МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ
ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Д'яков А.В., Зачек О.І., Магеровська Т.В., Мусійовська М.М.

ПРОТИДІЯ ТОРГІВЛІ ЛЮДЬМИ, ЯКА ЗДІЙСНЮЄТЬСЯ З ВИКОРИСТАННЯМ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Монографія

2026

УДК 343.9:004.9:343.431
П 83

Рекомендовано до друку Вченою Радою
Львівського державного університету внутрішніх справ
(протокол №___ від_____2026 р.)

Рецензенти:

Сеник В.В. - доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка», кандидат технічних наук, доцент

Рудий Т.В. - доцент кафедри інформаційних технологій ЛьвДУВС, кандидат технічних наук, доцент

Авторський колектив:

Д'яков А.В. – кандидат технічних наук, доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ (розділи 1-5);

Зачек О.І. – кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка» (передмова, розділ 6, бібліографічний опис, перелік умовних скорочень, висновки, загальна редакція);

Магеровська Т.В. – кандидат фізико-математичних наук, доцент, доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ, доцент кафедри обчислювальної математики та програмування Національного університету «Львівська політехніка» (розділ 7);

Мусійовська М.М. – кандидат технічних наук, доцент кафедри інформаційних технологій Львівського державного університету внутрішніх справ (розділ 8).

П 83 Протидія торгівлі людьми, яка здійснюється з використанням сучасних інформаційних технологій : монографія / А. В. Д'яков, О. І. Зачек, Т. В. Магеровська, М.М. Мусійовська; за редакцією О. І. Зачека. Львів: ЛьвДУВС, 2026. 363 с.

У монографії розглянуто теоретико-правові, інформаційно-аналітичні, кримінологічні та організаційно-технологічні засади протидії торгівлі людьми з використанням сучасних інформаційних технологій. Висвітлено можливості OSINT, аналізу великих даних, геоінформаційних технологій і штучного інтелекту, запропоновано підходи до інтеграції аналітичних інструментів, цифрової профілактики, захисту постраждалих осіб та оцінювання ефективності цифрових рішень. Видання може бути корисними науковцям, викладачам, здобувачам вищої освіти та фахівцям, які досліджують або застосовують інформаційно-аналітичні технології у правоохоронній діяльності.

The monograph examines the theoretical, legal, analytical, criminological, and organizational-technological foundations of combating human trafficking through modern information technologies. It explores the application of OSINT, big data analytics, geographic information systems, and artificial intelligence, and presents approaches to analytical integration, digital prevention, victim protection, and the evaluation of digital technologies' effectiveness. The publication may be useful to researchers, lecturers, higher education students, and specialists who study or apply information and analytical technologies in law enforcement.

ЗМІСТ

Перелік умовних скорочень.....12
ПЕРЕДМОВА.....15
РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ.....18
1.1. Визначення та динаміка розвитку явища торгівлі людьми.....18
1.2. Нормативно-правова база України та міжнародні стандарти.....19
1.3. Роль цифрових технологій у правозастосуванні.....21
Висновок до розділу 1.....23
РОЗДІЛ 2. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ВИЯВЛЕННІ ТОРГІВЛІ ЛЮДЬМИ.....25
2.1. Використання OSINT (open-source intelligence).....25
2.1.1. Джерела та сигнали.....25
2.1.2. Законність, етика, безпека.....29
2.1.3. Збирання та нормалізація.....32
2.1.4. Текстова аналітика.....32
2.1.5. Аналіз зображень та відео.....33
2.1.6. Графовий OSINT.....33
2.1.7. ГеоOSINT і просторовий аналіз.....34
2.1.8. Документування результатів.....34
2.1.9. Типові ризики й помилки.....35
2.2. Аналітика великих даних (Big Data) для виявлення підозрілих патернів.....36
2.2.1. Архітектура даних.....36
2.2.2. Якість і управління даними.....38
2.2.3. Аналітичні патерни.....39
2.2.4. Візуалізація й інструменти диспетчера.....42
2.2.5. Приклади запитів/обчислень.....48
2.3. Машинне навчання та штучний інтелект у виявленні торгівлі людьми.....50
2.3.1. Класифікація текстових повідомлень.....50
2.3.2. Виявлення аномалій у даних.....52
2.3.3. Кластеризація користувачів і оголошень.....55
Висновок до розділу 2.....57

РОЗДІЛ 3. КІБЕРБЕЗПЕКОВІ АСПЕКТИ ДОКУМЕНТУВАННЯ ТОРГІВЛІ ЛЮДЬМИ.....60
3.1. Цифрова криміналістика у розслідуванні торгівлі людьми.....60
3.2. Захист цифрових доказів у справах торгівлі людьми.....64
3.3. Виявлення фальсифікацій та протидія маніпуляціям.....68
3.3.1. Фальсифікація візуальних матеріалів.....68
3.3.2. Маніпуляції текстовими даними.....69
3.3.3. Протидія фальсифікаціям.....69
3.3.4. Практичні приклади.....69
3.4. Правові й етичні вимоги при документуванні торгівлі людьми.....70
3.4.1. Міжнародні правові стандарти.....70
3.4.2. Національні вимоги України.....71
3.4.3. Етичні принципи документування.....71
3.4.4. Виклики й ризики.....73
3.4.5. Практичне значення правових та етичних вимог.....74
Висновок до розділу 3.....75
РОЗДІЛ 4 ПРАКТИЧНІ КЕЙСИ ТА ПІЛОТНІ РЕАЛІЗАЦІЇ.....78
4.1. Загальна характеристика підходу.....78
4.1.1. Логіка впровадження пілотних кейсів.....78
4.1.2. Компоненти підходу.....79
4.1.3. Методологічні принципи.....81
4.1.4. Очікувані результати.....83
4.1.5. Візуалізаційна складова.....84
4.2. OSINT-кейс: виявлення мережі оголошень про «роботу за кордоном».....86
4.2.1. Постановка завдання.....86
4.2.2. Аналіз текстів оголошень.....86
4.2.3. Виявлення повторів контактних даних.....87
4.2.4. Аналіз візуальних матеріалів.....88
4.2.5. Графовий аналіз зв’язків.....89
4.2.6. Інтегрований результат і практичне значення.....90
4.3. GIS-кейс: просторовий аналіз «гарячих точок».....91
4.3.1. Обґрунтування завдання.....91
4.3.2. Вихідні дані.....91
4.3.3. Методологія.....92

4.3.4. Результати модельного аналізу.....92
4.3.5. Ілюстративні матеріали.....93
4.3.6. Практичне значення.....95
4.3.7. Висновки.....95
4.4. Big Data-кейс: інтеграція різнорідних даних.....96
4.4.1. Постановка завдання.....96
4.4.2. Архітектура Lakehouse.....96
4.4.3. Методи обробки.....98
4.4.4. Результати модельної апробації.....100
4.4.5. Практичне значення.....100
4.5. ML-кейс: виявлення аномалій у транзакціях.....101
4.5.1. Постановка завдання.....101
4.5.2. Характеристика даних.....102
4.5.3. Методи виявлення аномалій.....102
4.5.4. Результати аналізу.....104
4.5.5. Інтеграція у систему моніторингу.....105
4.5.6. Практичне значення.....105
Висновок до розділу 4.....106
РОЗДІЛ 5. ПЕРСПЕКТИВИ РОЗВИТКУ ТА ІНТЕГРАЦІЯ В НАЦІОНАЛЬНУ СИСТЕМУ БЕЗПЕКИ.....109
5.1. Необхідність інтеграції результатів у державну політику.....109
5.1.1. Передумови.....109
5.1.2. Основні напрями інтеграції.....110
5.1.3. Правові та стратегічні засади.....111
5.1.4. Організаційні умови та обмеження.....112
5.1.5. Очікуваний ефект інтеграції.....113
5.1.6. Висновки.....114
5.2. Технічні перспективи розвитку.....115
5.2.1. Розвиток Data Lakehouse як інтеграційного ядра.....115
5.2.2. Розвиток засобів штучного інтелекту та машинного навчання 116
5.2.3. Розвиток GIS-компонента.....118
5.2.4. Кіберзахист і стійкість платформи.....119
5.2.5. Інтероперабельність та API.....121
5.2.6. Хмарні та контейнерні технології.....121

5.2.7. Висновки.....122
5.3. Організаційні аспекти впровадження.....122
5.3.1. Міжвідомча координація.....123
5.3.2. Розподіл ролей і відповідальності.....123
5.3.3. Кадрове забезпечення.....123
5.3.4. Правові та етичні умови.....124
5.3.5. Очікуваний результат організаційного впровадження.....124
5.4. Міжнародна співпраця та інтеграція.....125
5.4.1. Необхідність міжнародної інтеграції.....125
5.4.2. Основні напрями міжнародної співпраці.....125
5.4.3. Технічні принципи інтеграції.....126
5.4.4. Очікуваний ефект.....126
5.4.5. Модель міжнародної інтеграції.....127
5.5. Перспективи для науки та освіти.....128
5.5.1. Формування професійних компетентностей.....128
5.5.2. Освітня складова.....128
5.5.3. Перспективні напрями наукових досліджень.....129
5.5.4. Очікуваний результат.....129
5.6. Етичні та правові аспекти розвитку платформи.....130
5.6.1. Правові основи.....130
5.6.2. Основні етичні ризики.....130
5.6.3. Практичні механізми захисту.....131
5.6.4. Баланс ефективності та прав людини.....131
5.6.5. Багаторівнева модель Data Governance.....131
Висновки до розділу 5.....132
РОЗДІЛ 6. КРИМІНОЛОГІЧНИЙ АНАЛІЗ ТА МОДЕЛЮВАННЯ РИЗИКІВ ТОРГІВЛІ ЛЮДЬМИ В ЦИФРОВОМУ СЕРЕДОВИЩІ.....135
6.1. Кримінологічна характеристика сучасної торгівлі людьми.....135
6.1.1. Основні форми та способи вчинення торгівлі людьми.....136
6.1.2. Суб’єкти та структура злочинної діяльності.....138
6.1.3. Типові моделі вербування, переміщення та експлуатації.....140
6.1.4. Транснаціональний характер злочинних мереж.....141
6.1.5. Цифрова трансформація механізмів торгівлі людьми.....143
6.2. Фактори та індикатори ризику.....145
6.2.1. Соціально–економічні фактори.....146

6.2.2. Міграційні та геополітичні фактори.....148
6.2.3. Цифрові фактори ризику.....149
6.2.4. Поведінкові індикатори.....150
6.2.5. Просторові та часові фактори.....151
6.2.6. Фінансові індикатори.....152
6.2.7. Комплексна система індикаторів ризику.....153
6.3. Моделювання злочинних мереж.....156
6.3.1. Графове представлення злочинної діяльності.....157
6.3.2. Виявлення ключових учасників мережі.....159
6.3.3. Виявлення прихованих зв'язків.....160
6.3.4. Аналіз підгруп та ієрархії злочинних мереж.....162
6.3.5. Динамічне моделювання мереж.....164
6.4. Прогнозування ризиків торгівлі людьми.....166
6.4.1. Прогнозування часової активності.....168
6.4.2. Просторове прогнозування.....169
6.4.3. Прогнозування нових каналів вербування.....171
6.4.4. Моделі ризик–скорингу.....172
6.4.5. Машинне навчання для прогнозування.....174
6.4.6. Пояснюваний штучний інтелект (Explainable AI) у прогнозуванні.....176
6.5. Формування моделі раннього попередження.....179
6.5.1. Слабкі сигнали та їх агрегація.....181
6.5.2. Багатофакторна оцінка ризику.....183
6.5.3. Порогові значення та рівні небезпеки.....184
6.5.4. Автоматизоване формування попереджень.....185
6.5.5. Human–in–the–Loop у системі раннього попередження.....187
6.6. Концептуальна модель кримінологічної дата-аналітики.....191
6.6.1. Джерела даних.....193
6.6.2. Аналітичні рівні.....195
6.6.3. Моделі прогнозування.....196
6.6.4. Механізм формування управлінського рішення.....198
6.6.5. Обмеження та ризики прогнозної аналітики.....200
Висновки до розділу 6.....204
РОЗДІЛ 7. ЦИФРОВІ ТЕХНОЛОГІЇ У ПРОФІЛАКТИЦІ ТОРГІВЛІ ЛЮДЬМИ ТА ЗАХИСТІ ПОСТРАЖДАЛИХ.....208

7.1. Трансформація профілактики торгівлі людьми в умовах цифрового середовища.....209
7.2. Цифрові канали профілактичного інформування та запобігання вербуванню.....213
7.2.1. Соціальні мережі, месенджери та вебресурси як канали профілактики.....214
7.2.2. Від загального попередження до незалежної перевірки.....215
7.3. Цифрова грамотність і формування навичок безпечної поведінки 217
7.3.1. Персональні дані, документи та фінансова інформація.....219
7.3.2. Соціальна інженерія та маніпулятивна комунікація.....220
7.3.3. Безпечне користування акаунтами та цифровими каналами. .220
7.3.4. Навчання без перекладання відповідальності на потенційну постраждалу особу.....221
7.4. Цифрові засоби звернення по допомогу.....223
7.4.1. Канали цифрового звернення.....224
7.4.2. Анонімність, псевдонімність і мінімізація даних.....226
7.4.3. Безпечність комунікації та доступність.....226
7.4.4. Автоматизація і межі використання чат-ботів.....227
7.4.5. Перехід від цифрового контакту до реальної допомоги.....228
7.5. Цифрова підтримка первинного контакту з постраждалою особою 228
7.5.1. Безпечний канал і умови подальшої комунікації.....229
7.5.2. Поетапний збір інформації та робота з цифровими матеріалами 230
7.5.3. Комунікація, конфіденційність і збереження контролю постраждалої особи.....231
7.5.4. Людський контроль і завершення первинного контакту.....233
7.6. Цифрові системи перенаправлення та координації допомоги.....234
7.6.1. Організація цифрового перенаправлення.....234
7.6.2. Обмін даними, виправлення та підзвітність.....235
7.6.3. Взаємодія державних, громадських і міжнародних суб’єктів 237
7.6.4. Інтероперабельність і транскордонне перенаправлення.....237
7.6.5. Координація допомоги без надмірного цифрового контролю239
7.7. Цифрові технології у процесі відновлення та реінтеграції постраждалих.....240

7.7.1. Безперервність психологічної, медичної та правової підтримки 241
7.7.2. Освіта, професійна адаптація та економічна самостійність....242
7.7.3. Доступ до державних, соціальних послуг і соціальна реінтеграція..... 243
7.7.4. Відновлення цифрової автономії та поступове завершення спеціалізованої підтримки..... 245
7.8. Цифрова безпека постраждалої особи..... 246
7.8.1. Відновлення контролю над акаунтами, номером телефону та пристроями..... 247
7.8.2. Геолокація, stalkerware, трекери та інші форми цифрового стеження..... 248
7.8.3. Соціальні мережі, цифрове переслідування та імітація особи249
7.8.4. Індивідуальний цифровий план безпеки та відновлення автономії..... 251
7.9. Захист дітей та забезпечення диференційованої доступності цифрових сервісів..... 254
7.9.1. Дружні до дитини цифрові сервіси та безпечне звернення.…254
7.9.2. Особи з інвалідністю та цифрова доступність..... 256
7.9.3. Мовні, цифрові та функціональні бар'єри..... 257
7.9.4. Автономія користувача та універсальність без уніфікації..... 258
7.10. Правові, етичні та безпекові вимоги до цифрових сервісів профілактики й допомоги..... 259
7.10.1. Мінімізація даних, прозорість і поінформована згода..... 260
7.10.2. Privacy by design, safety by design і підхід, орієнтований на постраждалу особу..... 261
7.10.3. Межі автоматизації та використання штучного інтелекту…263
7.10.4. Недискримінація, доступність і життєвий цикл даних..... 264
7.10.5. Реагування на інциденти та підзвітність операторів цифрового сервісу..... 265
Висновки до розділу 7..... 267
РОЗДІЛ 8. МЕТОДОЛОГІЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ..... 270
8.1. Поняття та критерії ефективності цифрової протидії..... 270
8.1.1. Поняття ефективності інформаційно-аналітичної системи.…271
8.1.2. Критерії оперативності..... 273
8.1.3. Критерії точності..... 274

8.1.4. Критерії повноти.....275
8.1.5. Критерії доказовості.....277
8.1.6. Критерії кіберстійкості.....279
8.2. Система показників оцінювання.....281
8.2.1. Precision, Recall та F1-score.....283
8.2.2. False Positive Rate та False Negative Rate.....285
8.2.3. Час виявлення загрози.....287
8.2.4. Час реагування.....288
8.2.5. Якість прогнозування.....289
8.2.6. Масштабованість системи.....291
8.2.7. Економічна ефективність.....293
8.3. Оцінювання ефективності окремих технологічних компонентів..296
8.3.1. Ефективність OSINT.....297
8.3.2. Ефективність Big Data.....298
8.3.3. Ефективність GIS.....299
8.3.4. Ефективність ML/AI.....300
8.3.5. Ефективність цифрової криміналістики.....302
8.3.6. Ефективність інтегрованої аналітичної платформи.....304
8.4. Методика порівняльного оцінювання.....305
8.4.1. Традиційний та цифровий підходи.....306
8.4.2. Формування контрольних і тестових вибірок.....309
8.4.3. Експериментальна перевірка алгоритмів.....313
8.4.4. Порівняння результатів.....317
8.4.5. Статистична достовірність результатів.....319
8.5. Оцінювання надійності та стійкості аналітичної системи.....322
8.5.1. Стійкість до неповних даних.....323
8.5.2. Стійкість до зашумлення інформації.....323
8.5.3. Стійкість до навмисної маніпуляції даними.....324
8.5.4. Адаптація до зміни поведінки злочинців.....325
8.5.5. Кіберстійкість платформи.....325
8.6. Комплексна модель оцінювання ефективності.....326
8.6.1. Інтегральний показник ефективності.....328
8.6.2. Багатокритеріальна модель оцінювання.....331
8.6.3. Баланс «ефективність – законність – права людини».....333
8.6.4. Формування рейтингу ризиків.....336

8.6.5. Використання результатів оцінювання для вдосконалення системи.....338
Висновки до розділу 8.....341
ВИСНОВКИ.....343
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....348

Перелік умовних скорочень

ABAC – керування доступом на основі атрибутів (Attribute-Based Access Control).

AI – штучний інтелект (Artificial Intelligence).

AI/ML – штучний інтелект і машинне навчання (Artificial Intelligence / Machine Learning).

API – програмний інтерфейс прикладного програмування (Application Programming Interface).

BERT – двонапрямні контекстні представлення на основі трансформерів (Bidirectional Encoder Representations from Transformers).

DBSCAN – просторова кластеризація на основі щільності з урахуванням шуму (Density-Based Spatial Clustering of Applications with Noise).

