовувати будь-яким чином». Ця думка є юридично помилковою.

Публічність даних не ліквідує права суб'єкта даних. Людина, яка публікує пост у відкритому акаунті Twitter, надає згоду на перегляд цього поста іншими користувачами. Але вона не надає згоди на автоматизований масовий збір, агрегацію в базі даних, продаж третім сторонам або використання для профілювання. Це підтверджено рішенням Суду ЄС у справі Schrems II (2020), яке підкреслило, що контекст збору даних є правово значущим. Посилання: <https://curia.europa.eu/juris/document/document.jsf?docid=228677>

Принцип контекстної цілісності (Contextual Integrity), сформульований правознавцем Ніссенбаум (2004), стверджує: інформація «належить» до певного

соціального контексту, і її переміщення в інший контекст може бути порушенням приватності навіть тоді, коли вона технічно публічна. Публікація у групі «Мама Лівова» є публічною, але її агрегація у базі даних для таргетингу фармацевтичної реклами виходить за межі очікуваного контексту. Посилання: <https://doi.org/10.1086/375574>

Тест на мінімізацію даних вимагає обробляти лише ті дані, які є необхідними для конкретної законної мети. Якщо мета - моніторинг репутації бренду, то обробка повного профілю автора поста - включаючи всю його активність, зв'язки та поведінкові патерни - є непропорційною. Інструменти моніторингу повинні бути налаштовані на збір мінімального обсягу даних, достатнього для досягнення мети.

GDPR ТА ЙОГО ВПЛИВ НА МОНІТОРИНГ СОЦІАЛЬНИХ МЕРЕЖ

Структура GDPR: ключові принципи для аналітика

GDPR містить сім ключових принципів обробки персональних даних (стаття 5), кожен з яких безпосередньо впливає на практику моніторингу соціальних мереж.

Принцип GDPR	Зміст	Застосування у моніторингу СМ
Законність, справедливість, прозорість	Обробка лише на законній підставі, чесно та прозоро	Моніторинг має мати правову підставу (законний інтерес або згода); умови обробки мають бути доступні
Обмеження мети	Збір лише для конкретних, явних та законних цілей	Дані, зібрані для моніторингу бренду, не можна використовувати для профілювання людей
Мінімізація даних	Збирати тільки необхідні дані	Не зберігати повні профілі авторів, якщо потрібен лише текст публікацій
Точність	Дані мають бути точними і актуальними	Регулярне оновлення та видалення застарілих записів про осіб
Обмеження зберігання	Не зберігати довше, ніж потрібно	Визначити строки збереження архівів моніторингу та видаляти після їх закінчення
Цілісність та конфіденційність	Забезпечити безпеку даних	Захищати бази даних з результатами моніторингу від несанкціонованого доступу

Підзвітність	Контролер несе відповідальність за відповідність	Документувати підстави та процедури моніторингу; призначити DPO за необхідності
---------------------	--	---



Рис. 7.1. Сім принципів обробки даних GDPR та їх застосування у моніторингу

Законний інтерес як підстава для моніторингу

У більшості комерційних сценаріїв моніторингу соціальних мереж правовою підставою є «законний інтерес» контролера (Legitimate Interest, стаття 6(1)(f) GDPR). Проте ця підстава не є «універсальною відмовкою» - вона вимагає проходження тристадійного тесту.

Стадія 1. Ідентифікація законного інтересу. Організація повинна визначити конкретний інтерес: моніторинг репутації, виявлення шахрайства, дослідження ринку, забезпечення безпеки. Розпливчасті формулювання на кшталт «знати, що говорять про нас» - недостатні.

Стадія 2. Необхідність обробки. Чи є обробка персональних даних необхідною для досягнення цього інтересу? Чи існує менш інвазивний спосіб досягти тієї ж мети? Якщо мета - дізнатися, що кажуть про бренд, аналіз анонімізованого тексту публікацій може бути достатнім без збору даних про авторів.

Стадія 3. Балансування інтересів (Balancing Test). Чи переважають інтереси контролера над правами та свободами суб'єктів даних? Враховуються характер даних, очікування суб'єктів, масштаб обробки та потенційні ризики. Масовий збір та зберігання даних мільйонів користувачів без їхнього відома навряд чи пройде балансування.

Важливий нюанс: суб'єкти даних мають право заперечити проти обробки на підставі законного інтересу (Право на заперечення, стаття 21 GDPR). Організація зобов'язана розглянути таке заперечення і припинити обробку, якщо не може довести переважаючі законні підстави.