DOI – цифровий ідентифікатор об’єкта (Digital Object Identifier).

ЄС – Європейський Союз.

EXIF – формат метаданих цифрових зображень (Exchangeable Image File Format).

F1-score – узагальнений показник точності та повноти класифікації.

FN – хибнонегативний результат (False Negative).

FNR – частка хибнонегативних результатів (False Negative Rate).

FP – хибнопозитивний результат (False Positive).

FPR – частка хибнопозитивних результатів (False Positive Rate).

GDPR – Загальний регламент ЄС про захист даних (General Data Protection Regulation).

GIS – географічна інформаційна система (Geographic Information System).

GeoJSON – географічний формат обміну даними на основі JSON.

GPT – генеративний попередньо навчений трансформер (Generative Pre-trained Transformer).

GPS – глобальна система позиціонування (Global Positioning System).

HDBSCAN – ієрархічна кластеризація на основі щільності (Hierarchical DBSCAN).

IOM – Міжнародна організація з міграції (International Organization for Migration).
INTERPOL – Міжнародна організація кримінальної поліції (International Criminal Police Organization).
IP – міжмережевий протокол (Internet Protocol).
ISO – Міжнародна організація зі стандартизації (International Organization for Standardization).
ISO/IEC – Міжнародна організація зі стандартизації / Міжнародна електротехнічна комісія (International Organization for Standardization / International Electrotechnical Commission).
JSON – текстовий формат подання структурованих даних (JavaScript Object Notation).
JSON-LD – формат подання пов’язаних даних на основі JSON (JSON for Linked Data).
KDE – ядерна оцінка щільності (Kernel Density Estimation).
LOF – коефіцієнт локальної аномальності (Local Outlier Factor).
MAE – середня абсолютна похибка (Mean Absolute Error).
MAD – медіанне абсолютне відхилення (Median Absolute Deviation).
ML – машинне навчання (Machine Learning).
MLAT – договір про взаємну правову допомогу (Mutual Legal Assistance Treaty).
MOM – Міжнародна організація з міграції.
MSE – середньоквадратична похибка (Mean Squared Error).
NIST – Національний інститут стандартів і технологій США (National Institute of Standards and Technology).
NLP – оброблення природної мови (Natural Language Processing).
ОБСЄ – Організація з безпеки і співробітництва в Європі.
ООН – Організація Об’єднаних Націй.
OSCE – Організація з безпеки і співробітництва в Європі (Organization for Security and Co-operation in Europe).
OSINT – розвідка на основі відкритих джерел (Open-Source Intelligence).

QR-код – двовимірний код швидкого зчитування (Quick Response Code).
RBAC – керування доступом на основі ролей (Role-Based Access Control).
RMSE – корінь із середньоквадратичної похибки (Root Mean Squared Error).
SHA-256 – криптографічна хеш-функція з 256-бітним результатом (Secure Hash Algorithm 256-bit).
SHA-3 – сімейство криптографічних хеш-функцій SHA-3 (Secure Hash Algorithm 3).
SHAP – метод пояснення результатів моделей на основі значень Шеплі (SHapley Additive exPlanations).
SIM-карта – модуль ідентифікації абонента (Subscriber Identity Module).
SMS – служба коротких текстових повідомлень (Short Message Service).
SQL – мова структурованих запитів (Structured Query Language).
ST-DBSCAN – просторово-часова кластеризація на основі щільності (Spatio-Temporal DBSCAN).
TF-IDF – частота терміна з урахуванням оберненої частоти документа (Term Frequency–Inverse Document Frequency).
UNODC – Управління ООН з наркотиків і злочинності (United Nations Office on Drugs and Crime).
URL – уніфікований покажчик місцезнаходження ресурсу (Uniform Resource Locator).
VPN – віртуальна приватна мережа (Virtual Private Network).
WORM – технологія одноразового запису з багаторазовим читанням (Write Once, Read Many).
XAI – пояснюваний штучний інтелект (Explainable Artificial Intelligence).
ШІ – штучний інтелект.

ПЕРЕДМОВА

Торгівля людьми залишається одним із небезпечних кримінальних явищ, що посягає на свободу, гідність і безпеку людини. Сучасні інформаційні технології істотно змінюють способи вчинення таких кримінальних правопорушень: соціальні мережі, месенджери, онлайн-платформи та цифрові фінансові інструменти можуть використовуватися для вербування, встановлення контакту з потенційними потерпілими, організації переміщення, контролю та отримання незаконних доходів. Водночас цифрове середовище створює нові можливості для виявлення ознак злочинної діяльності, встановлення зв'язків між її учасниками, документування цифрових слідів і вдосконалення заходів протидії.

Ефективне використання цих можливостей потребує комплексного підходу, який поєднує правові засади, інформаційно-аналітичні методи, засоби кібербезпеки, кримінологічне моделювання, організаційні рішення та механізми захисту прав людини. Важливими є не лише технічні можливості окремих інструментів, а й достовірність отриманих відомостей, належне документування результатів, дотримання вимог щодо оброблення персональних даних і перевірка обґрунтованості аналітичних висновків. Цифрові технології мають доповнювати професійну діяльність уповноважених суб'єктів, а не підміняти встановлені законом процедури та відповідальність людини за прийняття рішень.

Метою монографії є дослідження теоретико-правових, інформаційно-аналітичних, кримінологічних і організаційно-технологічних засад протидії торгівлі людьми з використанням сучасних інформаційних технологій, а також обґрунтування підходів до їх практичного застосування, інтеграції та оцінювання ефективності.

Для досягнення цієї мети розглянуто нормативно-правові засади протидії торгівлі людьми та роль цифрових технологій у правоохоронній діяльності; досліджено можливості OSINT, аналізу великих даних, машинного навчання і штучного інтелекту для виявлення підозрілих ознак; висвітлено питання цифрової криміналістики, захисту цифрових доказів і протидії інформаційним

маніпуляціям. Окрему увагу приділено практичним кейсам застосування аналітичних інструментів, перспективам інтеграції відповідних рішень у національну систему безпеки, кримінологічному аналізу та моделюванню ризиків торгівлі людьми в цифровому середовищі.

Важливою складовою дослідження є розгляд цифрової профілактики торгівлі людьми, можливостей безпечного звернення по допомогу, доступності цифрових сервісів, захисту постраждалих осіб і відновлення їхньої автономії. Такий підхід передбачає врахування потреб людини, ризиків повторної віктимізації, вимог конфіденційності та безпеки, а також обмежень автоматизованого опрацювання інформації.

Завершальний напрям дослідження становить методологія оцінювання ефективності цифрових технологій у протидії торгівлі людьми. У цьому контексті розглянуто критерії та систему показників оцінювання, підходи до визначення результативності окремих технологічних рішень, зокрема засобів аналізу відкритих джерел та інформаційно-аналітичних інструментів. Принципове значення має розмежування технічних характеристик системи та її фактичної юридичної й суспільної ефективності: швидкість оброблення інформації або точність алгоритму самі по собі не підтверджують правильності висновку про наявність торгівлі людьми.

Методологічну основу монографії становлять загальнонаукові та спеціальні методи дослідження, зокрема аналіз і синтез, системний та порівняльний підходи, методи кримінологічного аналізу, моделювання ризиків, опрацювання даних і оцінювання технологічних рішень. Їх застосування дає змогу розглянути протидію торгівлі людьми як комплексну діяльність, у якій інформаційні технології мають поєднуватися з правовими, організаційними та людиноцентричними механізмами.

Практичне значення монографії полягає в систематизації підходів до використання цифрових засобів виявлення, аналізу та документування ознак торгівлі людьми, розгляді можливостей інтеграції інформаційних ресурсів і формуванні методологічних орієнтирів для оцінювання результативності

відповідних технологій. Матеріали можуть бути використані у наукових дослідженнях, освітньому процесі та діяльності фахівців, залучених до протидії торгівлі людьми, за умови врахування їхніх повноважень і вимог чинного законодавства.

РОЗДІЛ 1. ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

1.1. Визначення та динаміка розвитку явища торгівлі людьми

Торгівля людьми у сучасному світі виступає як багатовимірне соціально-правове явище, що порушує базові права людини та посягає на її свободу і гідність. Вона поєднує ознаки злочинів проти особистості та є складовою організованої злочинності.

У міжнародно-правовій практиці основу визначення цього поняття закладено у Протоколі ООН, де підкреслюється, що сутність явища полягає у вербуванні, транспортуванні чи приховуванні людей із використанням примусу, обману чи інших протиправних засобів задля подальшої експлуатації [1].

В Україні кримінальна відповідальність за торгівлю людьми встановлена ст. 149 Кримінального кодексу України, яка охоплює торгівлю людиною, а також її вербування, переміщення, переховування, передачу або одержання з метою експлуатації за передбачених законом умов [2].

Сучасні тенденції:

- глобалізація процесів: торгівля людьми набуває транснаціонального характеру, охоплюючи кілька держав одночасно;
- зростання ролі цифрових технологій: вербування дедалі частіше відбувається через соціальні мережі, месенджери та онлайн-оголошення;
- зміна форм експлуатації: крім сексуальної та трудової, поширюються примусове жебрацтво, використання у злочинній діяльності, незаконне усиновлення;
- вразливість мігрантів: збройні конфлікти, економічна нестабільність та масові міграційні процеси посилюють ризики потрапляння до рук торговців людьми [3].

Таким чином, торгівля людьми постає як складний виклик для національних правових систем і міжнародного співтовариства, що потребує комплексного підходу.

1.2. Нормативно-правова база України та міжнародні стандарти

Протидія торгівлі людьми регулюється сукупністю міжнародних зобов'язань, національних норм кримінального та соціального законодавства і процесуальних правил. Їх взаємодія має принципове значення для правозастосування: кваліфікація діяння, встановлення обставин справи та надання допомоги постраждалій особі пов'язані між собою, але вирішують різні правові завдання.

Міжнародну основу становить Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, та покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності. Він визначає торгівлю людьми через поєднання відповідних дій, засобів впливу та мети експлуатації, а також орієнтує держави на криміналізацію, запобігання, захист постраждалих і співпрацю [1]. Конвенція Ради Європи про заходи щодо протидії торгівлі людьми поглиблює правозахисний вимір цих зобов'язань: увагу зосереджено на виявленні постраждалих, доступі до допомоги, захисті їхніх прав і незалежному моніторингу виконання Конвенції [4]. З цього випливає, що реагування держави має охоплювати потреби та безпеку людей, яких стосується експлуатація, поряд із притягненням винних до відповідальності.

В Україні організаційні засади цієї діяльності визначає Закон України «Про протидію торгівлі людьми». Його положення охоплюють запобігання, боротьбу з торгівлею людьми, взаємодію уповноважених суб'єктів, встановлення статусу особи, яка постраждала від торгівлі людьми, та надання їй допомоги [6]. Кримінально-правові ознаки торгівлі людьми і відповідальність за неї встановлено статтею 149 Кримінального кодексу України [2]. Якщо виникає питання про використання отриманих відомостей у кримінальному провадженні, порядок збирання та оцінювання доказів визначається Кримінальним процесуальним кодексом України [57]. Отже, соціально-правовий захист постраждалої особи, кваліфікація злочину та доказування потребують узгодження, проте кожен із цих напрямів має власні підстави й процедури.

На інституційному рівні протидія торгівлі людьми потребує узгоджених дій органів соціального захисту, правоохоронних органів, інших установ і організацій, залучених до виявлення випадків експлуатації та підтримки постраждалих. Міністерство соціальної політики, сім'ї та єдності України як національний координатор висвітлює механізми допомоги та напрями взаємодії у цій сфері [7]. Для практики важливо, щоб передавання інформації між учасниками супроводжувалося визначенням мети, компетенції та відповідальності кожного з них. Потреби особи, яка звертається по допомогу, мають оцінюватися з огляду на її захист і відновлення, а не лише на можливе значення її відомостей для розслідування.

Окреме місце в аналізі міжнародного досвіду посідають щорічні звіти Державного департаменту США про торгівлю людьми. Звіт за 2023 рік містить порівняльні оцінки державних заходів і відомості про тенденції, які можуть використовуватися як аналітичний матеріал [5]. Такий звіт не є міжнародним договором або нормативним актом і не встановлює юридичних обов'язків для України. Його висновки слід співвідносити з періодом спостереження та методикою оцінювання.

Цифрова обробка відомостей про ймовірні випадки торгівлі людьми породжує окремі вимоги до захисту інформації. В Україні правові підстави і межі оброблення персональних даних визначаються, зокрема, Законом України «Про захист персональних даних» [10]. Для порівняльного аналізу європейського регулювання слід розмежовувати загальний режим Регламенту (ЄС) 2016/679 і спеціальний режим Директиви (ЄС) 2016/680, який стосується оброблення даних компетентними органами для цілей запобігання, розслідування та переслідування кримінальних правопорушень [9, 56]. Ці акти не замінюють українських норм, проте їх урахування є важливим під час визначення умов міжнародного обміну інформацією.

Таким чином, правова основа протидії торгівлі людьми поєднує кримінальну відповідальність, процесуальні гарантії та захист постраждалих осіб. Для інформаційно-аналітичних систем це означає необхідність ще на етапі

проєктування визначати законні джерела даних, повноваження користувачів, порядок передавання відомостей і способи перевірки результатів аналізу.

1.3. Роль цифрових технологій у правозастосуванні

Цифрові сервіси змінюють інформаційне середовище, у якому можуть відбуватися вербування, комунікація та приховування пов’язаних дій. Оголошення про роботу, повідомлення в соціальних мережах і цифрові платіжні сліди іноді містять відомості, значущі для перевірки обставин справи. Наявність таких відомостей сама по собі не свідчить про торгівлю людьми: законні пропозиції працевлаштування, звичайне користування месенджерами чи віртуальними активами не можуть автоматично тлумачитися як ознаки злочину. Завдання правозастосування полягає у встановленні контексту та перевірці конкретних зв’язків між подіями.

На початковому етапі аналіз відкритих джерел дає змогу зіставляти публікації, контакти, зображення і час їх появи та формувати перевірювані гіпотези. Публічна доступність матеріалу не усуває вимог до мети, обсягу й правових підстав подальшого оброблення персональних даних [10]. Тому аналітик має фіксувати джерело кожного спостереження, відокремлювати встановлені факти від припущень і шукати незалежне підтвердження виявлених збігів. Методи аналізу мережевих зв’язків допомагають упорядкувати повторювані ідентифікатори, однак наявність зв’язку в графі не визначає характеру взаємин між людьми [14].

Геоінформаційні методи додають до аналізу просторовий контекст. Вони можуть виявляти концентрації географічно прив’язаних публікацій або подій і допомагати перевіряти припущення про їхню просторову та часову пов’язаність. Статистичні методи просторового сканування й кластеризації становлять методичну основу для такого аналізу [11, 12, 13]. Водночас місце розміщення оголошення, адреса реєстрації користувача або геопозначка не є підтвердженим місцем експлуатації чи маршрутом переміщення людини. Практичний висновок потребує перевірки точності координат, походження даних і альтернативних пояснень виявленого кластера.

Оброблення великих масивів даних і алгоритми машинного навчання можуть прискорювати пошук повторів, групування схожих матеріалів та відбір нетипових спостережень. Методи виявлення аномалій дозволяють визначати об’єкти для поглибленого аналізу, проте статистична нетиповість не дорівнює протиправності [15]. За таких умов результат алгоритму доцільно використовувати для пріоритизації роботи фахівця із зазначенням вихідних даних, критеріїв відбору та можливих помилок. Остаточне тлумачення відомостей залежить від обставин конкретної справи й не може бути повністю делеговане автоматизованій системі.

Коли цифровий матеріал може мати значення для кримінального провадження, на перший план виходять його походження, цілісність і відтворюваність процедури отримання. Підходи цифрової криміналістики передбачають документування роботи з електронними об’єктами, контроль змін, належне збереження оригінальних даних і простежуваність дій із ними [8, 44]. Хешування та фіксація часу допомагають перевіряти окремі технічні властивості збереженого матеріалу, але не встановлюють достовірності його змісту або допустимості доказу. Процесуальне значення цифрових відомостей визначається відповідно до вимог Кримінального процесуального кодексу України [57].

Застосування цифрових інструментів також має враховувати можливу шкоду від помилкової ідентифікації людини та розкриття відомостей про постраждалих. Доступ до персональних даних потрібно обмежувати службовою необхідністю, а результати автоматизованої обробки – перевіряти до їх використання для рішень щодо конкретних осіб [10]. У співпраці з європейськими партнерами додаткового значення набуває правильне визначення режиму оброблення та передавання даних відповідно до сфери дії Регламенту (ЄС) 2016/679 або Директиви (ЄС) 2016/680 [9, 56].

Отже, роль цифрових технологій у правозастосуванні полягає у підтримці послідовного переходу від інформаційного сигналу до перевіреної обставини. Аналітичні інструменти допомагають знайти й зіставити відомості, цифрова криміналістика – зберегти можливість їх технічної перевірки, а правові

процедури та експертна оцінка визначають межі їх використання. Таке розмежування створює підґрунтя для детального аналізу OSINT, GIS, великих даних і машинного навчання в наступних розділах роботи.

Висновок до розділу 1

Торгівля людьми є складним правовим і соціальним явищем, для встановлення якого недостатньо виявити окрему підозрілу дію чи інформаційний слід. Значення мають мета експлуатації, спосіб впливу на людину, взаємозв'язок дій учасників та обставини конкретного випадку. Такий підхід запобігає як невиправданому ототожненню ризикової ситуації зі встановленим злочином, так і пропуску випадків експлуатації, ознаки яких розподілені між різними джерелами інформації.

Міжнародні стандарти й законодавство України формують взаємопов'язані напрями реагування: запобігання торгівлі людьми, притягнення винних до відповідальності та захист постраждалих осіб. Кожен із них має власні правові підстави й процедури. Потреба людини в допомозі не повинна оцінюватися лише через її можливу участь у доказуванні, а кримінально-правовий висновок не може ґрунтуватися тільки на аналітичному припущенні. Для практичного застосування цих положень необхідна узгоджена робота установ, які виявляють випадки експлуатації, здійснюють розслідування та забезпечують підтримку постраждалих.

Цифрове середовище створює додаткові можливості для встановлення зв'язків між оголошеннями, контактами, повідомленнями, місцями й подіями. Проте повторюваний ідентифікатор, просторове скупчення або алгоритмічно виявлена аномалія є інформаційним сигналом, зміст якого залежить від контексту. Правозастосовна цінність цифрових технологій полягає у формуванні перевірюваних гіпотез і визначенні напрямів подальшої роботи. Висновки щодо конкретних осіб та обставин потребують зіставлення з незалежними відомостями і професійної оцінки.

Перехід від аналітичного сигналу до відомостей, які можуть використовуватися у кримінальному провадженні, вимагає документування походження цифрового матеріалу, збереження його цілісності та дотримання процесуальних правил. Водночас збирання й поєднання даних про людей мають бути обмежені законною метою та необхідним обсягом. Особливого захисту потребує інформація про осіб, які постраждали або можуть постраждати від торгівлі людьми: помилкова ідентифікація чи розголошення відомостей здатні створити для них додаткову небезпеку.

Отже, правові та етичні вимоги визначають умови застосування інформаційно-аналітичних методів на кожному етапі – від отримання даних до використання результату. Подальший аналіз OSINT, GIS, великих даних і машинного навчання має виходити з цього положення: технології підтримують виявлення та перевірку обставин, а відповідальність за їх правове тлумачення і рішення щодо людини залишається за уповноваженим фахівцем.

РОЗДІЛ 2. ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У ВИЯВЛЕННІ ТОРГІВЛІ ЛЮДЬМИ

2.1. Використання OSINT (open-source intelligence)

2.1.1. Джерела та сигнали

Аналіз джерел відкритої інформації (OSINT) дає змогу ідентифікувати початкові маркери (сигнали), що свідчать про можливу діяльність злочинних груп у сфері торгівлі людьми. Їх можна розглядати як «слабкі сигнали», котрі у поєднанні з іншими факторами формують основу для подальшого інформаційно-аналітичного дослідження. Важливим є не лише перелік джерел, але й методологія виявлення закономірностей, кореляцій і повторюваних структур у даних.

Класифікація джерел та характерні ознаки

Важливим джерелом відкритої інформації у сфері протидії торгівлі людьми є інтернет-ресурси працевлаштування та сервіси оголошень. Самі по собі такі платформи мають законне призначення і використовуються переважно для пошуку роботи та роботодавців. Водночас окремі публікації можуть містити ознаки, які потребують додаткової перевірки. До них належать нечіткий опис умов працевлаштування, відсутність відомостей про роботодавця чи трудові обов’язки, непропорційно висока обіцяна винагорода, повторне використання однакових контактних даних у різних оголошеннях, а також акцент на терміновому виїзді, мінімальній перевірці документів або анонімності. Жодна з таких ознак окремо не свідчить про протиправну діяльність, однак їх поєднання може бути підставою для поглибленого аналізу.

Соціальні мережі та месенджери також становлять значний інтерес для OSINT-дослідження, оскільки через них поширюється великий обсяг інформації про роботу, поїздки, послуги та інші пропозиції. Аналізу можуть підлягати випадки масового поширення однотипних повідомлень у різних спільнотах, одночасної активності пов’язаних акаунтів у кількох регіонах, повторного використання однакових текстів або контактів, а також діяльність облікових записів із мінімальною історією чи ознаками автоматизованого поширення

контенту. Водночас використання псевдонімів, нових акаунтів або месенджерів саме по собі не може розглядатися як доказ протиправної поведінки.

Окремим напрямом аналізу можуть бути онлайн-платформи, на яких розміщуються оголошення про інтимні або ескорт-послуги. У цьому середовищі особливо важливо уникати автоматичного ототожнення самої присутності оголошення з фактом експлуатації. Аналітичну увагу можуть привертати повторне використання одного й того самого зображення в різних профілях, невідповідність між зазначеними іменами, контактами або географічними даними, а також швидка зміна місця публікації одних і тих самих матеріалів. Такі збіги можуть свідчити про пов’язаність окремих публікацій, однак потребують перевірки іншими джерелами.

Транспортні та міграційні дані можуть доповнювати загальну аналітичну картину. Відкриті розклади рейсів, транспортні сервіси та трекінгові системи дають змогу аналізувати повторюваність маршрутів, часові закономірності та зв’язок між окремими інформаційними подіями. Наприклад, інтерес може становити збіг у часі між появою великої кількості термінових пропозицій роботи та активізацією певних маршрутів. Однак самі по собі групові поїздки, переміщення до прикордонних регіонів або регулярне використання одного перевізника не є індикатором торгівлі людьми й повинні розглядатися лише в сукупності з іншими перевіреними ознаками.

Державні відкриті реєстри доцільно використовувати для верифікації відомостей про юридичних осіб, підприємців, адреси реєстрації та інші публічно доступні атрибути. Вони можуть допомагати встановлювати зв’язки між організаціями, контактними даними та адресами, перевіряти тривалість діяльності суб’єкта або зіставляти інформацію з інших відкритих джерел. При цьому короткий строк існування компанії, спільна адреса реєстрації кількох суб’єктів або згадування особи у відкритих судових матеріалах не повинні автоматично інтерпретуватися як ознаки злочинної діяльності. Такі факти мають значення лише у відповідному контексті та після додаткової перевірки.

Додаткову інформацію можуть містити закриті або напівзакриті сегменти мережі, а також відкриті дані про криптовалютні транзакції. У таких випадках аналіз може бути спрямований на виявлення повторюваних ідентифікаторів, адрес криптогаманців, контактних даних чи псевдонімів, які одночасно зустрічаються у різних інформаційних середовищах. Важливим є саме встановлення перехресних зв'язків між відкритими джерелами, форумами, оголошеннями та фінансовими ідентифікаторами. Водночас наявність криптовалютного гаманця, використання сервісів із підвищеним рівнем анонімності або присутність певного контакту в різних сегментах мережі не може самостійно підтверджувати причетність до торгівлі людьми.

Таким чином, цінність OSINT полягає не у пошуку окремої «підозрілої ознаки», а у зіставленні незалежних джерел, повторюваних характеристик і контексту. Аналітичний висновок має формуватися лише на основі сукупності взаємопов'язаних сигналів, із чітким розмежуванням між фактом, припущенням, аналітичною гіпотезою та встановленою обставиною.

Узагальнені індикатори

Під час аналізу відкритих джерел важливо розглядати окремі ознаки не як підтвердження протиправної діяльності, а як індикатори, що можуть потребувати додаткової перевірки. Найбільшу аналітичну цінність вони набувають тоді, коли повторюються у різних джерелах, поєднуються між собою або формують стійку закономірність.

Одним із таких індикаторів є повторюваність контактних даних. Використання одного й того самого номера телефону, адреси електронної пошти, нікнейма чи іншого ідентифікатора у значній кількості оголошень або на різних платформах може свідчити про зв'язок між відповідними публікаціями. Водночас сам факт повторення контакту не є доказом протиправної діяльності, оскільки один контакт може законно використовуватися роботодавцем, посередником або організацією.

Додаткової уваги можуть потребувати оголошення з нетиповими або недостатньо визначеними умовами працевлаштування. Йдеться, зокрема, про

обіцянки непропорційно високого заробітку без чіткого опису роботи, вимоги термінового виїзду, мінімальну інформацію про роботодавця чи відсутність зрозумілих умов оформлення трудових відносин. Такі характеристики доцільно оцінювати в контексті ринку праці та інших доступних відомостей.

Важливим аналітичним сигналом є також повторне використання контенту. Ідентичні або майже однакові тексти, фотографії чи інші матеріали в різних оголошеннях можуть вказувати на спільне походження публікацій або їх централізоване розміщення. Для виявлення таких зв’язків можуть застосовуватися пошук текстових збігів, зворотний пошук зображень та перцептивне хешування. Однак саме дублювання контенту не дозволяє встановити характер діяльності осіб, які його поширюють.

Географічні зміни у публікаціях також можуть становити інтерес для аналізу. Наприклад, поява однакових матеріалів із зазначенням різних міст або країн у короткі проміжки часу може свідчити про зміну географії розміщення оголошень, використання централізованого акаунта або інші особливості інформаційної активності. Коректніше розглядати такі випадки як географічну динаміку публікацій, а не як підтверджене переміщення конкретної особи.

Фінансові дані можуть доповнювати загальну картину лише за умови законного доступу до них та належного контексту. Повторне використання певної криптовалютної адреси, нетипова структура платежів або зв’язок одного фінансового ідентифікатора з декількома інформаційними об’єктами можуть бути підставою для подальшого аналізу. Водночас використання криптовалют саме по собі не є ознакою протиправної діяльності, а статистична аномалія у транзакціях не повинна автоматично трактуватися як доказ злочину.

Таким чином, узагальнені індикатори доцільно використовувати як *систему сигналів для формування та перевірки аналітичних гіпотез*, а не як механізм автоматичного визначення осіб або подій як злочинних. Поєднання текстових, візуальних, контактних, просторових і фінансових характеристик дозволяє виявляти повторювані зв’язки та закономірності, після чого результати можуть бути перевірені іншими незалежними джерелами. Саме такий підхід

створює основу для подальшого застосування методів машинного навчання, графового та геопросторового аналізу із збереженням принципів пропорційності, перевірюваності та недопущення необґрунтованих висновків.

2.1.2. Законність, етика, безпека

Застосування OSINT у сфері протидії торгівлі людьми дає змогу отримувати з відкритих джерел інформацію, яка може бути корисною для формування аналітичних гіпотез, встановлення зв'язків між інформаційними об'єктами та визначення напрямів подальшої перевірки. Водночас доступність інформації в мережі не означає автоматичної можливості її необмеженого збирання, зберігання та використання. Особливої обережності потребують відомості, що стосуються конкретних осіб, їхніх контактів, місця перебування, соціальних зв'язків, фотографій та інших персональних характеристик. Тому використання OSINT доцільно розглядати у взаємозв'язку трьох складових – законності, етичності та безпеки.

Законність

Правомірність роботи з відкритими джерелами визначається не лише тим, чи доступна певна інформація публічно, а й метою її збирання, обсягом, способом подальшого використання та правовими підставами обробки персональних даних. У європейському правовому просторі загальні вимоги до захисту персональних даних визначаються GDPR [9], тоді як в Україні базові принципи їх обробки закріплені Законом України «Про захист персональних даних» [10]. У міжнародних рекомендаціях, зокрема матеріалах UNODC та FRA [18], використання інформаційно-аналітичних технологій у правоохоронній діяльності також пов'язується з необхідністю дотримання прав людини, пропорційності втручання та відповідальності за використання отриманих даних.

Для OSINT принциповим є розмежування відкритого отримання інформації та несанкціонованого доступу до інформаційних систем. Аналіз публічно доступних вебсторінок, відкритих реєстрів, повідомлень у соціальних мережах або інших загальнодоступних ресурсів належить до сфери роботи з

відкритою інформацією. Водночас обхід засобів автентифікації, отримання доступу до закритих облікових записів без належних повноважень або втручання в інформаційні системи не є OSINT-діяльністю і може мати самостійні правові наслідки.

Важливо також враховувати принцип цільового використання. Інформація повинна збиратися не «про всяк випадок», а для конкретного аналітичного завдання. Наявність технічної можливості отримати значний масив персональних даних не означає необхідності його накопичення. Такий підхід особливо важливий у випадках, коли інформація може стосуватися осіб, які постраждали від торгівлі людьми або перебувають у вразливому становищі.

Етика

Етичний вимір OSINT виходить за межі формального дотримання законодавства. Навіть правомірно отримані дані можуть бути використані способом, який створює ризики для приватності, безпеки або гідності людини. Саме тому одним із базових принципів має бути мінімізація даних – збирання лише тієї інформації, яка обґрунтовано необхідна для конкретного завдання.

Особливу увагу слід приділяти недопущенню автоматичного профілювання осіб або соціальних груп. Походження, стать, вік, національність, характер зайнятості, місце проживання чи використання певної онлайн-платформи самі по собі не можуть трактуватися як ознаки причетності до протиправної діяльності. Алгоритмічні моделі також можуть відтворювати упередження, присутні у вихідних даних, тому їхні результати доцільно використовувати як допоміжний аналітичний інструмент, а не як автоматичний висновок щодо конкретної особи.

Не менш важливим є принцип перевірюваності. Аналітик повинен мати можливість пояснити, з яких джерел отримано інформацію, які операції з нею виконувалися та на підставі яких ознак сформовано певну гіпотезу. Це дозволяє відокремити встановлений факт від припущення, статистичної закономірності або результату автоматизованої класифікації.

Під час роботи з інформацією про осіб, які можуть постраждати від експлуатації, пріоритетним має залишатися принцип «не зашкодь». Публічне

поширення персональних відомостей, фотографій, адрес або інших ідентифікаторів може створювати додаткові ризики для таких осіб. Тому аналітична цінність інформації повинна постійно співвідноситися з можливими наслідками її використання.

Безпека

Безпека OSINT-діяльності охоплює одночасно захист отриманих матеріалів, персональних даних, технічної інфраструктури та самих аналітиків.

Для забезпечення цілісності цифрових матеріалів доцільно фіксувати їх походження, час отримання та основні етапи подальшої обробки. Криптографічне хешування, зокрема із застосуванням алгоритмів SHA-256 або SHA-3, дозволяє контролювати незмінність файлів після їх збереження. Для підтвердження часу фіксації можуть застосовуватися механізми довіреного цифрового таймстемпінгу, а в окремих випадках – інші технологічні рішення, зокрема розподілені реєстри. Водночас такі технічні засоби підтверджують певні властивості цифрового об’єкта, але самі по собі не визначають його процесуальний статус.

Важливою складовою захисту є псевдонімізація або, де це можливо, анонімізація даних. У проміжних аналітичних наборах замість прямих персональних ідентифікаторів доцільно використовувати умовні коди, а доступ до інформації, яка дозволяє встановити особу, обмежувати відповідно до службових повноважень. Особливе значення це має для відомостей про постраждалих осіб, свідків та інших учасників подій, розголошення інформації про яких може створити додаткову небезпеку.

Захисту потребує й робоче середовище аналітика. Для дослідження потенційно небезпечних ресурсів можуть застосовуватися ізольовані середовища, окремі профілі або віртуалізовані системи, а використання захищених мережевих з’єднань допомагає зменшувати ризики розкриття технічної інформації про дослідника. Такі заходи не повинні використовуватися для обходу встановлених правових обмежень доступу.

Інформаційна інфраструктура OSINT повинна передбачати розмежування прав доступу, журналювання дій користувачів, резервне копіювання, контроль

цілісності даних та захист від несанкціонованого втручання. Це дозволяє не лише зменшити ризик втрати або компрометації інформації, а й забезпечити простежуваність роботи з нею.

Таким чином, законність, етичність і безпека не є окремими додатковими вимогами до OSINT, а становлять невід'ємну частину самої методології його використання. Ефективний аналіз відкритих джерел передбачає не максимальне накопичення інформації, а обґрунтоване отримання мінімально необхідних даних, їх перевірку, захищене зберігання та відповідальне використання**.** Такий підхід дозволяє поєднати інформаційно-аналітичні можливості OSINT із захистом приватності, гідності та безпеки людини, а також підвищує прозорість і перевірюваність отриманих результатів.

2.1.3. Збирання та нормалізація

Систематизація відкритих даних передбачає два взаємопов'язані процеси – збирання та нормалізацію. Перший аспект включає використання автоматизованих методів: офіційних API (якщо вони доступні) або веб-скрапінгу у правовому полі. Другий аспект полягає у приведенні даних до уніфікованих форматів. Наприклад, телефонні номери зводяться до міжнародного стандарту *E.164*, географічні назви – до форматів *ISO 3166*, а часові дані – до *ISO 8601*.

Особливу увагу слід приділяти уникненню дублювань. Це досягається через зіставлення ключових ідентифікаторів (телефонів, e-mail), аналіз текстової подібності (*fuzzy matching*), а також за допомогою перцептивних хешів для зображень.

Таким чином, нормалізація даних не лише зменшує інформаційний «шум», але й створює передумови для точнішої аналітики, знижуючи ризики хибнопозитивних сигналів.

2.1.4. Текстова аналітика

Оголошення та повідомлення у соціальних мережах є головними каналами комунікації вербувальників. Їх аналіз можливий завдяки сучасним методам обробки природної мови. Важливим є формування словників ризикової лексики,

що включають не лише прямі згадки («робота за кордоном», «швидкий заробіток»), але й евфемізми, заміну символів, використання емодзі.

Для класифікації текстів застосовуються алгоритми машинного навчання: від класичних моделей (TF-IDF у поєднанні з логістичною регресією) до трансформерних архітектур, здатних враховувати контекст. Окремим напрямом є автоматичне виявлення сутностей (Named Entity Recognition), яке дозволяє виділяти контакти, географічні назви та грошові суми, що часто виступають ключовими ознаками вербувальної діяльності.

Таким чином, текстовий аналіз формує основу для автоматичного виявлення та групування підозрілих повідомлень, створюючи передумови для раннього виявлення ризиків.

2.1.5. Аналіз зображень та відео

Візуальні матеріали – фотографії та відео – супроводжують більшість оголошень і профілів у мережі. Вони несуть як явну інформацію (зовнішність осіб, обстановка), так і приховані цифрові атрибути.

Методи зворотного пошуку зображень дають змогу виявляти повторне використання фотографій у різних анкетах або на різних ресурсах. Аналіз метаданих (*EXIF*) допомагає встановити дату, час чи навіть географічні координати зйомки. Перцептивні хеші (*pHash*) застосовуються для виявлення дублювання зображень, навіть якщо вони були модифіковані (обрізані, змінені за кольорами). Для відео можливим є використання алгоритмів комп’ютерного зору з метою ідентифікації характерних об’єктів, архітектурних деталей чи дорожніх знаків, що полегшує геолокацію.

Аналіз візуальних матеріалів створює додатковий рівень перевірки автентичності даних і допомагає поєднувати розрізнені сигнали у єдину аналітичну картину.

2.1.6. Графовий OSINT

Аналіз соціальних і комунікаційних зв’язків є одним із найефективніших методів виявлення мережевої структури злочинних угруповань. У практиці OSINT підхід ґрунтується на побудові графових моделей, де вузлами виступають

об’єкти (телефонні номери, акаунти в соціальних мережах, криптовалютні гаманці), а ребрами – зв’язки між ними (спільне використання фото, дублювання текстів, фінансові транзакції).

Застосування показників центральності дозволяє визначати координаторів або «брокерів» мережі. Наприклад, високі значення міжпосередницької центральності свідчать про те, що вузол виконує роль «посередника» між групами. Методи виявлення спільнот (алгоритм *Louvain, Leiden*) допомагають виділяти підгрупи учасників, що взаємодіють між собою частіше, ніж із зовнішніми об’єктами.

Таким чином, графовий OSINT перетворює розрізнені цифрові сліди на структуровану модель, здатну показати як локальні, так і глобальні закономірності у діяльності злочинних мереж.

2.1.7. ГеоOSINT і просторовий аналіз

Географічний вимір даних є критично важливим для протидії торгівлі людьми, оскільки більшість схем включає транспортування осіб через країни або регіони. ГеоOSINT поєднує геокодування адрес, аналіз транспортних маршрутів та просторову візуалізацію «гарячих точок».