Права суб'єктів даних, що релевантні для моніторингу

GDPR надає суб'єктам даних комплекс прав, що безпосередньо впливають на практику моніторингу. Аналітик повинен розуміти ці права, щоб організація могла на них реагувати.

Право на доступ (стаття 15) дозволяє особі отримати підтвердження того, чи обробляються її дані, і доступ до цих даних. Якщо система моніторингу зберігає профіль конкретної особи, вона може запитати: «Які мої дані ви обробляєте?» - і організація зобов'язана відповісти протягом одного місяця.

Право на стирання («право на забуття», стаття 17) дозволяє особі вимагати видалення своїх даних за певних умов: якщо вони більше не потрібні для мети збору, якщо відкликана згода, або якщо обробка була незаконною. Системи моніторингу повинні мати технічну можливість ідентифікувати та видалити записи про конкретну особу.

Право на заперечення (стаття 21) - як зазначено вище, особа може заперечити проти обробки на підставі законного інтересу. Відмова розглянути таке заперечення є порушенням GDPR.

Право не бути об'єктом автоматизованого прийняття рішень (стаття 22) особливо актуальне для систем, що використовують AI для профілювання осіб або автоматизованого прийняття рішень з правовими або подібно значущими наслідками. Системи sentiment analysis та автоматична категоризація осіб за поведінковими патернами підпадають під цю статтю.

Штрафні санкції та правозастосування

GDPR передбачає два рівні санкцій: до 10 мільйонів євро або 2% річного глобального обороту за менш серйозні порушення; до 20 мільйонів євро або 4% річного глобального обороту за серйозні порушення, включаючи порушення основних принципів та прав суб'єктів даних. Обирається більша сума.

Наочний приклад правозастосування: у 2023 році ірландський регулятор DPC оштрафував Meta на 1,2 мільярда євро за незаконну передачу персональних даних громадян ЄС до США - найбільший штраф у історії GDPR на той момент. Для порівняння: британська компанія Clearview AI отримала штраф на 7,5 мільйона фунтів від ICO (2022) за незаконне збирання мільярдів фотографій з соціальних мереж без відома або дозволу осіб.

УМОВИ ВИКОРИСТАННЯ ПЛАТФОРМ (ToS): ЮРИДИЧНЕ ЗНАЧЕННЯ ТА ОБМЕЖЕННЯ

Що таке Terms of Service і чому вони мають значення

Terms of Service (ToS) або Terms of Use - це договір між платформою та її користувачами, а також між платформою та розробниками, які використовують її API або дані. Для аналітика соціальних мереж ToS є юридично обов'язковим документом, порушення якого може мати наслідки від блокування акаунту до судового позову.

Більшість великих платформ забороняють або обмежують автоматизований збір даних без дозволу. Twitter/X Developer Agreement (2023) забороняє використання API для масового збору даних із метою навчання AI-моделей без окремої ліцензії. Facebook Platform Terms (2024) забороняє збирати дані користувачів у спосіб, що виходить за межі дозволеного функціоналу платформи. LinkedIn User Agreement забороняє scraping навіть публічних профілів без письмового дозволу. Посилання: <https://twitter.com/en/tos>, <https://developers.facebook.com/terms/>, <https://www.linkedin.com/legal/user-agreement>

Прецедентне значення має справа LinkedIn Corp. v. hiQ Labs, Inc. (США, 2022), де Верховний суд США повернув справу до нижчих інстанцій без остаточного вирішення, але апеляційний суд 9-го округу постановив, що scraping

публічних даних не порушує Закону про комп'ютерне шахрайство і зловживання (CFAA). Проте це рішення стосується лише публічних даних і лише в контексті CFAA - воно не звільняє від відповідальності за порушення ToS чи GDPR. Джерело: <https://cdn.ca9.uscourts.gov/datastore/opinions/2022/04/18/17-16783.pdf>

Офіційні API vs scraping: правові та технічні відмінності

Ключова розвилка у практиці моніторингу соціальних мереж - спосіб отримання даних: через офіційний API платформи або через технічне збирання (web scraping). Ця відмінність має суттєві правові, технічні та етичні наслідки.