Використання методів оцінки щільності (kernel density estimation) дає змогу виділити зони концентрації підозрілих оголошень поблизу транспортних вузлів – вокзалів, прикордонних пунктів, хостелів. Просторово-часові моделі дозволяють виявляти «коридори» переміщення жертв, що мають регулярний характер.

Інтеграція геоданих із результатами графового аналізу створює багатовимірну картину: виявлені у графі контакти можуть співвідноситися з конкретними географічними маршрутами, що підвищує інформаційну цінність аналітичних висновків та дає змогу формувати обґрунтовані напрями подальшої перевірки.

2.1.8. Документування результатів

Результати OSINT можуть використовуватися як інформаційно-аналітичні матеріали, а за умови належного процесуального отримання, фіксації та

оцінювання – набувати доказового значення відповідно до вимог кримінального процесуального законодавства.

У практиці OSINT це досягається завдяки створенню стандартизованих «пакетів доказів», що включають зафіксовані джерела інформації, метадані збору та криптографічні підтвердження автентичності.

Найбільш поширеним методом забезпечення незмінності даних є хешування (*SHA-256*), яке дозволяє перевірити, що файл не зазнав модифікацій. Для фіксації часу збору застосовується цифровий таймстемпінг, у тому числі з використанням блокчейн-рішень. Крім того, важливим є ведення журналу дій аналітика, який описує, коли і яким чином було отримано конкретний доказ.

Документування походження, цілісності та послідовності оброблення цифрових матеріалів сприяє їх перевірюваності й оцінюванню автентичності; питання належності та допустимості доказів вирішується відповідно до процесуального законодавства.

2.1.9. Типові ризики й помилки

Застосування OSINT у сфері протидії торгівлі людьми має не лише переваги, але й обмеження, що слід враховувати.

Першим ризиком є плутанина між кореляцією та причинністю: той факт, що два акаунти використовують однакові фотографії, ще не доводить їх злочинний характер. Другим поширеним недоліком є надмірна кількість хибнопозитивних результатів, що призводить до перевантаження аналітиків. Це пов’язано з рідкістю «позитивних» випадків та складністю їх чіткого маркування.

Окрему проблему становить адаптація злочинців: використання одноразових акаунтів, систематичне спотворення текстів та фото, а також переміщення діяльності у закриті мережі. Безперервне оновлення словників, алгоритмів і методик стає необхідною умовою підтримки ефективності OSINT.

Комплексне застосування методів OSINT – від текстового аналізу до геопросторового та графового моделювання – формує багаторівневу систему виявлення торгівлі людьми. Водночас лише дотримання законності, етичності й

безпеки, а також належне документування результатів дають змогу використовувати такі дані у практичній діяльності правоохоронних органів.

2.2. Аналітика великих даних (Big Data) для виявлення підозрілих патернів

Зростання обсягів інформації, що супроводжує явище торгівлі людьми, потребує використання методів обробки великих даних. Виклики полягають у різнорідності джерел (соціальні мережі, оголошення, транспортні потоки, криптовалютні транзакції), високій швидкості їх появи та значному рівні «шуму». Технології Big Data дають змогу здійснювати інтеграцію, очищення, багатовимірний аналіз та візуалізацію інформаційних потоків у масштабах, що підвищують результативність заходів реагування.

2.2.1. Архітектура даних

Створення інформаційно-аналітичної системи для протидії торгівлі людьми вимагає спеціально спроєктованої архітектури даних, яка здатна працювати з різнорідними, часто неструктурованими потоками інформації. На відміну від традиційних баз даних, що зберігають чітко структуровану інформацію, тут необхідно інтегрувати тексти оголошень, фото- та відеоматеріали, транспортні логи, записи з державних реєстрів, повідомлення із соціальних мереж та дані з відкритих API.

У сучасних підходах дедалі частіше використовується *концепція Data Lakehouse*, яка поєднує можливості «озера даних» (*Data Lake*) і «сховища даних» (*Data Warehouse*). Це дозволяє одночасно зберігати сирі дані у їх первісному вигляді та формувати структуровані набори для аналітики.

Архітектура поділяється на кілька рівнів.

Рівень Bronze. Містить сирі дані з усіх доступних джерел: текстові оголошення, файли із соціальних мереж, зображення та відео, транспортні та міграційні логи, дані з державних реєстрів. На цьому рівні інформація

зберігається без значної попередньої обробки, що гарантує можливість повторного використання для різних цілей.

Рівень Silver. Тут дані очищуються та нормалізуються: видаляються дублікати, стандартизуються телефонні номери (E.164), географічні назви (ISO 3166), часові мітки (ISO 8601). Важливим завданням є приведення текстових корпусів до уніфікованого формату для подальшої обробки методами NLP, а також переведення зображень у стандартизовані формати з контрольними хешами для перевірки автентичності.

Рівень Gold. На цьому рівні дані агрегуються та перетворюються у вигляд, зручний для алгоритмів машинного навчання та інтерактивних дашбордів. Формуються ознаки (features): частота появи певних ключових слів, щільність оголошень у геопросторі, метрики мережевої центральності, ризик-скорингові показники для транзакцій у криптовалюті.

Окреме місце в архітектурі займає баланс між *потоковою обробкою (streaming) та пакетною обробкою (batch processing)*. Пакетна обробка використовується для ретроспективного аналізу, побудови довготривалих трендів та моделей прогнозування.

Для підвищення гнучкості архітектури інтегруються спеціалізовані сховища:

графові бази даних (*Neo4j, JanusGraph*) – для збереження соціальних і транзакційних мереж;

геоінформаційні бази (*PostGIS, GeoMesa***)** – для просторового аналізу маршрутів і «гарячих точок»;

пошукові індекси (*Elasticsearch, Solr***)** – для повнотекстового аналізу оголошень та повідомлень у великих корпусах.

Архітектура має забезпечувати масштабованість, відмовостійкість і безпеку. Використання контейнеризації (*Docker, Kubernetes*) дозволяє гнучко керувати навантаженнями, а застосування технологій шифрування – захищати чутливі дані.

Таким чином, побудова архітектури даних на основі підходу *Data Lakehouse* дозволяє поєднати універсальність збереження різнорідних інформаційних потоків із можливістю глибокого аналітичного оброблення. Це створює фундамент для подальших етапів – контролю якості, пошуку аналітичних патернів та їх візуалізації у вигляді інструментів підтримки рішень.

2.2.2. Якість і управління даними

Аналіз даних у сфері протидії торгівлі людьми є ефективним лише за умови високої якості вхідної інформації. Величезні масиви цифрових слідів містять помилки, дублювання, пропуски чи суперечливі записи. Без належного управління даними результати обробки стають ненадійними, що у криміналістичному чи судовому контексті може призвести до хибних висновків [19,20].

Якість даних у цьому контексті визначається за кількома критеріями: повнотою, точністю, узгодженістю та своєчасністю. Подібні характеристики описані у міжнародному стандарті ISO/IEC 25012:2008 «*Data quality model*» [20].

Контракти та стандартизація даних. У сучасних системах застосовується концепція *data contracts*, що задає вимоги до структури й атрибутів інформації. Контракт даних визначає схему, типи полів і правила їх перевірки» [22]. Це дозволяє уникати неоднозначностей при подальшому аналізі.

Управління метаданими регламентується стандартом ISO/IEC 11179-1 описує рамку реєстрів метаданих» [21].

Автоматизоване тестування якості. Для перевірки використовуються інструменти автоматичного контролю, наприклад *Great Expectations*, що дозволяють відстежувати повноту, унікальність і коректність даних [23]. Такі системи повідомляють аналітику про пропущені значення, дублікати чи відхилення від специфікацій.

Лінійність і простежуваність. Принцип *data lineage* забезпечує відстежуваність усього життєвого циклу даних: від моменту збору до кінцевого використання. Використання таких рішень, як *OpenLineage* чи *Marquez,* дозволяють відстежувати походження і перетворення даних» [24]. Це є особливо

важливим у криміналістичному контексті, коли кожен доказ має бути відтворюваним.

Стратегії та механізми захисту персональної інформації

З огляду на те, що відкриті джерела (OSINT) можуть містити персональні ідентифікатори (наприклад, імена, контактні номери, зображення), надзвичайно важливим є дотримання вимог *GDPR* [9] та українського Закону «Про захист персональних даних» [10]. У практиці це реалізується шляхом мінімізації обсягу зібраної інформації, її маскування чи псевдонімізації, застосуванням рольових моделей доступу та контролем через журнали аудиту.

Значення для аналітичних систем

Якісно зібрані й правильно керовані дані забезпечують достовірність висновків і юридичну силу доказів. Вони є основою для інтеграції з міжнародними системами (*Europol, Interpol*), а також для використання алгоритмів машинного навчання, які вимагають чистих і узгоджених наборів [19].

2.2.3. Аналітичні патерни

У процесі аналізу великих даних щодо торгівлі людьми важливо не лише накопичувати інформацію, але й виявляти закономірності («патерни»), що характеризують поведінку злочинних мереж. Застосування математичних і статистичних методів дозволяє перетворити масиви даних на формалізовані знання, які можуть бути використані для прогнозування та оперативного реагування.

Основні напрями аналітичних патернів

Часові патерни. Аналіз часових рядів дає змогу виявляти циклічність у появі оголошень (денні та тижневі піки, сезонні хвилі). Для цього застосовуються методи аналізу часових рядів, зокрема автокореляційна функція (ACF), що широко використовується у класичних підходах Бокса–Дженкінса [16]:

$$R(k) = \frac{1}{N-k} \sum_{t=1}^{N-k} (x_t - x)(x_{t+k} - x) \qquad (1)$$

де *R(k)* – автокореляція на лагу *k, x_t* – кількість оголошень у момент часу *t, x* – середнє значення.

Просторово-часові кластери. У дослідженнях злочинності широко застосовуються методи кластерного аналізу (DBSCAN та його просторово-часові модифікації ST-DBSCAN), що дають змогу виділяти «гарячі точки» [12, 13]. Для статистичного підтвердження локальних скупчень подій використовується скан-статистика Кулдорфа [11]:

$$\exists q \in D; dist_{spatial}(p,q) \le \varepsilon_{sp},\ dist_{temporal}(p,q) \le \varepsilon_{t},\ |N_{\varepsilon}(p)| \ge minPts \quad (2)$$

де ε_{sp}, ε_t – просторовий і часовий радіуси, *MinPts* – мінімальна кількість точок.

Це дозволяє виявляти «коридори» переміщення жертв чи групові виїзди.

Графові патерни. Аналіз соціальних мереж дозволяє відобразити структуру злочинних угруповань. Методи соціометрії (Wasserman, Faust [14Error: Reference source not found]) дозволяють виділяти ключові вузли:

ступінь вузла:

$$deg(\vartheta) = \sum_{\vartheta \in V}^{\square} a_{\vartheta u} \quad (3)$$

міжпосередницька центральність:

$$G_B(\vartheta) = \sum_{s \ne \vartheta \ne t}^{\square} \frac{\sigma_{st(\vartheta)}}{\sigma_{st}} \quad (4)$$

де σ_{st} – кількість найкоротших шляхів між *s, t,* $\sigma_{st}(v)$ – кількість шляхів, що проходять через вузол *v*.

Аномалії у даних. Для виявлення «нестандартної» поведінки (наприклад, раптове зростання кількості вакансій з одного акаунта) застосовуються методи детекції викидів. Огляд *Chandola* та співавторів охоплює статистичні методи виявлення аномалій» [15]:

$$Z = \frac{x - \mu}{\sigma} \quad (5)$$

де *x* – значення показника (наприклад, кількість оголошень), μ – середнє, σ – стандартне відхилення. Значення $|Z|>3$ інтерпретується як аномалія.

Значення для протидії торгівлі людьми

Виявлення аналітичних патернів у різнорідних даних може підвищувати інформативність аналізу та допомагати визначати напрями подальшої перевірки. Водночас результати математичного або алгоритмічного аналізу слід розглядати як *аналітичні індикатори,* а не як самостійне підтвердження факту злочинної діяльності.

Аналіз часових закономірностей дає змогу встановлювати періоди підвищення або зниження інтенсивності певної інформаційної активності, наприклад появи однотипних оголошень чи повторюваних контактів. Такі спостереження можуть використовуватися для оцінювання динаміки та формування гіпотез щодо можливих змін активності, однак самі по собі не дозволяють прогнозувати поведінку конкретних осіб.

Просторово-часовий аналіз допомагає виявляти зони концентрації спостережень, повторювані просторові зв’язки та зміни їх розподілу в часі. Отримані кластери можуть вказувати на ділянки або напрямки, що потребують додаткового вивчення, проте не повинні автоматично інтерпретуватися як встановлені маршрути переміщення постраждалих осіб.

Графові моделі дають можливість представити взаємозв’язки між інформаційними об’єктами – акаунтами, контактними даними, оголошеннями, адресами електронної пошти, зображеннями чи іншими ідентифікаторами. Метрики центральності та алгоритми виявлення спільнот дозволяють виділяти структурно значущі вузли та групи пов’язаних об’єктів. Водночас така структура відображає зв’язки в досліджуваних даних і не є самостійним доказом існування або внутрішньої організації злочинної мережі.

Методи виявлення аномалій, своєю чергою, допомагають знаходити спостереження, які істотно відрізняються від типової поведінки досліджуваної сукупності. Такі випадки можуть отримувати підвищений аналітичний пріоритет, але їх нетиповість не свідчить автоматично про протиправний характер і потребує перевірки за іншими джерелами.

Отже, застосування часових, просторово-часових, графових і статистичних методів [11, 12, 13, 14, 15, 16] створює формалізовану основу для виявлення повторюваних закономірностей, зв’язків та нетипових спостережень у великих масивах даних. Їх практичне значення полягає насамперед у *підтримці аналітичної діяльності, пріоритизації інформації та формуванні перевірюваних гіпотез.* За наявності достатніх і якісних даних такі методи можуть також використовуватися для дослідження динаміки процесів і побудови прогнозних моделей, однак отримані результати мають оцінюватися з урахуванням невизначеності, якості вихідних даних та необхідності експертної перевірки.

2.2.4. Візуалізація й інструменти диспетчера

Великі дані стають корисними лише тоді, коли їх результати представлені у наочній і зрозумілій для користувача формі. Візуалізація є ключовим етапом перетворення числових та текстових масивів у інформаційно-аналітичні знання, придатні для практичного використання оперативними аналітиками та диспетчерами правоохоронних органів. Вона виконує роль інтерфейсу між складними алгоритмами та практикою прийняття рішень [17].

Геоінформаційні карти

Найбільш поширеною формою представлення даних у сфері протидії торгівлі людьми є карти.

Теплові карти (heatmaps). Застосування ядерної оцінки щільності (KDE) дозволяє виявляти просторові «гарячі точки» оголошень чи активності акаунтів. KDE використовується для оцінки функції щільності й дозволяє візуально виділити регіони з підвищеною активністю [25]:

$$f(x) = \frac{1}{nh} \sum_{i=1}^{n} K\left(\frac{x - x_i}{h}\right) \qquad (6)$$

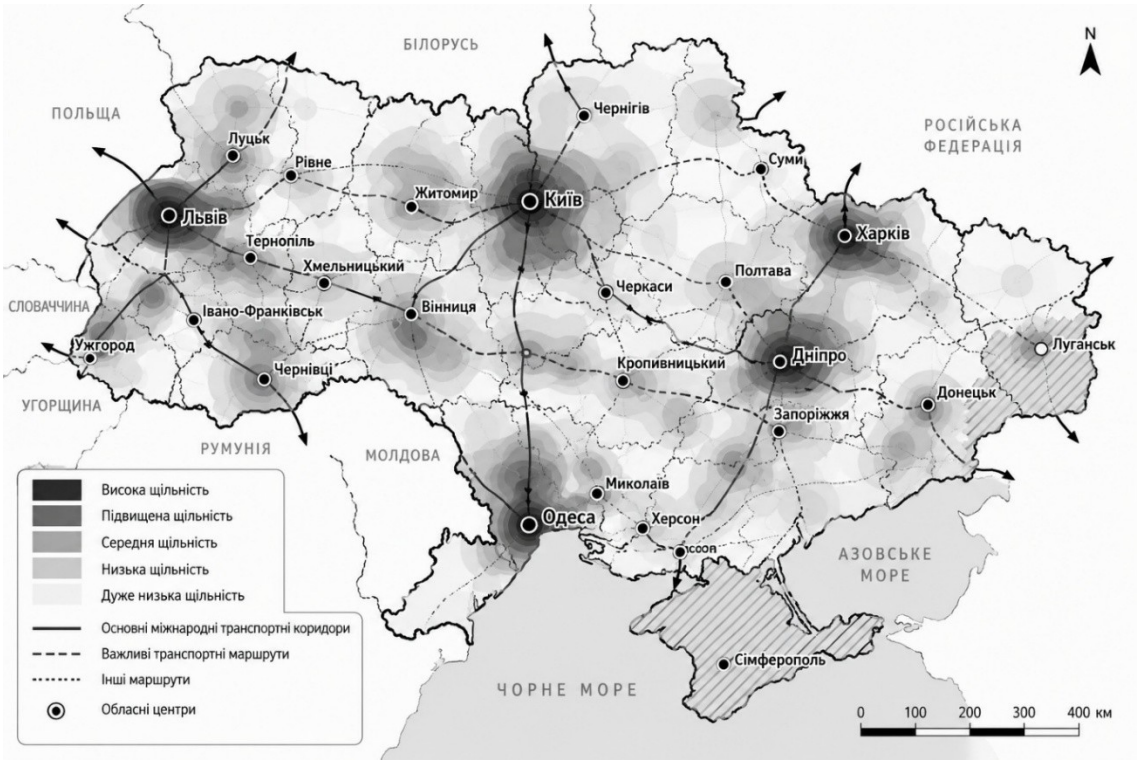


Рис. 2.1. Приклади візуалізації теплових карти (heatmaps)

Маршрутні карти. На основі транспортних і міграційних даних можна будувати схеми переміщень осіб, виявляти транзитні коридори та узгоджувати їх з часовими інтервалами.

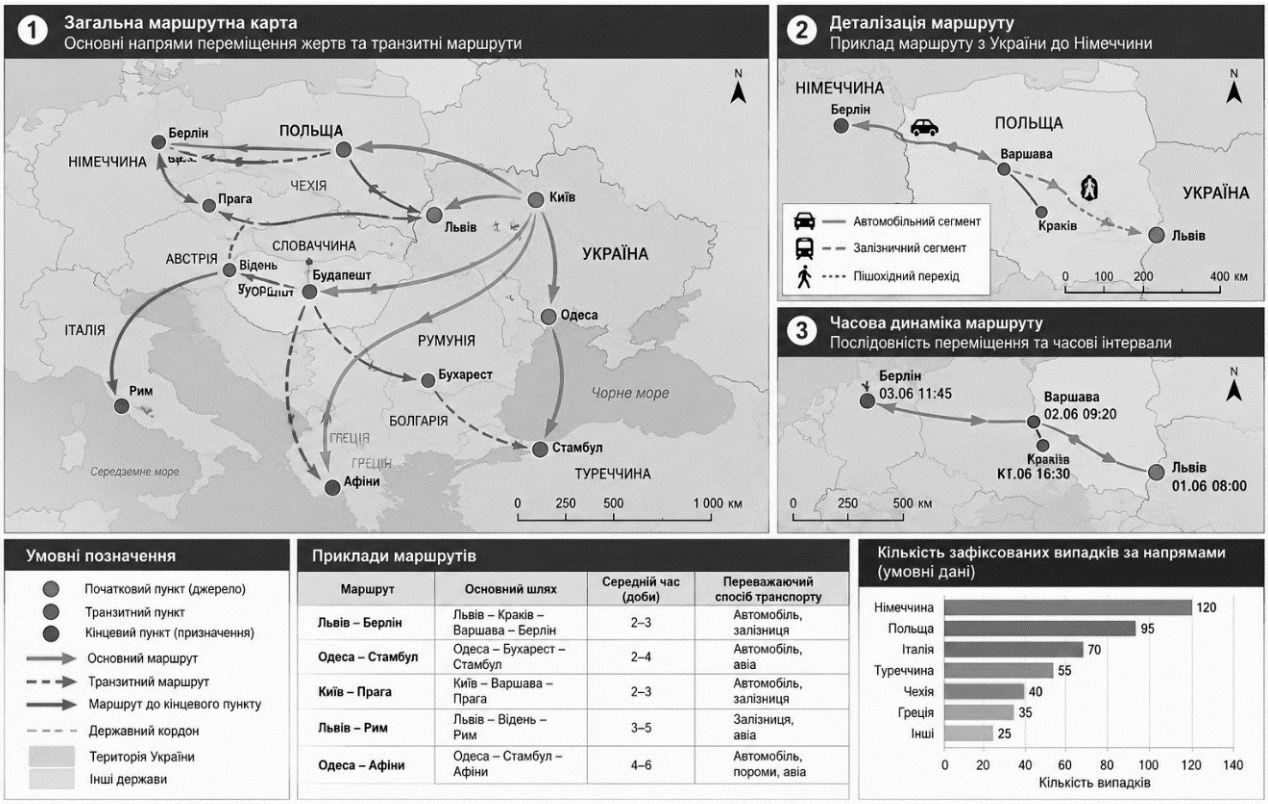


Рис. 2.2. Приклади візуалізації маршрутних карт

Часові візуалізації

Часові графіки й інтерактивні шкали часу (timelines) допомагають виявляти динаміку появи оголошень та циклічні закономірності. Використання ковзних середніх чи автокореляцій (Box, Jenkins [16]) дозволяє ідентифікувати сезонні піки. Наприклад, улітку збільшується кількість оголошень щодо сезонної роботи за кордоном, що є типовим ризиком вербування.

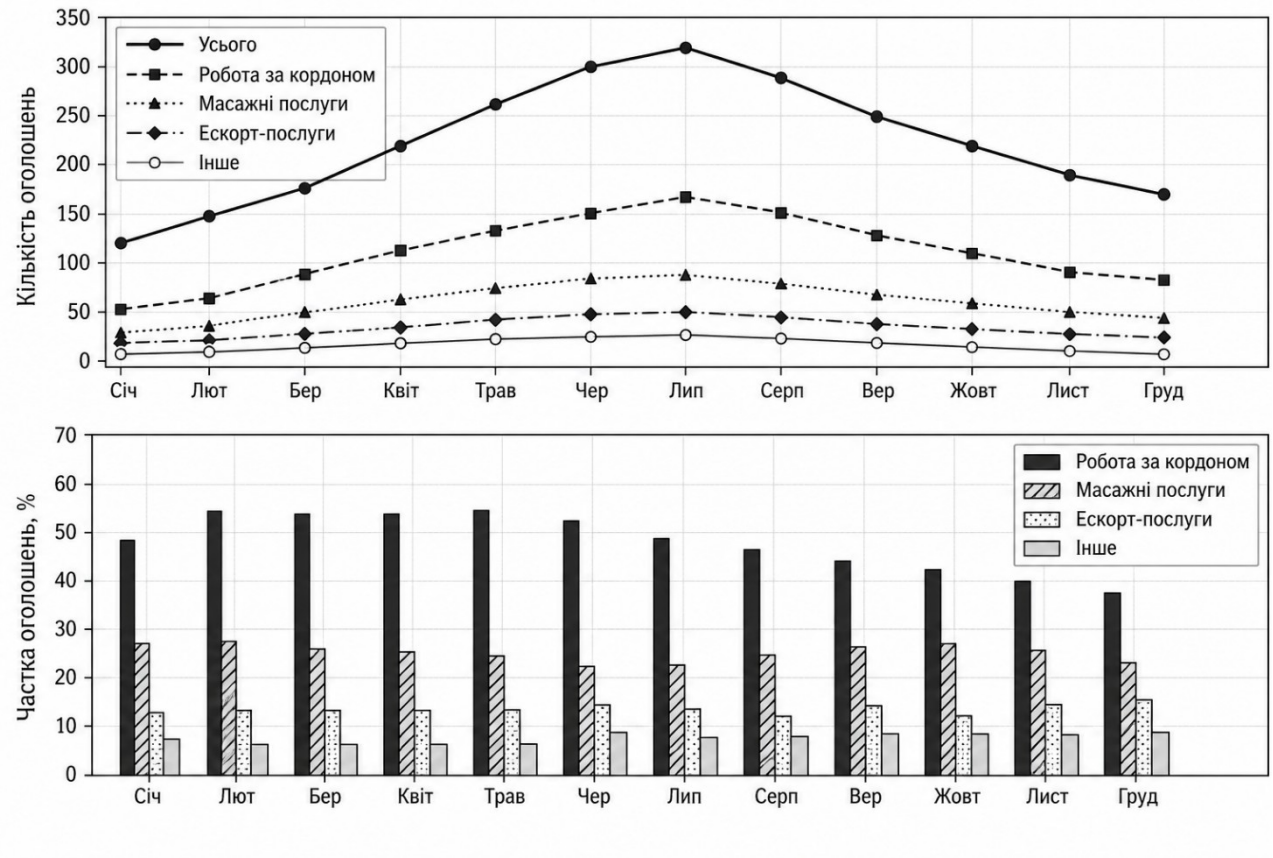


Рис. 2.3. Приклади часової візуалізації та кластерізації оголошень

Часовий графік – показує динаміку кількості підозрілих оголошень за днями (можна демонструвати сезонність або пікові навантаження).

Кластеризація оголошень (k-Means) – ілюструє групування профілів за ознаками (наприклад, текст, географія, контакти), що дозволяє виділяти типові схеми вербування.

Графові діаграми

Соціальні мережі та комунікаційні зв’язки зручно представляти у вигляді графів. Інтерактивні графові візуалізації дозволяють аналітику:

- виділяти кластери тісно пов’язаних акаунтів;

- ідентифікувати «центральні вузли» за показниками ступеня та міжпосередницької центральності;

- аналізувати транзакційні мережі (наприклад, криптовалютні).

Застосування методів виявлення спільнот (Fortunato, Hric [26]) дозволяє знаходити підгрупи, що відображають внутрішню структуру злочинної мережі.

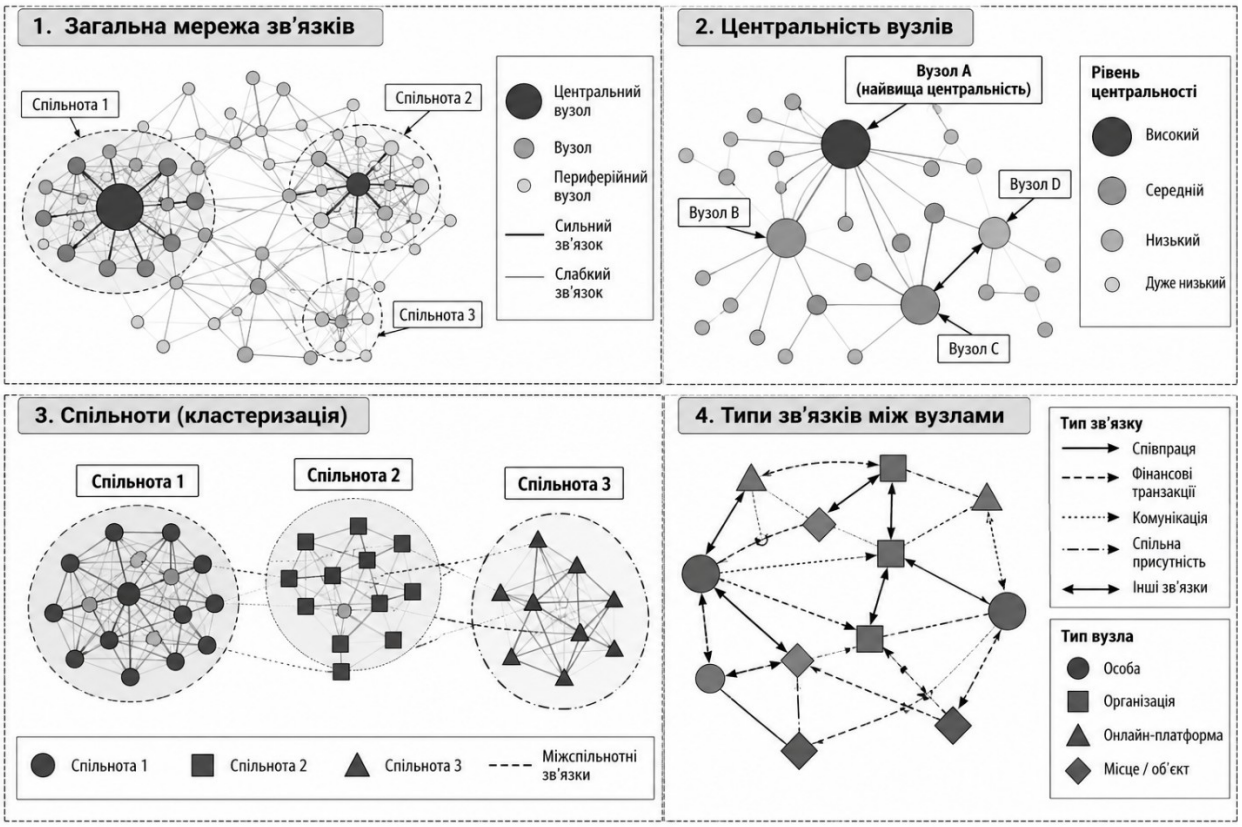


Рис. 2.4 Графові діаграми

Графові моделі дають змогу наочно представляти зв'язки між інформаційними об'єктами, зокрема обліковими записами, контактними даними, оголошеннями, зображеннями, фінансовими ідентифікаторами та іншими сутностями, виявленими під час аналізу. Їх використання допомагає перейти від розгляду окремих інформаційних фрагментів до дослідження структури взаємозв'язків між ними.

Одним із напрямів такого аналізу є виявлення груп щільно пов'язаних вузлів. Наприклад, кілька облікових записів можуть використовувати однакові контактні дані, повторювати ті самі тексти чи зображення або бути пов'язаними з одними й тими самими інформаційними ресурсами. Формування такого кластера свідчить про наявність структурного зв'язку між об'єктами, але саме по собі не

підтверджує їх належність до спільної організації чи причетність до протиправної діяльності.

Для оцінювання ролі окремих вузлів у графі використовуються показники центральності. Ступінь вузла (*degree centrality*) характеризує кількість його безпосередніх зв'язків, тоді як міжпосередницька центральність (*betweenness centrality*) показує, наскільки часто вузол розташовується на найкоротших шляхах між іншими елементами мережі. Високе значення таких показників дозволяє виділити структурно значущі об'єкти для подальшого аналізу, однак не дає підстав автоматично визначати їх як координаторів або організаторів певної діяльності.

Додаткові можливості надають методи виявлення спільнот (*community detection*), які групують вузли за щільністю внутрішніх зв'язків. Для цього можуть застосовуватися, зокрема, алгоритм *Louvain*, алгоритм *Leiden* або метод *Girvan–Newman*, заснований на аналізі міжпосередницької центральності ребер. Такі методи дозволяють виявляти внутрішню структуру самого графа та виділяти групи інформаційних об'єктів із підвищеною взаємопов'язаністю. Праці Fortunato та Hric доцільніше розглядати як теоретико-методологічну основу дослідження методів виявлення спільнот, а не як назви окремих алгоритмів.

Графовий підхід може застосовуватися і до аналізу фінансових та криптовалютних даних за умови законного доступу до відповідної інформації. У такому графі вузлами можуть бути адреси гаманців або інші фінансові ідентифікатори, а ребрами – зафіксовані транзакційні зв'язки. Повторювані маршрути переказів, концентрація зв'язків навколо певних вузлів або формування стійких груп можуть розглядатися як аналітичні індикатори, що потребують подальшої перевірки. Нетипова структура транзакцій сама по собі не свідчить про їх злочинне походження.

Таким чином, графові моделі доцільно використовувати не для автоматичного «виявлення злочинних структур», а для встановлення структурних закономірностей, пов'язаних груп і значущих інформаційних

вузлів. Вони допомагають формувати та перевіряти аналітичні гіпотези, зіставляти результати з іншими джерелами й визначати об’єкти, які потребують поглибленого дослідження. Остаточні висновки щодо характеру встановлених зв’язків мають ґрунтуватися на сукупності незалежно перевірених даних.

Інтерактивні дашборди

інтерактивні панелі моніторингу (*dashboards)*:

- відображення KPI (кількість нових оголошень, кількість повторів контактів, інтенсивність транзакцій);
- фільтри за регіонами, часовими інтервалами, типами сигналів;
- система автоматизованих сповіщень.

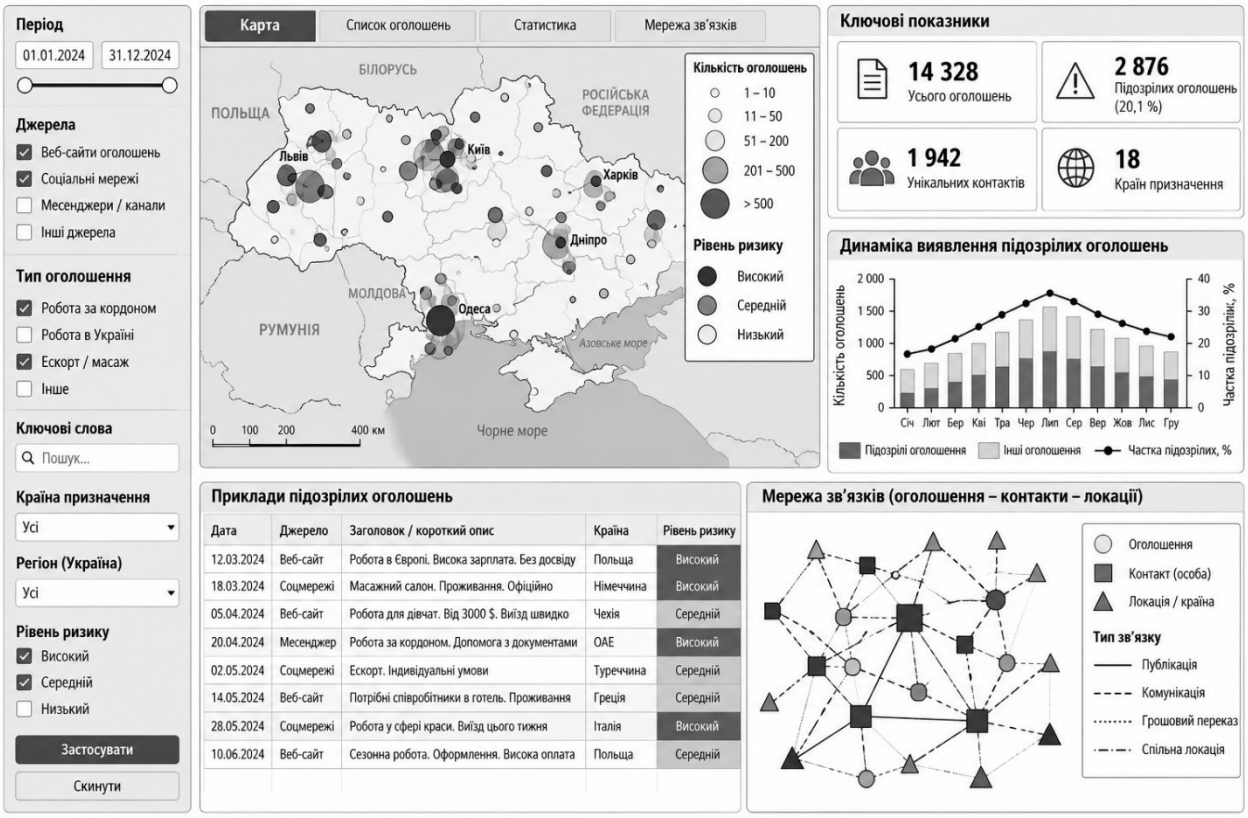


Рис. 2.5 Інтерактивні дашборди

У системах такого типу сповіщення будуються на основі порогових моделей:

$$Alert = \begin{cases} 1, & якщо \ \ x_t > \mu + z \cdot \sigma \\ 0, & інакше, \end{cases} \tag{7}$$

де x_t_ – поточне значення показника, μ – середнє значення, σ – стандартне відхилення, z – параметр чутливості.

Інструменти диспетчера

Диспетчер є кінцевим користувачем системи. Він отримує сповіщення у режимі реального часу про нові ризикові оголошення, пріоритизацію сигналів за допомогою багатофакторного ризик-скорингу та сценарне моделювання, яке дозволяє оцінювати навантаження на ресурси при зміні умов (наприклад, різке зростання потоку мігрантів).

Важливо, щоб диспетчерські інтерфейси були інтегровані із картами, графами та часовими шкалами, забезпечуючи багатовимірний огляд ситуації.

Візуалізація та інтегровані диспетчерські інструменти перетворюють результати складної аналітики у зручну форму для оперативного використання. Вони скорочують час реагування, підвищують якість рішень і дозволяють синхронізувати аналітичний та практичний рівні протидії торгівлі людьми.

2.2.5. Приклади запитів/обчислень

Ефективність системи аналізу великих даних визначається не лише архітектурою чи якістю вхідної інформації, але й практичною можливістю здійснювати конкретні обчислення та отримувати прикладні результати. У цьому контексті доречно розглянути приклади запитів, які демонструють, яким чином OSINT-дані інтегруються в середовище Big Data та стають основою для виявлення підозрілих патернів.