Критерій	Офіційний API	Web Scraping
Правовий статус	Дозволений контрактом з платформою	Заборонений більшістю ToS, потенційно незаконний
Обсяг даних	Обмежений ліцензійним рівнем; безкоштовні рівні значно скорочені з 2023 р.	Технічно необмежений, але незаконний понад дозволений обсяг
Надійність	Висока, структуровані дані JSON/XML	Нестабільна, залежить від структури HTML, яка змінюється
Риски	Зміна умов API може обмежити доступ; платні рівні коштовні	Блокування IP, судові позови, штрафи за GDPR
Рекомендація	✓ Завжди використовувати офіційний API	✗ Уникати без окремого юридичного висновку

Слід враховувати, що платформи суттєво змінили свою API-політику у 2022–2024 роках. Twitter/X з 2023 року перейшов на повністю платний API, суттєво скоротивши можливості для академічних та некомерційних досліджень. Reddit закрити безкоштовний API у 2023 році. Це обмеження є важливим практичним чинником при проектуванні систем моніторингу.

Telegram і особливості правового статусу в Україні

Як зазначалося у попередніх лекціях, Telegram відіграє особливу роль в українському інформаційному просторі - особливо у контексті воєнного часу. Правовий статус моніторингу Telegram має свою специфіку.

Telegram не надає офіційного API для моніторингу публічних каналів у тому ж обсязі, що Twitter або Facebook. MTProto API (офіційний API Telegram)

призначений для розробки клієнтських застосунків, а не для масового збору даних. Використання Telethon або аналогічних бібліотек для збору повідомлень з Telegram-каналів технічно суперечить ToS платформи, хоча правозастосування цих обмежень Telegram здійснює непослідовно.

З правової точки зору GDPR поширюється на дані користувачів Telegram, якщо вони є громадянами ЄС або знаходяться в ЄС. Збір даних із приватних каналів або закритих груп є однозначним порушенням як ToS, так і GDPR. Збір даних із публічних каналів знаходиться у «сірій зоні», але все одно вимагає правового обґрунтування, мінімізації даних та обмеження мети.

ЕТИЧНІ ОСНОВИ МОНІТОРИНГУ: ПРИВАТНІСТЬ, ПРОПОРЦІЙНІСТЬ, ПРОЗОРИСТЬ

Чому право недостатнє: етичний вимір

Правове регулювання встановлює мінімальні вимоги - те, що заборонено робити. Але між «не заборонено» і «правильно» існує великий простір, де визначальну роль відіграє професійна етика. Численні скандали у сфері даних виникали не тоді, коли порушувалося законодавство, а коли компанії та дослідники робили те, що було технічно законним, але глибоко неетичним.

Класичний приклад: дослідження Facebook «Emotional Contagion» (2014), де алгоритми платформи маніпулювали емоційним станом 689 000 користувачів без їхнього відома, впливаючи на зміст їхніх стрічок. Технічно це не порушувало ToS та діюче законодавство США. Але громадська реакція була настільки негативною, що змусила Facebook публічно вибачитися та змінити процедури досліджень. Джерело: <https://www.pnas.org/doi/10.1073/pnas.1320040111>

Для аналітика соціальних мереж три базові етичні принципи є практичними орієнтирами при проектуванні та здійсненні моніторингу.

Принцип поваги до приватності

Приватність - це не лише юридична вимога, а фундаментальне право людини (стаття 8 Хартії основних прав ЄС, стаття 17 Конституції України). У контексті моніторингу соціальних мереж це означає ставлення до кожного

публічного профілю та публікації не як до «даних», а як до вираження особистості конкретної людини, яка має право на контроль над своїм цифровим образом.

Практично це виявляється у кількох правилах. Перше: не збирати більше, ніж потрібно. Якщо мета - моніторинг настроїв навколо бренду, збір повних профілів авторів є надмірним. Друге: анонімізувати де можливо. Перед зберіганням та аналізом замінювати ідентифікатори осіб (usernames, ID) хешами або видаляти їх, якщо конкретна особа не є предметом дослідження. Третє: не агрегувати дані для неочевидних цілей. Комбінування публічних даних із різних джерел для побудови детального профілю приватної особи є порушенням принципу приватності навіть без збирання закритої інформації.

Принцип пропорційності

Пропорційність вимагає, щоб обсяг та інвазивність моніторингу відповідали його меті. Моніторинг публічних згадок бренду - пропорційна практика для бізнесу. Систематичне відстеження активності конкретних приватних осіб - вже ні.