1. Виявлення повторюваних контактів у вакансіях

Телефонні номери часто використовуються для масових оголошень з різними текстами, але одним організатором. Запит у SQL (PostgreSQL/PostGIS) дозволяє швидко знайти такі збіги:

```
SELECT phone_number, COUNT(*) AS total_ads, array_agg(ad_id) AS ad_list
FROM job_ads
GROUP BY phone_number
HAVING COUNT(*) > 5
ORDER BY total_ads DESC;
```

Цей приклад виявляє «центри тяжіння» – телефони, що повторюються у багатьох оголошеннях, і формує список відповідних публікацій [27].

2. Просторовий пошук «гарячих точок»

Для ідентифікації зон підвищеної концентрації оголошень використовується підхід ядерного оцінювання щільності ймовірнісного розподілу (Kernel Density Estimation, KDE). Його реалізація у середовищах PyQGIS та PostGIS може мати такий вигляд:

```
SELECT ST_KDE(geom, 0.01)
FROM ads_points
WHERE date >= '2025-01-01' AND date <= '2025-03-31';
```

У результаті формується растровий шар щільності, де ділянки з найвищими значеннями відображають просторові «гарячі точки» [26].

3. Часовий аналіз появи оголошень

Для ідентифікації циклічності можна використати агрегування за днями чи тижнями.

```
SELECT date_trunc('week', published_at) AS week, COUNT(*) AS ads_count
FROM job_ads
GROUP BY week
ORDER BY week;
```

Отриманий ряд дозволяє будувати часові графіки та застосовувати автокореляцію для виявлення повторюваних інтервалів [16Error: Reference source not found].

4. Побудова графа контактів

Інтеграція даних у графову базу (наприклад, Neo4j) дозволяє формувати мережеві моделі:

```
MATCH (a:Ad)-[:HAS_PHONE]->(p:Phone)
MATCH (a)-[:HAS_EMAIL]->(e:Email)
RETURN p, e, COUNT(*) AS links
ORDER BY links DESC;
```

Запит знаходить спільні контактні вузли; центральність потребує окремого розрахунку» [14, 29].

5. Виявлення аномалій у транзакціях

Для транзакцій у криптовалюті можна застосувати статистичні критерії виявлення аномалій. Наприклад, через Z-оцінку:

$$Z = \frac{x - \mu}{\sigma} \tag{8}$$

де x – сума транзакції, μ – середнє значення, σ – стандартне відхилення. Значення $|Z|$, що перевищує встановлений статистичний поріг, може використовуватися для попереднього відбору нетипових спостережень, які потребують додаткового аналізу.

Реалізація у SQL:

```
SELECT tx_id, amount,
       (amount - avg_amount)/stddev_amount AS z_score
FROM crypto_tx
WHERE ABS((amount - avg_amount)/stddev_amount) > 3;
```

Це дозволяє відбирати нетипові операції для подальшої перевірки» [30].

Наведені приклади демонструють, як практичні запити й обчислення реалізують аналітичні завдання у системах Big Data. Вони охоплюють різні аспекти – від текстової та просторової аналітики до графових моделей і фінансового моніторингу. Поєднання таких запитів формує «набір інструментів» для аналітика, який дозволяє перетворювати великі масиви розрізненої інформації на докази та прогностичні моделі.

2.3. Машинне навчання та штучний інтелект у виявленні торгівлі людьми

2.3.1. Класифікація текстових повідомлень

Аналіз текстів, що супроводжують торгівлю людьми, є одним із найважливіших напрямів використання штучного інтелекту. У більшості випадків вербування починається з публікації оголошення у відкритому доступі – на сайтах працевлаштування, у соціальних мережах чи месенджерах. Тому класифікацію можна застосовувати для попереднього відбору текстів; результат потребує оцінювання» [31, 34].

Методи представлення текстів

Для побудови моделей машинного навчання тексти необхідно подати у числовій формі:

Мішок слів (Bag-of-Words). Класичний підхід, де кожен документ подається як вектор частот вживання слів. Недолік – ігнорується контекст.

*TF-IDF (Term Frequency – Inverse Document Frequency)***.** Дає змогу зважувати слова залежно від їхньої важливості:

$$TF\text{-}IDF(t,d) = TF(t,d) \cdot \log \frac{N}{DF(t)} \quad (9)$$

де *TF(t,d)* – частота терміну *t* у документі *d, N* – кількість документів, *DF(t)* – кількість документів, де зустрічається термін *t* [32].

Векторизація слів (Word2Vec, GloVe). Вектори відображають семантичну близькість слів, дозволяючи алгоритмам враховувати контекст.

Трансформерні моделі (BERT, GPT). Найсучасніший підхід, що враховує не лише значення слів, але й контекст усієї фрази [32, 34]

Алгоритми класифікації

Залежно від складності задачі застосовуються різні алгоритми:

Логістична регресія. Добре працює з TF-IDF, забезпечує інтерпретованість результатів.

SVM (Support Vector Machines). Виявляє нелінійні закономірності у текстах.

Random Forest / XGBoost. Використовуються для багатокласової класифікації.

Нейронні мережі. LSTM і трансформери (BERT, RoBERTa) показують найкращі результати на великих корпусах.

Формально задача класифікації формулюється так: маючи множину текстів $D=\{d1,d2,...,dn\}$, кожен документ d_i подається у вигляді вектора ознак $x_i \in R^m$. Метою є побудова функції:

$$f: R^m \to [0;1] \quad (10)$$

де 0 – нейтральне оголошення, 1 – потенційно пов’язане з вербуванням.

Приклад SQL/NLP-запиту

У системі, інтегрованій із PostgreSQL та модулем Python (PL/Python), можна реалізувати просту класифікацію:

```
SELECT ad_id, classify_text(content) AS risk_label
FROM job_ads
WHERE published_at > '2025-01-01';
```

Функція `classify_text()` може базуватися на попередньо навчений моделі TF-IDF + логістична регресія. У більш просунутих системах вона підключає REST API до моделі BERT.

Оцінка якості класифікації

Результати моделей оцінюються за метриками:

a. Точність (Accuracy): $\frac{TP+TN}{TP+TN+FP+FN}$

b. Прецизійність (Precision): $\frac{TP}{TP+FP}$

c. Повнота (Recall): $\frac{TP}{TP+FN}$.

d. F1-score: гармонійне середнє *Precision* та *Recall.*

У задачі виявлення торгівлі людьми важливішим є **Recall** (щоб не пропустити небезпечні оголошення), навіть за умови більшої кількості хибнопозитивних спрацювань.

Класифікація текстових повідомлень є базовим елементом у системі ШІ для протидії торгівлі людьми. Вона забезпечує відбір підозрілих об’яв для подальшого аналізу, дозволяє зменшити навантаження на аналітиків і створює умови для масштабування системи. Використання трансформерних моделей відкриває можливість контекстного аналізу, що значно підвищує ефективність розпізнавання вербувальних патернів [33].

2.3.2. Виявлення аномалій у даних

Однією з ключових задач у виявленні торгівлі людьми є пошук нетипових подій, які вирізняються серед масиву «звичайних» даних. Це можуть бути раптові сплески оголошень із одного акаунта, аномальні фінансові транзакції, поява контактних номерів у незвичних регіонах чи нетипові маршрути переміщення. Виявлення таких відхилень неможливе звичайними методами фільтрації й потребує застосування спеціалізовані алгоритми машинного навчання, розроблені для виявлення відхилень та аномальних патернів у даних (*anomaly detection*) [15].

Формалізація задачі

Нехай $X=\{x_1,x_2,\ldots,x_n\}$ – множина об'єктів, де кожен $x_i \in R^m$ є вектором ознак (наприклад, кількість оголошень, середня довжина тексту, географічні координати). Метою є побудова функції:

$$f(x_i)=\begin{cases} 0, \text{ якщо } x_i \text{ належить до нормальних} \\ 1, \text{ якщо } x_i \text{ є аномалією} \end{cases} \quad (11)$$

Методи виявлення аномалій

1. **Z-score (статистичний підхід).** Використовується для даних з приблизно нормальним розподілом.

$$Z=\frac{x-\mu}{\sigma} \quad (12)$$

де x – значення ознаки, μ – середнє, σ – стандартне відхилення. За обраного порога |Z| > 3 спостереження позначають як потенційний викид» [3Error: Reference source not found4].

2. **Isolation Forest.** Метод базується на ідеї, що аномалії легше «ізолювати», ніж нормальні дані. Будуються випадкові дерева, і середня глибина, на якій елемент ізольовано, є індикатором його «аномальності».

3. Аномалії отримують високі значення **anomaly score** [36].

4. **Local Outlier Factor (LOF).** Визначає «аномальність» об'єкта за відношенням його локальної щільності до середньої щільності сусідів. Якщо

$$LOF(p)>1 \quad (13)$$

то об'єкт *p* розглядається як потенційна аномалія [37].

4. **One-Class SVM.** Алгоритм шукає гіперплощину, що відокремлює більшість даних від початку координат. Об'єкти, що лежать «поза межею», класифікуються як аномальні. Використовується для багатовимірних ознак (тексти, графові метрики, транзакційні дані) [38].

Приклади

SQL-запит для фінансових транзакцій:

```
SELECT tx_id, amount,
       (amount - avg(amount) OVER()) / stddev(amount) OVER() AS z_score
FROM crypto_tx
WHERE ABS((amount - avg(amount) OVER()) / stddev(amount) OVER()) > 3;
```

Цей запит виділяє транзакції з відхиленням понад три стандартні відхилення від середнього:

```
from sklearn.ensemble import IsolationForest
model = IsolationForest(contamination=0.02)
model.fit(X)
y_pred = model.predict(X)  # -1 = аномалія, 1 = нормальний
```

Використання в контексті протидії торгівлі людьми

Методи виявлення аномалій можуть застосовуватися для пошуку нетипових змін у великих масивах даних, які потребують додаткової аналітичної уваги. Наприклад, різке збільшення кількості однотипних публікацій з одного або кількох пов’язаних акаунтів може свідчити про зміну характеру інформаційної активності. Проте така активність сама по собі не є ознакою торгівлі людьми і має оцінюватися разом з іншими доступними даними.

У просторово-часовому аналізі аномалією може вважатися поява нетипових маршрутів або незвичних змін у географічному розподілі спостережень. Такі результати дозволяють виділяти напрямки, які потребують додаткової перевірки, але не дають підстав автоматично трактувати їх як маршрути переміщення постраждалих осіб.

Подібний підхід може застосовуватися і до фінансових даних за умови законного доступу до них. Незвична сума, частота, послідовність або структура транзакцій може бути визначена алгоритмом як статистично нетипова порівняно зі звичайним профілем операцій. Водночас аномальність транзакції не свідчить про її протиправний характер, а лише визначає її як об’єкт для подальшого аналізу.

Таким чином, алгоритми детекції аномалій доцільно розглядати як інструмент раннього виявлення нетипових інформаційних, просторових або фінансових патернів, а не як засіб автоматичного встановлення фактів торгівлі людьми. Особливо корисними вони можуть бути за відсутності достатньої кількості попередньо розмічених даних, коли неможливо сформувати повноцінні навчальні вибірки з достовірно визначеними класами. У таких випадках статистичні методи та алгоритми машинного навчання без учителя допомагають

пріоритезувати спостереження для подальшої експертної перевірки. Поєднання різних методів аналізу підвищує можливості виявлення нетипових процесів, однак остаточні висновки повинні ґрунтуватися на сукупності незалежно перевірених даних і враховувати можливість хибнопозитивних результатів [15, 35].

2.3.3. Кластеризація користувачів і оголошень

У багатьох випадках злочинна діяльність проявляється не в окремих повідомленнях, а у цілих групах, що мають спільні характеристики. Завдання кластеризації зводиться до ідентифікації подібних груп серед великої кількості об'єктів (користувачів, оголошень, акаунтів), не маючи наперед визначених класів. Це дозволяє виявляти групи подібних профілів чи оголошень для перевірки» [39].

Формалізація задачі

Нехай $X=\{x_1,x_2,\ldots,x_n\}$ – множина об'єктів, де кожен об'єкт $xi \in R^m$ описується вектором ознак (довжина тексту, кількість згадувань контактів, географічні координати, лінгвістичні патерни). Завдання полягає у знаходженні відображення:

$$f: X \to \{C_1,\ C_2,\ldots C_k\} \qquad (14)$$

де Cj – кластер, який об'єднує подібні об'єкти.

Алгоритми кластеризації

1. **k-Means.** Найпоширеніший метод, що мінімізує відстань об'єктів до центроїдів:

$$J=\sum_{i=1}^{n} \square \sum_{j=1}^{k} ||x_i - \mu_j|| \qquad (14)$$

де r_{ij}=1, якщо x_i належить кластеру C_j, інакше 0, μ_j – центр кластера [40]. Застосовується для сегментації оголошень за стилістикою тексту чи ціною.

2. **Density-Based Spatial Clustering of Applications with Noise, DBSCAN**. Формує кластери, виходячи з локальної щільності точок, що дозволяє виявляти групи довільної конфігурації. Якщо кількість сусідніх об'єктів у заданому радіусі ε перевищує поріг *MinPts* [12], то точка класифікується як така,

що належить кластеру. Цей підхід добре зарекомендував себе при роботі з просторовими даними, наприклад для ідентифікації «гарячих зон» активності.

3. **HDBSCAN (Hierarchical DBSCAN).** Алгоритмічне розширення DBSCAN дозволяє створювати ієрархічну організацію кластерів і придатне для аналізу багатовимірних та складно структурованих даних. Найчастіше його використовують для дослідження мережевих структур і корпусів текстів значного обсягу [41].

Приклади застосування

Кластеризація користувачів. Акаунти з подібними номерами телефонів, адресами *e-mail*, шаблонами текстів можуть групуватися в один кластер, що вказує на «ферми акаунтів».

Кластеризація оголошень. Оголошення з подібними ключовими словами, стилістикою й географією можна об’єднувати для виявлення типових схем вербування.

Просторовий аналіз. DBSCAN виділяє скупчення оголошень у прикордонних регіонах, що може сигналізувати про транзитні пункти.

Приклад у Python (HDBSCAN)

```
import hdbscan
import numpy as np
# X – матриця ознак (наприклад, TF-IDF текстів оголошень)
clusterer = hdbscan.HDBSCAN(min_cluster_size=5)
labels = clusterer.fit_predict(X)
print(set(labels))  # -1 означає "шум" (аномалії)
```

У результаті аналітик отримує групи «подібних» об’яв, а також аномальні випадки (шум), що заслуговують окремої уваги.

Використання у протидії торгівлі людьми

Методи кластеризації можуть застосовуватися для виявлення груп інформаційних об’єктів, які мають подібні характеристики або демонструють схожі моделі поведінки. Йдеться, зокрема, про облікові записи, оголошення, контактні дані чи інші цифрові сутності, між якими простежуються спільні ознаки. Формування такого кластера може свідчити про структурну подібність

або потенційний взаємозв’язок між об’єктами, однак саме по собі не підтверджує існування організованої вербувальної мережі.

Кластеризація також дає змогу виявляти повторювані сценарії інформаційної активності, наприклад сезонні, регіональні або тематичні групи оголошень. Такі закономірності можуть допомагати аналітику формувати гіпотези щодо характеру та динаміки певних процесів і визначати напрями для подальшої перевірки. Водночас подібність текстів, часу публікації або географії розміщення не повинна автоматично трактуватися як ознака спільного походження чи протиправної діяльності.

Окреме значення має виявлення спостережень, які не входять до сформованих кластерів і суттєво відрізняються від основної сукупності. Такі об’єкти доцільніше розглядати як нетипові випадки або інформаційні винятки, що можуть потребувати додаткової уваги. Їхня нетиповість не означає підвищеної небезпеки сама по собі, але може бути корисним сигналом для поглибленого аналізу.

Кластеризація дозволяє перейти від аналізу окремих елементів до вивчення структурних груп. Це дає змогу виявляти закономірності, які залишаються непомітними при індивідуальному аналізі, та створювати «профілі» злочинних схем. Комбінація k-Means, DBSCAN та HDBSCAN забезпечує як просту сегментацію, так і виявлення складних, багатовимірних патернів [12, 40, 41, 42].

Таким чином, кластеризація у сфері протидії торгівлі людьми доцільна насамперед як інструмент структурування великих масивів даних, виявлення подібних груп, повторюваних патернів і нетипових спостережень. Отримані результати мають використовуватися для підтримки аналітичної роботи та перевірки гіпотез, а не для автоматичного визначення осіб або груп як причетних до злочинної діяльності.

Висновок до розділу 2

Аналіз можливостей сучасних інформаційних технологій у сфері протидії торгівлі людьми свідчить, що найбільшу практичну цінність має не окремий

інструмент, а поєднання різних методів оброблення та зіставлення даних. Відкриті джерела, просторові дані, текстові матеріали, зображення, контактні ідентифікатори та, за наявності законних підстав, фінансова інформація формують різнорідне інформаційне середовище, у якому значущі ознаки часто проявляються не ізольовано, а через повторюваність, взаємозв'язки та нетипові комбінації.

У цьому контексті OSINT доцільно розглядати насамперед як засіб первинного виявлення інформаційних сигналів і формування аналітичних гіпотез. Повторювані контактні дані, подібні тексти, повторне використання зображень або збіги між різними платформами можуть свідчити про структурний зв'язок між окремими інформаційними об'єктами. Водночас жодна з таких ознак сама по собі не підтверджує факт торгівлі людьми або причетність конкретної особи до протиправної діяльності. Їх значення виникає лише у поєднанні з іншими перевіреними даними та відповідним контекстом.

Застосування технологій Big Data розширює можливості такого аналізу за рахунок інтеграції великих і різнорідних масивів інформації. Основною перевагою є можливість виявляти повторювані часові, просторові, мережеві та поведінкові закономірності, які складно встановити під час ручного опрацювання. Разом із тим масштабування аналітики підвищує вимоги до якості даних, їх походження, нормалізації, простежуваності та правомірності використання. Недостатньо якісні або упереджені вихідні дані можуть призводити до хибних закономірностей і, відповідно, необґрунтованих аналітичних висновків.

Методи машинного навчання та штучного інтелекту доцільно розглядати як інструменти підтримки аналітичної діяльності, а не як механізми автоматичного встановлення злочинної поведінки. NLP-моделі можуть допомагати структурувати тексти, виявляти семантичну подібність, розпізнавати сутності та відбирати повідомлення для подальшої перевірки. Алгоритми кластеризації дозволяють групувати об'єкти за подібними характеристиками, а методи виявлення аномалій – визначати нетипові спостереження. Проте кластер,

аномалія або результат автоматичної класифікації є лише аналітичним сигналом і потребує змістовної перевірки.

Еефективність інформаційно-аналітичної системи визначається не лише точністю алгоритмів, а й здатністю забезпечити пояснюваність результатів, простежуваність джерел, можливість експертної перевірки та дотримання принципів мінімізації даних, пропорційності й недискримінації. Особливо це важливо у сфері протидії торгівлі людьми, де помилковий висновок може безпосередньо впливати на права, безпеку та гідність конкретної людини.

Отже, сучасні інформаційні технології створюють значний потенціал для підвищення ефективності аналітичної роботи, однак їх практичне застосування має ґрунтуватися на принципі *«алгоритм формує сигнал – людина перевіряє контекст – рішення приймається на основі сукупності верифікованих даних».* Саме така модель дозволяє поєднати масштабованість автоматизованого аналізу з вимогами правової обґрунтованості, наукової коректності та захисту прав людини.

РОЗДІЛ 3. КІБЕРБЕЗПЕКОВІ АСПЕКТИ ДОКУМЕНТУВАННЯ ТОРГІВЛІ ЛЮДЬМИ

3.1. Цифрова криміналістика у розслідуванні торгівлі людьми

Сучасні форми торгівлі людьми дедалі частіше залишають цифрові сліди. Вони можуть виникати під час публікації пропозицій працевлаштування, комунікації через соціальні мережі та месенджери, передавання фотографій і відеоматеріалів, використання електронних платіжних сервісів або криптовалют. Водночас наявність певного цифрового об’єкта, контакту чи транзакції сама по собі не підтверджує факту торгівлі людьми. Значення цифрової криміналістики полягає у тому, щоб належним чином виявити, зафіксувати, зберегти, дослідити та інтерпретувати цифрові дані у сукупності з іншими матеріалами провадження.

Особливість цифрових слідів полягає у їхній нестійкості. Вебсторінка може бути змінена або видалена, повідомлення – зникнути, файл – зазнати редагування, а метадані – змінитися внаслідок звичайного копіювання чи оброблення. Тому принципове значення має фіксація стану цифрового об’єкта на момент його отримання та документування подальших операцій із ним.

Контроль цілісності та фіксація часу

Одним із базових засобів контролю цілісності цифрових матеріалів є криптографічне хешування. Для файлу обчислюється хеш-значення, наприклад за алгоритмом *SHA-256* або *SHA-3* [44, 46]. Якщо надалі вміст файлу змінюється, змінюється і відповідне хеш-значення. Це дозволяє перевірити, чи залишався конкретний цифровий об’єкт незмінним після його фіксації.

Разом із тим хешування не слід трактувати як автоматичне підтвердження автентичності або правдивості змісту. Воно засвідчує насамперед цілісність конкретної копії від моменту, коли для неї було обчислено контрольне значення**.** Якщо вихідний файл був змінений до його отримання, хешування саме по собі цього не встановить.

Не менш важливою є фіксація часу отримання матеріалу. Для цього можуть використовуватися системні часові мітки, журнали подій, електронні підписи та сервіси довіреного таймстемпінгу. Такі механізми допомагають

підтвердити, що певний цифровий об’єкт існував або був зафіксований у визначений момент. У технічній літературі розглядаються також рішення на основі розподілених реєстрів [43], однак сам факт розміщення хешу в блокчейні не визначає процесуальної допустимості матеріалу і не підтверджує достовірність його змісту. Це лише один із можливих способів додаткової фіксації контрольного значення та часу.

Простежуваність роботи з цифровими матеріалами

Для цифрової криміналістики критично важливо мати можливість відтворити весь життєвий цикл цифрового об’єкта: звідки він був отриманий, ким і коли зафіксований, за допомогою яких засобів створено копію, де вона зберігалася, які операції з нею виконувалися та хто мав до неї доступ. Така система документування відповідає принципу *chain of custody* – простежуваності поводження з доказовими матеріалами [44, 48].

Належне ведення такого ланцюга не «гарантує» автоматичної допустимості доказу, однак дозволяє перевірити його походження, цілісність і умови оброблення. Це особливо важливо для цифрових матеріалів, оскільки їх можна легко копіювати, передавати й модифікувати без очевидних зовнішніх ознак.

У справах про торгівлю людьми джерелом інформації можуть бути, наприклад, оголошення, історія комунікації, файли з мобільних пристроїв, фотографії, відеозаписи, журнали браузера або відомості про електронні платежі. При цьому скріншот чи окреме повідомлення не слід розглядати ізольовано як самодостатній доказ певної події. Значення такого матеріалу залежить від можливості підтвердити його походження, контекст, спосіб отримання та взаємозв’язок з іншими даними.

Інструменти цифрової криміналістики

Для дослідження цифрових носіїв застосовуються спеціалізовані програмні комплекси.

Autopsy використовується для аналізу файлових систем, пошуку цифрових артефактів, дослідження образів носіїв та відновлення частини видалених даних.

FTK (Forensic Toolkit) надає засоби індексування, пошуку та аналізу великих масивів цифрової інформації, зокрема електронної пошти, файлів і вебартефактів.

EnCase застосовується для створення та дослідження криміналістичних копій цифрових носіїв, аналізу файлових систем і документування результатів експертної роботи [8, 45, 48].

Важливо, однак, не ототожнювати можливості програмного забезпечення з гарантованим відновленням будь-якої інформації. Результат залежить від типу пристрою, файлової системи, способу видалення даних, використання шифрування, стану носія та багатьох інших факторів. У деяких випадках вилучення або відновлення даних може бути технічно неможливим.

Людиноцентричний підхід до цифрових матеріалів

Робота з цифровими даними у справах про торгівлю людьми потребує особливої уваги до приватності та безпеки постраждалих осіб. Фотографії, листування, геолокаційні дані, медична або інша чутлива інформація можуть містити відомості, розголошення яких здатне спричинити додаткову шкоду або повторну травматизацію [4, 9, 10, 56].

Тому доцільно застосовувати принцип мінімізації даних: вилучати, копіювати та аналізувати лише ті відомості, які мають обґрунтоване значення для конкретного завдання. Доступ до матеріалів повинен бути розмежований, а в навчальних, аналітичних або публічних матеріалах прямі ідентифікатори необхідно замінювати умовними кодами або іншими засобами псевдонімізації.

Не менш важливо уникати формулювань, за яких цифровий слід автоматично перетворюється на висновок про роль конкретної людини. Наявність номера телефону у декількох оголошеннях, контакту в месенджері або адреси криптовалютного гаманця є інформаційним фактом, але не підтверджує самостійно статус особи як організатора, вербувальника чи іншого учасника злочинної діяльності.

Технічні та організаційні обмеження

Суттєвою проблемою залишається швидка зміна цифрового середовища. Шифрування, системи автоматичного видалення повідомлень, хмарне

зберігання, багатофакторна автентифікація, використання VPN або Tor можуть ускладнювати отримання та інтерпретацію даних. Водночас саме використання таких технологій не повинно розглядатися як ознака злочинної діяльності, оскільки вони широко застосовуються і для законного захисту приватності.

Додаткові труднощі виникають тоді, коли цифрові дані зберігаються за межами України або контролюються іноземними постачальниками послуг. У таких випадках отримання інформації може потребувати міжнародної правової та правоохоронної взаємодії, процедур збереження даних і звернення до відповідних компетентних органів. *Europol, Interpol, UNODC* та інші міжнародні структури можуть відігравати різні ролі у такій співпраці, однак їх не слід трактувати як універсальні сховища, через які автоматично отримуються потрібні цифрові дані.

Значення цифрової криміналістики для протидії торгівлі людьми

Цифрова криміналістика створює методологічну основу для контрольованої роботи з цифровими слідами – від моменту їх виявлення до аналізу та представлення результатів. Її практична цінність полягає у забезпеченні цілісності матеріалів, простежуваності операцій із ними, можливості відновлення частини цифрових артефактів та встановлення взаємозв’язків між різними джерелами інформації.

Водночас цифрові матеріали не повинні розглядатися поза контекстом. Хеш-значення не доводить правдивість змісту файла, аномальна транзакція не підтверджує злочинне походження коштів, а цифровий контакт між двома особами не визначає характер їхніх взаємовідносин. Значення конкретного цифрового об’єкта формується лише через його перевірку, зіставлення з іншими матеріалами та належну правову оцінку.

Таким чином, роль цифрової криміналістики у справах про торгівлю людьми полягає не в автоматичному «доведенні злочину» за цифровими слідами, а у забезпеченні надійного, відтворюваного та контрольованого процесу роботи з цифровими даними. Поєднання технічної коректності, належного документування, правомірності отримання інформації та захисту приватності постраждалих осіб є необхідною умовою того, щоб результати цифрового

дослідження могли бути обґрунтовано використані в подальшій слідчій, експертній та процесуальній діяльності.

3.2. Захист цифрових доказів у справах торгівлі людьми

Захист цифрових матеріалів у справах про торгівлю людьми має одночасно технічний, процесуальний та етичний вимір. Цифрові об’єкти можуть містити важливу інформацію про комунікацію, публікацію оголошень, використання електронних сервісів, фінансові операції або інші обставини, що досліджуються у кримінальному провадженні. Водночас такі матеріали є вразливими до зміни, копіювання, видалення чи втрати, тому важливо забезпечити їх цілісність, конфіденційність, контрольований доступ і можливість відтворити історію роботи з ними.

Не слід виходити з припущення, що скріншот, повідомлення у месенджері або інший цифровий об’єкт автоматично є доказом певної обставини. Його значення визначається походженням, способом отримання, контекстом, збереженням цілісності, можливістю перевірки та оцінкою у сукупності з іншими матеріалами провадження.

Захист даних під час зберігання і передавання

Одним із базових механізмів забезпечення конфіденційності цифрових матеріалів є криптографічний захист. Для шифрування даних під час зберігання можуть застосовуватися сучасні алгоритми, зокрема AES із ключами достатньої довжини, тоді як передавання інформації захищеними каналами може здійснюватися із використанням TLS 1.3, IPsec VPN та інших актуальних криптографічних протоколів [46].

Ефективність такого захисту визначається не лише обраним алгоритмом. Не менш важливими є належне керування ключами, розмежування доступу, своєчасне оновлення програмного забезпечення та захист облікових даних користувачів. Наприклад, під час передавання цифрових матеріалів між підрозділами доцільно використовувати захищений канал та контрольований контейнер або сховище, доступ до якого надається лише уповноваженим особам.

Шифрування забезпечує конфіденційність інформації, однак саме по собі не підтверджує її автентичність і не замінює документування походження та історії оброблення цифрового об’єкта.

Керування доступом і аудит

Захист цифрових матеріалів потребує чіткого визначення того, хто і в якому обсязі може з ними працювати. Одним із поширених підходів є рольова модель керування доступом – RBAC (*Role-Based Access Control*), за якої права користувача визначаються його службовими функціями та необхідністю доступу до конкретної інформації [47].

Це особливо важливо у справах про торгівлю людьми, де матеріали можуть містити персональні дані, приватне листування, фотографії, відомості про місцеперебування або іншу чутливу інформацію про постраждалих осіб.

Система доступу повинна доповнюватися журналюванням операцій. Доцільно фіксувати входи до системи, перегляд і копіювання матеріалів, їх переміщення, експорт та інші значущі дії. Журнал аудиту не виключає можливості зловживання, але створює механізм простежуваності та дозволяє встановити, хто, коли і які операції виконував.

Для додаткового захисту можуть застосовуватися багатофакторна автентифікація, апаратні токени та інші засоби посиленої ідентифікації користувачів [46]. Їх використання доцільно визначати з урахуванням рівня чутливості даних та вимог конкретної інформаційної системи.

Запобігання втраті та несанкціонованій зміні

Цифрові матеріали потребують захисту не лише від навмисного втручання, а й від випадкової втрати, технічної несправності або помилки користувача. Тому важливим елементом інфраструктури є резервне копіювання.

Поширений підхід 3-2-1 передбачає наявність кількох копій даних, їх зберігання на різних типах носіїв і винесення щонайменше однієї резервної копії в окреме захищене середовище. Конкретна схема резервування повинна відповідати вимогам організації щодо конфіденційності, доступності та відновлення інформації.

Для матеріалів, що потребують захисту від подальшого переписування або видалення, можуть застосовуватися WORM-сховища (*Write Once, Read Many*). Такі технології призначені для обмеження можливості зміни записаних даних протягом установленого періоду зберігання. Їх доцільно поєднувати з криптографічними хешами, журналами аудиту та резервним копіюванням.

Водночас жодна окрема технологія не «гарантує автентичність» цифрового матеріалу. Надійність забезпечується сукупністю процедур – належним отриманням, фіксацією, контролем цілісності, документуванням і захищеним зберіганням.

Захист постраждалих осіб і мінімізація даних

У справах про торгівлю людьми особливого значення набуває захист інформації про постраждалих осіб. Цифрові матеріали можуть містити відомості, розголошення яких здатне створити ризик повторної ідентифікації, стигматизації, психологічної шкоди або фізичної небезпеки.

Тому в аналітичних і робочих масивах доцільно використовувати псевдонімізацію. Замість прямих ідентифікаторів особи можуть застосовуватися нейтральні умовні позначення, наприклад `CASE-102`, тоді як інформація, що дозволяє встановити особу, повинна зберігатися окремо з обмеженим доступом.

Під час підготовки матеріалів для навчання, наукового аналізу, міжвідомчого обміну або іншого використання, яке не потребує розкриття особи, фотографії, імена, контактні дані та інші прямі ідентифікатори мають бути видалені, замасковані або замінені. У процесуальних документах спосіб використання таких відомостей визначається відповідними нормами законодавства та процедурою конкретного провадження.

Принцип мінімізації означає, що слід обробляти лише той обсяг персональних даних, який обґрунтовано необхідний для визначеної законної мети [9]. Особливо небажаним є накопичення чутливої інформації «про всяк випадок», якщо її зв’язок із предметом дослідження або провадження не встановлений.

Міжнародний аспект

Цифрові дані, що мають значення для розслідування, нерідко перебувають під контролем іноземних постачальників послуг або фізично зберігаються за межами України. У таких випадках отримання та збереження інформації потребує використання передбачених законом механізмів міжнародної співпраці.

Взаємна правова допомога у кримінальних справах може забезпечувати офіційне отримання електронних доказів від компетентних органів іншої держави. Механізми MLAT (*Mutual Legal Assistance Treaties*) передбачають взаємодію між державами, а не безпосереднє довільне отримання правоохоронним органом інформації від іноземного сервісу.

Europol та Interpol забезпечують спеціалізовані механізми й захищені канали міжнародного правоохоронного інформаційного обміну в межах своїх повноважень. Однак їх не слід розглядати як універсальні сховища цифрових доказів або автоматичний спосіб отримання даних від приватних платформ.

Важливим міжнародно-правовим інструментом залишається Конвенція про кіберзлочинність, яка визначає механізми міжнародного співробітництва щодо кіберзлочинності та електронних доказів [55]. Її положення та пов’язані з нею механізми співпраці мають значення і для розслідувань, у яких цифрові матеріали перебувають в іншій юрисдикції.

Практичне застосування

Практичний сценарій захисту цифрового матеріалу може включати первинне законне отримання файла або повідомлення, фіксацію джерела та часу отримання, створення контрольної копії, обчислення хеш-значення, розміщення матеріалу у захищеному сховищі та реєстрацію подальших операцій із ним. Для аналітичної роботи доцільно використовувати копію, залишаючи вихідний зафіксований матеріал незмінним.

Якщо матеріал містить дані постраждалої особи, до цього процесу додаються псевдонімізація, розмежування доступу та контроль можливості подальшого розкриття ідентифікаційної інформації.

Захист цифрових матеріалів у справах про торгівлю людьми слід розглядати як безперервний процес, у якому технічні заходи взаємопов'язані з процесуальними та етичними вимогами. Шифрування, контроль доступу, резервне копіювання, WORM-сховища, хешування та аудит забезпечують різні аспекти захисту, але жоден із цих механізмів окремо не визначає доказового значення інформації.

Не менш важливими є документоване походження матеріалу, простежуваність роботи з ним, законність отримання та захист персональних даних постраждалих осіб. Тому надійна модель захисту повинна будуватися за принципом *«зберегти цілісність – обмежити доступ – забезпечити простежуваність – мінімізувати розкриття персональних даних – зберегти можливість незалежної перевірки».*

Саме поєднання цих складових дозволяє створити технічно надійне й людиноцентричне середовище для роботи з цифровими матеріалами, не підміняючи при цьому процесуальну оцінку доказів суто технологічними механізмами.

3.3. Виявлення фальсифікацій та протидія маніпуляціям

Фальсифікація цифрових доказів у справах торгівлі людьми є серйозною загрозою для ефективності слідства. Злочинні угруповання застосовують широкий спектр методів: від підробки фото й відео до створення фейкових акаунтів та маніпуляцій із текстами. Тому важливим завданням цифрової криміналістики стає не лише збір даних, але й перевірка їх достовірності.

3.3.1. Фальсифікація візуальних матеріалів

Перцептивні хеші (pHash). Метод дозволяє визначати подібність зображень незалежно від незначних змін (обрізання, зміна яскравості). Наприклад, оголошення на різних сайтах можуть містити однакове фото жертви з різними іменами, *pHash* допомагає знайти візуально схожі зображення для подальшої перевірки» [50].

Аналіз метаданих (EXIF). Навіть при зміні контенту у файлі зберігається технічна інформація: модель камери, дата та місце зйомки. Це дозволяє виявити невідповідності: наприклад, фото, яке нібито зроблене у 2024 році, може містити EXIF із датою 2018 року [50].

Deepfake та синтетичний контент. Сучасні мережі дедалі частіше застосовують технології deepfake для створення відео чи зображень, що вводять в оману. Для ідентифікації таких матеріалів застосовуються алгоритми комп'ютерного зору, зокрема CNN та XceptionNet, які виявляють мікродеформації у русі обличчя, специфічні артефакти в очах і неприродні відблиски. [53].

3.3.2. Маніпуляції текстовими даними

Фальшиві оголошення. Злочинці часто замінюють літери на символи або використовують емодзі, щоб обійти автоматичні системи виявлення ризикових ключових слів. Алгоритми NLP (обробки природної мови) дозволяють «очистити» текст і відновити його зміст [30, 32, 34].

Фейкові акаунти. Автоматизовані профілі у соціальних мережах мають неприродну активність: публікація сотень однакових постів, одноманітні фотографії, повторювані контакти. Виявлення здійснюється через аналіз часових патернів і мережевих зв'язків.

3.3.3. Протидія фальсифікаціям

Порівняння версій документів. Використання систем контролю версій (Git) або блокчейн-журналів дозволяє зафіксувати всі зміни файлів та їхню історію.