Тест на пропорційність включає чотири питання. Перше - чи є мета моніторингу законною і суспільно виправданою? Друге - чи є обраний метод найменш інвазивним з тих, що дозволять досягти мети? Третє - чи є потенційна шкода для суб'єктів даних пропорційною користі від моніторингу? Четверте - чи є заходи захисту даних адекватними ризикам?

Особливо гострим є питання пропорційності у контексті моніторингу журналістів, активістів, опозиційних діячів або звичайних громадян. Навіть якщо окремі публікації таких осіб є публічними, систематичний збір інформації про них без законної підстави є порушенням їхніх прав. В Україні це питання набуває особливої ваги в умовах конфлікту, де моніторинг може використовуватись як інструмент цілеспрямованого переслідування.

Моніторинг працівників у соціальних мережах: особлива зона ризику

Окремої уваги вимагає моніторинг соціальних мереж власних працівників або кандидатів на посади - практика, що набула поширення у HR-процесах. З правової точки зору такий моніторинг є особливо ризикованим.

По-перше, збір інформації про кандидатів із соціальних мереж може розкрити спеціальні категорії даних (расова приналежність, релігія, стан здоров'я, сексуальна орієнтація), що є забороненою підставою для прийняття рішень про найм у більшості юрисдикцій.

По-друге, Директива ЄС про умови праці та ряд рішень DPA вимагають, щоб роботодавці повідомляли працівників про будь-який моніторинг їхньої діяльності - включаючи аналіз публічних акаунтів, пов'язаних з ними.

По-третє, рішення про найм або звільнення, що ґрунтуються на автоматизованому аналізі соціальних мереж без участі людини в прийнятті рішення, можуть порушувати статтю 22 GDPR (заборона автоматизованого прийняття рішень).

ПРАКТИЧНІ КЕЙСИ: ПРАВОВІ ТА ЕТИЧНІ ПОРУШЕННЯ У МОНІТОРИНГУ

Кейс Clearview AI: масовий збір біометричних даних

Clearview AI - американська компанія, що зібрала понад 10 мільярдів зображень облич людей з соціальних мереж, веб-сайтів та публічних джерел для побудови системи розпізнавання облич, яку вона продавала правоохоронним органам та приватним компаніям.

Clearview AI грубо порушила кілька правових та етичних норм. З точки зору права: масовий збір фотографій без згоди є обробкою біометричних даних (спеціальна категорія за GDPR); збір здійснювався без правової підстави та в порушення ToS всіх задіяних платформ. Наслідки: штрафи від регуляторів ЄС на суму понад 50 мільйонів євро, канадський Privacy Commissioner визнав діяльність компанії незаконною, у 2022 році ICO Великобританії видав штраф на 7,5 мільйона фунтів. Джерело: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-clearview-ai-inc-more-than-7-5million-and-orders-uk-data-deleted/>

Урок для аналітика: масовий збір публічних фотографій є обробкою біометричних даних - навіть якщо зображення були публічними. Технічна можливість «зробити щось» не означає правової або етичної допустимості.

Кейс Cambridge Analytica: профілювання без згоди

У 2018 році стало відомо, що Cambridge Analytica збрала дані 87 мільйонів профілів Facebook без відома та згоди їхніх власників - через додаток «Thisisyourdigitallife», що збирав дані не лише тих, хто встановив додаток, але й їхніх друзів. Ці дані використовувались для мікротаргетингу виборців під час президентських виборів у США 2016 року та референдуму Brexit.

Ключові порушення: збір даних без законної правової підстави; передача даних третій стороні (Cambridge Analytica) без відома суб'єктів; використання даних для цілей, що кардинально відрізнялись від тих, для яких вони збирались (соціальна гра vs. політичне профілювання). Наслідки: Facebook оштрафований FTC США на 5 мільярдів доларів; Cambridge Analytica ліквідована. Джерело: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>

Урок для аналітика: принцип обмеження мети є критичним. Дані, зібрані для однієї мети, не можуть використовуватися для іншої без нової правової підстави та (як правило) нової згоди.

Кейс з моніторингом протестів в Україні (2013-2014)

У період Євромайдану правоохоронні органи використовували дані соціальних мереж для ідентифікації учасників протестів. Мобільні оператори надавали геолокаційні дані абонентів до правоохоронних органів без судового дозволу. Активістів ідентифікували за публікаціями у VKontakte та Facebook.

Цей кейс ілюструє декілька важливих аспектів. По-перше, дані соціальних мереж у поєднанні з іншими джерелами (телефонні записи, відео) утворюють надзвичайно потужний інструмент масового стеження. По-друге, «публічна» публікація про участь у протесті може стати підставою для переслідування в авторитарному або перехідному суспільстві. По-третє, комерційні інструменти

моніторингу соціальних мереж можуть використовуватись не за призначенням - для контролю над громадянами замість управління репутацією бренду.

Урок для аналітика: розуміти кінцеве використання систем та даних, які ти будуєш і обслуговуєш - це не лише технічна, а й моральна відповідальність.

Кейс з корпоративним шпигунством у Telegram-каналах (Україна, 2021-2023)

Кілька корпоративних скандалів в Україні показали практику «корпоративної розвідки»: компанії замовляли моніторинг конкурентів, включаючи закриті Telegram-групи співробітників. У деяких випадках агентства навмисно впроваджувались до цих груп для збору інформації.

Такі практики порушують одразу кілька правових норм: Закон України «Про захист персональних даних» (незаконна обробка); статті Кримінального кодексу України про порушення таємниці листування та несанкціонований доступ до комп'ютерних систем (статті 163, 361); принцип добросовісної конкуренції відповідно до Закону «Про захист від недобросовісної конкуренції».

ПОБУДОВА ВІДПОВІДАЛЬНОГО МОНІТОРИНГУ: PRIVACY BY DESIGN TA ETHICAL AI FRAMEWORK

Privacy by Design: сім принципів

Концепція Privacy by Design (PbD), розроблена Анн Каворкян та закріплена у статті 25 GDPR, передбачає, що захист приватності має бути вбудований у систему від самого початку проектування, а не додаватись як «нашлепка» після завершення розробки. Для систем моніторингу соціальних мереж це означає наступне.

Перший принцип: проактивний, а не реактивний. Передбачати проблеми приватності до їх виникнення. Перед запуском моніторингу провести Privacy Impact Assessment (PIA).

Другий принцип: приватність як налаштування за замовчуванням. Максимальний захист приватності без додаткових дій. Наприклад: за замовчуванням не зберігати ідентифікатори авторів; видаляти дані після досягнення мети.

Третій принцип: вбудованість у дизайн. Технічна архітектура повинна підтримувати принципи приватності. Де можливо - анонімізація або псевдонімізація на рівні збору, а не постобробки.

Четвертий принцип: повна функціональність. Захист приватності не повинен знижувати функціональність системи. Треба знайти рішення, що забезпечить і ефективний моніторинг, і повагу до даних.

П'ятий принцип: безпека наскрізь. Захист даних упродовж всього циклу - від збору до видалення. Шифрування при зберіганні та передачі, суворий контроль доступу.

Шостий принцип: видимість та прозорість. Документувати та публікувати практики обробки. Забезпечити доступ суб'єктів даних до інформації про обробку.

Сьомий принцип: повага до користувача. Проектувати систему, виходячи з інтересів суб'єктів даних, а не лише з інтересів організації.

Ethical AI Framework для систем аналізу соціальних мереж

Із поширенням AI-інструментів для аналізу тональності, профілювання та прогнозування поведінки у системах моніторингу виникає необхідність у специфічних етичних рамках для AI-компонентів.

EU AI Act (2024) класифікує системи AI за рівнем ризику. Системи аналізу соціальних мереж для оцінки особистості або поведінки людей відносяться до «високого ризику» або «недозволеного ризику» (якщо використовуються для «social scoring»). Навіть якщо система формально не підпадає під регулювання AI Act, Ethical AI Framework визначає сім ключових вимог. Перша - Human Oversight: рішення, що впливають на людей, не можуть прийматися виключно AI. Друга - Fairness: моделі не повинні демонструвати упередженість за ознаками статі, раси, релігії. Третя - Transparency: можливість пояснити, чому система прийняла конкретне рішення. Четверта - Accountability: визначена відповідальність за рішення системи. П'ята - Privacy: дотримання GDPR та мінімізація даних. Шоста - Security: захист від маніпуляцій та атак. Сьома - Non-

maleficence: не заподіювати шкоди. Джерело: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Практичний чеклист відповідального моніторингу

На основі матеріалу цієї лекції аналітик перед запуском будь-якої системи моніторингу соціальних мереж повинен відповісти на такий перелік питань.

Питання для перевірки	Так / Потрібна дія	Примітка
Чи визначена законна правова підстава для обробки (GDPR, ст. 6)?		Законний інтерес або згода
Чи пройдений тест балансування для законного інтересу?		
Чи дотримується принцип мінімізації даних?		Лише необхідні дані
Чи визначені строки зберігання та механізм видалення?		
Чи є технічна можливість реалізувати права суб'єктів (доступ, стирання)?		
Чи використовується офіційний API (а не scraping)?		
Чи проведена Privacy Impact Assessment?		Обов'язково для масового збору
Чи задокументовані підстави та процедури в Privacy Notice?		
Чи не збираються спеціальні категорії даних без окремої підстави?		Стаття 9 GDPR
Чи є Human Oversight для AI-компонентів, що стосуються людей?		

КОНТРОЛЬНІ ПИТАННЯ

1. Поясніть концепцію екстериторіальної дії GDPR. Чому українська компанія, що моніторить публікації польських користувачів, підпадає під GDPR?

2. У чому різниця між «публічними даними» та «дані, які можна вільно використовувати будь-яким чином»? Наведіть приклад порушення принципу контекстної цілісності.

3. Опишіть тристадійний тест для законного інтересу як правової підстави обробки даних. Наведіть приклад сценарію моніторингу, що пройде цей тест, і сценарію, що не пройде.

4. Які права суб'єктів даних є найбільш релевантними для систем моніторингу соціальних мереж? Як технічно забезпечити їх реалізацію?

5. Чим відрізняються юридичні наслідки використання офіційного API від web scraping? Що говорить справа hiQ Labs v. LinkedIn про правовий статус scraping публічних даних?

6. Поясніть принцип Privacy by Design. Як він змінює підхід до розробки системи моніторингу порівняно з традиційним підходом «додати захист після розробки»?

7. Чому моніторинг Telegram-каналів знаходиться у правовій «сірій зоні»? Які умови необхідні, щоб такий моніторинг був правомірним?

8. Проаналізуйте кейс Cambridge Analytica з точки зору принципів GDPR. Які конкретні принципи та статті були порушені?

9. Що таке Privacy Impact Assessment і в яких випадках вона є обов'язковою? Які компоненти вона повинна включати?

10. Чому моніторинг соціальних мереж кандидатів на посаду є особливо ризикованим з правової точки зору? Якими нормами він регулюється?

ВИСНОВКИ

Правове регулювання моніторингу соціальних мереж є багаторівневим і охоплює міжнародні конвенції, GDPR та національне законодавство. Для практики важливо усвідомлювати екстериторіальний характер GDPR: якщо дані стосуються громадян ЄС, GDPR застосовується незалежно від місцезнаходження організації. Незнання цих вимог не звільняє від відповідальності, а штрафи можуть досягати 4% від глобального обороту.

«Публічність» даних у соціальних мережах не означає їх необмеженої доступності для будь-якого використання. Принцип контекстної цілісності вимагає враховувати контекст, у якому дані були оприлюднені. Масовий автоматизований збір, агрегація та профілювання - це принципово інші дії, ніж читання публічних постів, і вони вимагають окремої правової підстави.

Офіційний API є єдиним законним і технічно надійним способом збору даних соціальних мереж у масштабі. Web scraping суперечить ToS практично всіх великих платформ, несе суттєві правові ризики та є технічно ненадійним. Обмеження API, що запровадили платформи у 2022-2024 роках, є практичним викликом, але не підставою для переходу до незаконних методів.

Право - мінімальний стандарт. Між «не заборонено» і «правильно» існує великий простір, де визначає професійна етика. Три базові етичних принципи - повага до приватності, пропорційність та прозорість - є практичними орієнтирами, що допомагають будувати системи моніторингу, які суспільство може довіряти. Privacy by Design перетворює ці принципи на конкретну технічну архітектуру.

Матеріал цієї лекції є безпосередньою теоретичною основою для лабораторної роботи, що передбачає проведення правового та етичного аудиту конкретного сценарію моніторингу та розробку Ethical Monitoring Charter для модельної організації. Розуміння принципів, викладених у лекції, є обов'язковою умовою якісного виконання завдань.

Література

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 (зі змінами). 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://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

Наукова та навчальна література

1. Малюга Л.Ю., Шкрібляк К.П. Особливості захисту персональних даних у процесі цифровізації трудових відносин в Україні: теоретико-правовий аналіз. Науковий вісник Ужгородського національного університету. Серія

Право. 2025. № 91. ч. 2. с. 114-120. URL: <https://doi.org/10.24144/2307-3322.2025.91.2.14>

2. 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>