Автоматизований моніторинг соціальних мереж. Системи раннього попередження здатні виявляти масове поширення підозрілих повідомлень, дублювання контенту чи активність ботів.

Міжнародна співпраця. Для підтвердження достовірності цифрових матеріалів необхідний доступ до серверів провайдерів (Meta, Telegram, Binance). Це здійснюється в рамках MLAT або каналів Europol/Interpol.

3.3.4. Практичні приклади

Україна (2021). У ході OSINT-розслідування виявлено оголошення на різних сайтах із однаковими фотографіями жінок. Завдяки алгоритму *pHash* було доведено, що фото належать до однієї серії, хоча злочинці змінювали фони та накладали фільтри.

ЄС (2022). Європол задокументував випадки використання deepfake-відео для маскування вербувальників під «жертв». Системи аналізу виявили неприродну міміку та артефакти, що довело синтетичність контенту.

США (2020). Під час розслідування справи про трудову експлуатацію виявлено групу акаунтів у Facebook, які мали синхронні публікації кожні 30 хвилин. Це було ідентифіковано як бот-мережа, що поширювала оголошення з фальшивими вакансіями.

Таким чином, фальсифікація цифрових доказів у справах торгівлі людьми використовується злочинцями як спосіб маскування та введення в оману слідчих органів. Використання алгоритмів для виявлення підробок (pHash, EXIF-аналіз, детекція deepfake), перевірка текстових даних та автоматизований моніторинг соціальних мереж дозволяють протидіяти таким діям. Це забезпечує достовірність доказів і підвищує шанси на успішне розслідування та судове переслідування організаторів торгівлі людьми.

3.4. Правові й етичні вимоги при документуванні торгівлі людьми

Фіксація злочинів, що пов’язані з торгівлею людьми, передбачає роботу з великою кількістю персональних та чутливих даних. Йдеться про фотографії та відео постраждалих, їхні контакти, листування, а також відомості про міграційні маршрути. Така інформація одночасно є доказовою базою і вразливим ресурсом, що потребує спеціального правового та етичного захисту.

3.4.1. Міжнародні правові стандарти

Протокол ООН про попередження і припинення торгівлі людьми (Palermo Protocol, 2000). Встановлює зобов’язання держав забезпечувати безпечне

документування злочинів із дотриманням прав жертв, включаючи конфіденційність та безпеку персональних даних [1].

Як зазначено в Конвенції Ради Європи про заходи протидії торгівлі людьми (2005 р.), усі процедури, пов'язані з документуванням, мають проводитися з дотриманням принципу поваги до людської гідності. Інформація про постраждалих не може застосовуватися таким чином, щоб створювати ризики дискримінації чи стигматизації [4].

GDPR (2016). Регламент ЄС накладає жорсткі обмеження на обробку персональних даних. У випадках торгівлі людьми це означає, що обсяг даних, які збирають правоохоронці чи аналітики, повинен бути мінімально необхідним («принцип мінімізації»), а доступ до них – суворо обмежений [Error: Reference source not found].

Interpol Digital Evidence Guidelines (2020). Міжнародний стандарт, який підкреслює: дані жертв повинні оброблятися лише у межах законності, а будь-яка передача цифрових доказів між державами має супроводжуватись механізмами шифрування та протоколювання [56].

3.4.2. Національні вимоги України

Закон України «Про протидію торгівлі людьми» (2011). Визначає механізми ідентифікації жертв та гарантує їм захист у процесі розслідувань, зокрема при зборі та документуванні доказів [6].

Закон «Про захист персональних даних» (2010). Встановлює принципи пропорційності та добровільності при обробці даних. Важливо, що навіть у кримінальних провадженнях не допускається збір даних, які прямо не стосуються предмета доказування [10].

Кримінальний процесуальний кодекс України (2012). Закріплює поняття допустимість доказів – ст. 86–89; документи – ст. 99 КПК України» [57].

Закон "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII визначає правові основи кібербезпеки, зокрема щодо критичної інфраструктури» [58].

3.4.3. Етичні принципи документування

Принцип «не зашкодь». Документування матеріалів у справах про торгівлю людьми має здійснюватися з урахуванням безпеки, гідності та психологічного стану постраждалих осіб. Необхідно уникати дій, здатних спричинити повторну травматизацію, стигматизацію або додаткові ризики, зокрема необґрунтованого поширення фотографій, відеозаписів, приватного листування чи інших чутливих відомостей. Обсяг збирання та подальшого використання таких даних повинен відповідати конкретній законній меті й бути пропорційним поставленому завданню.

Захист ідентифікаційних даних. У наукових публікаціях, навчальних матеріалах, аналітичних і статистичних звітах відомості, які дозволяють безпосередньо або опосередковано ідентифікувати постраждалу особу, повинні бути вилучені, узагальнені або належним чином захищені. Для цього можуть застосовуватися псевдонімізація, заміна імен нейтральними кодами, маскування контактних даних, розмиття облич та інших ідентифікаційних ознак. У матеріалах кримінального провадження порядок обмеження доступу до таких відомостей визначається процесуальними нормами та необхідністю забезпечення прав учасників провадження.

Інформованість і повага до автономії постраждалої особи. Особа має бути, наскільки це допускається обставинами провадження, поінформована про мету отримання її даних, можливі способи їх використання та передавання. У випадках, коли законодавство або характер відповідної діяльності передбачає отримання згоди, вона повинна бути добровільною, конкретною та усвідомленою. Водночас згода не є універсальною правовою підставою для всіх дій у межах кримінального провадження, тому оброблення персональних даних має здійснюватися відповідно до встановлених законом повноважень і з необхідними гарантіями конфіденційності.

Пояснюваність алгоритмічного аналізу. Якщо для аналізу оголошень, повідомлень, зображень або інших цифрових матеріалів застосовуються системи штучного інтелекту, результати їх роботи мають бути достатньо зрозумілими для

фахівця, який приймає рішення. Це відповідає підходу *explainable AI* і передбачає можливість встановити, які дані та ознаки вплинули на результат, оцінити обмеження моделі та перевірити її висновок [54]. Алгоритмічна оцінка не повинна автоматично визначати статус особи або підтверджувати факт протиправної діяльності; вона має використовуватися як допоміжний аналітичний інструмент із подальшою перевіркою людиною.

Дотримання цих принципів дозволяє поєднати потреби документування з повагою до прав, приватності та гідності постраждалих осіб. Етичність у цьому контексті є не додатковою вимогою, а складовою якості та надійності всього процесу роботи з цифровими матеріалами.

3.4.4. Виклики й ризики

Одним із ключових викликів є необхідність одночасно забезпечити повноту документування та захист приватності постраждалих осіб. Для встановлення обставин події може виникати потреба в аналізі значного обсягу цифрових даних – листування, контактів, геолокаційної інформації, фотографій, відеозаписів або відомостей про фінансові операції. Водночас збирання надмірного обсягу інформації, яка не має безпосереднього значення для конкретного завдання, збільшує ризик порушення приватності та несанкціонованого розкриття чутливих відомостей. Тому обсяг даних має визначатися принципами необхідності, пропорційності та мінімізації.

Суттєві складнощі створює транскордонний характер цифрового середовища. Дані користувачів можуть зберігатися або оброблятися постачальниками послуг, інфраструктура яких розташована в інших юрисдикціях. Це стосується соціальних мереж, месенджерів, хмарних сервісів, електронних платіжних систем і криптовалютних платформ. У таких ситуаціях доступ до інформації залежить не лише від технічної можливості її отримання, а й від правових процедур, правил конкретного сервісу та механізмів міжнародної співпраці. Додатковою проблемою може бути обмежений строк зберігання окремих даних, що підвищує значення своєчасної їх фіксації та належного оформлення відповідних запитів.

Окремий ризик пов’язаний із розголошенням інформації про постраждалих осіб. Публікація деталей кримінального провадження, фотографій, фрагментів листування або інших відомостей, за якими особу можна прямо чи опосередковано ідентифікувати, здатна спричинити стигматизацію, психологічну шкоду або створити загрозу її безпеці. Тому під час взаємодії правоохоронних органів із медіа та іншими зовнішніми суб’єктами необхідно дотримуватися принципів конфіденційності, мінімізації розкриття персональних даних і пріоритету безпеки постраждалої особи.

Поширення алгоритмів штучного інтелекту та автоматизованої аналітики створює додатковий комплекс ризиків. Модель може відтворювати упередження, наявні у вихідних даних, неправильно класифікувати інформаційні об’єкти або надавати завищене значення окремим ознакам. Унаслідок цього акаунт, оголошення, маршрут чи транзакція можуть помилково отримати підвищений рівень аналітичної уваги. Особливо небезпечним є автоматичне перенесення такого результату на оцінку конкретної людини. Алгоритмічний висновок має використовуватися як допоміжний сигнал для перевірки, а не як самостійна підстава для визначення причетності особи до протиправної діяльності.

Таким чином, основні ризики цифрового документування пов’язані не лише з технічним захистом інформації, а й із визначенням меж її збирання, правомірністю транскордонного доступу, збереженням конфіденційності та контролем автоматизованих рішень. Зменшення цих ризиків потребує поєднання принципів мінімізації даних, розмежування доступу, простежуваності операцій, експертної перевірки алгоритмічних результатів і пріоритетного захисту прав та безпеки постраждалих осіб.

3.4.5. Практичне значення правових та етичних вимог

У міжнародній практиці документування цифрових матеріалів дедалі більше уваги приділяється не лише їх технічному збереженню, а й законності отримання, пропорційності оброблення персональних даних та можливості подальшої перевірки походження інформації. Недотримання цих вимог може

поставити під сумнів належність і допустимість окремих матеріалів, а також створити додаткові ризики для постраждалих осіб.

Особливого значення набуває захист персональних даних. У робочих, аналітичних і міжвідомчих інформаційних системах доцільно застосовувати псевдонімізацію, розмежування доступу та використання нейтральних кодових ідентифікаторів замість прямих персональних даних. Це дозволяє зменшити ризик несанкціонованого розкриття інформації, не перешкоджаючи водночас законному використанню матеріалів у межах розслідування.

Під час міжнародного обміну інформацією важливим є принцип необхідності та пропорційності: передаватися має лише той обсяг персональних даних, який безпосередньо потрібний для конкретної законної мети. Такий підхід застосовується у міжнародній правоохоронній взаємодії та спрямований на поєднання ефективності розслідування із захистом прав людини [54].

Правові й етичні вимоги до документування торгівлі людьми формують єдину систему гарантій, у межах якої процесуальна належність матеріалів має поєднуватися із захистом постраждалих осіб та можливістю законного міжнародного обміну інформацією. Процесуальний аспект передбачає дотримання вимог кримінального процесуального законодавства щодо отримання, фіксації, зберігання та оцінки цифрових матеріалів. Захист постраждалих осіб охоплює конфіденційність, мінімізацію персональних даних, псевдонімізацію та запобігання повторній ідентифікації [56]. Міжнародна взаємодія, своєю чергою, потребує узгодження процедур обміну даними з відповідними правовими механізмами та стандартами захисту інформації.

Таким чином, ефективність документування у справах про торгівлю людьми визначається не максимальним обсягом зібраної інформації, а законністю її отримання, належністю фіксації, можливістю перевірки, пропорційністю використання та достатнім рівнем захисту постраждалих осіб**.** Саме такий підхід дозволяє поєднати інтереси розслідування з повагою до приватності, гідності та інших фундаментальних прав людини.

Висновок до розділу 3

Надійність цифрового документування у справах про торгівлю людьми визначається не окремим технічним засобом, а цілісністю всього процесу роботи з цифровими матеріалами – від моменту їх отримання до подальшого аналізу, зберігання та використання. Цифрові дані є потенційно нестійкими, легко копіюються, можуть бути змінені або втрачатися, тому їх практична цінність залежить від того, наскільки контрольованим і відтворюваним є весь життєвий цикл такого матеріалу.

Криптографічне хешування, часові мітки, журналювання операцій, контроль доступу, резервне копіювання та WORM-сховища виконують різні функції, але мають спільну мету – забезпечити цілісність, простежуваність і захищеність цифрових даних. При цьому жодна з цих технологій сама по собі не визначає доказового значення конкретного матеріалу. Хеш підтверджує незмінність конкретної копії після моменту його обчислення, часові мітки фіксують відповідний момент роботи з даними, а *chain of custody* дозволяє відтворити послідовність дій із цифровим об'єктом. Їх значення проявляється саме у поєднанні з належним документуванням походження матеріалу та умов його отримання.

Окремою проблемою є достовірність самого цифрового контенту. Повторне використання зображень, редагування метаданих, синтетичні відео або фальшиві облікові записи можуть ускладнювати інтерпретацію цифрових слідів. Тому *pHash*, аналіз *EXIF*, засоби виявлення ознак deepfake та інші інструменти доцільно використовувати не як механізми автоматичного встановлення фальсифікації, а як засоби виявлення невідповідностей, які потребують подальшої перевірки. Результат технічного аналізу має оцінюватися разом із контекстом, джерелом походження та іншими матеріалами провадження.

Кібербезпековий аспект цифрового документування також не обмежується захистом файлів від несанкціонованого доступу. Він охоплює керування правами користувачів, захист каналів передавання, журналювання дій, збереження резервних копій, контроль цілісності та мінімізацію ризику витоку персональних

даних. Особливого значення це набуває у справах про торгівлю людьми, де цифрові матеріали можуть містити приватне листування, фотографії, геолокаційні дані та іншу чутливу інформацію про постраждалих осіб.

Правові та етичні вимоги є невід'ємною частиною цієї системи. Технічно коректно збережений матеріал не може розглядатися поза законністю його отримання, пропорційністю використання та дотриманням вимог щодо захисту персональних даних. Саме тому принцип «не зашкодь», мінімізація даних, конфіденційність, псевдонімізація та контроль розкриття інформації мають розглядатися як складові якості цифрового документування, а не як додаткові обмеження.

Отже, ефективне використання цифрових матеріалів у справах про торгівлю людьми ґрунтується на поєднанні чотирьох взаємопов'язаних умов: *технічної цілісності, процесуальної простежуваності, інформаційної безпеки та захисту прав постраждалої особи.* Саме така модель дозволяє зменшити ризик втрати, спотворення або неправильної інтерпретації цифрових даних і створює підґрунтя для їх обґрунтованого використання у слідчій, експертній та процесуальній діяльності.

РОЗДІЛ 4 ПРАКТИЧНІ КЕЙСИ ТА ПІЛОТНІ РЕАЛІЗАЦІЇ

4.1. Загальна характеристика підходу

Практичне впровадження сучасних інформаційно-аналітичних технологій у сфері протидії торгівлі людьми передбачає не лише теоретичне опрацювання моделей та алгоритмів, але й їхню апробацію на практичних прикладах. Такий підхід має подвійне значення: **науково-дослідне** (перевірка життєздатності запропонованих методів, формування базових принципів для подальшого розвитку систем) **та прикладне** (забезпечення правоохоронних органів інструментами, які дозволяють ефективніше здійснювати виявлення, документування та попередження злочинів у сфері торгівлі людьми).

4.1.1. Логіка впровадження пілотних кейсів

Пілотні кейси доцільно розглядати як проміжний етап між концептуальним обґрунтуванням інформаційно-аналітичних методів і їх можливим практичним застосуванням. Їх основне призначення полягає не у доведенні ефективності запропонованих технологій у реальних розслідуваннях, а у перевірці того, наскільки коректно працюють окремі аналітичні підходи в контрольованих умовах та які обмеження виникають під час їх поєднання.

Використання тестових, модельних або синтетичних наборів даних дає можливість оцінити роботу методів OSINT, Big Data, машинного навчання та GIS без використання чутливої інформації про реальних постраждалих осіб. Такий підхід дозволяє перевірити логіку оброблення даних, послідовність аналітичних операцій, взаємодію між окремими компонентами системи та здатність алгоритмів виявляти задані закономірності, зв’язки або аномалії. Водночас результати такої апробації не повинні автоматично переноситися на реальне середовище, оскільки модельні дані не відтворюють у повному обсязі складність, неповноту та неоднорідність інформації, характерної для практичної діяльності.

Пілотування також дає змогу виявити обмеження, які не завжди помітні на етапі теоретичного проєктування. До них належать проблеми продуктивності,

масштабованості, якості та сумісності даних, розмежування прав доступу, розподілу відповідальності між учасниками процесу, а також дотримання вимог щодо захисту персональних даних. У цьому сенсі пілотний кейс виконує не лише демонстраційну, а й діагностичну функцію, оскільки дозволяє визначити, які елементи системи потребують доопрацювання до початку її ширшого застосування.

Практичне значення такого підходу полягає у тому, що рішення щодо подальшого масштабування можуть ґрунтуватися не лише на очікуваних перевагах технології, а й на результатах попередньої перевірки її обмежень. Перехід від локального пілота до регіонального, національного або міжнародного рівня потребує окремого оцінювання продуктивності, безпеки, правомірності оброблення даних, організаційної готовності та можливості незалежної перевірки результатів.

Таким чином, пілотні кейси створюють контрольоване середовище для оцінювання працездатності запропонованих методів, виявлення технічних і організаційно-правових ризиків та уточнення вимог до подальшого впровадження. Їх результати слід розглядати як підставу для вдосконалення аналітичної моделі та планування наступних етапів апробації, а не як остаточне підтвердження ефективності системи в реальних умовах.

4.1.2. Компоненти підходу

Інтегрований підхід до аналізу інформації у сфері протидії торгівлі людьми передбачає поєднання кількох технологічних компонентів, кожен із яких виконує окрему функцію в загальному аналітичному процесі. Його перевага полягає не в одночасному використанні максимальної кількості інструментів, а у послідовному переході від збору відкритих даних до їх структурування, аналізу, просторової інтерпретації та захищеного зберігання результатів.

OSINT формує первинний інформаційний рівень такої системи. Відкриті вебресурси, соціальні мережі, сайти оголошень, публічні реєстри та інші загальнодоступні джерела можуть містити відомості, придатні для виявлення повторюваних контактів, пов’язаних публікацій, схожих текстів, зображень та

інших цифрових слідів. Аналіз darknet-ресурсів можливий лише за наявності відповідних технічних, правових і безпекових умов. При цьому інформація, отримана з відкритих джерел, розглядається насамперед як основа для формування аналітичних гіпотез і подальшої перевірки, а не як автоматичне підтвердження протиправної діяльності.

Big Data-аналітика забезпечує інтеграцію різнорідних інформаційних масивів, які можуть істотно відрізнятися за структурою, обсягом, якістю та частотою оновлення. Архітектура *Data Lakehouse* у межах запропонованого підходу може використовуватися як середовище для консолідації структурованих і неструктурованих даних, їх очищення, нормалізації, збереження та підготовки до подальшого аналізу. Практична цінність такого рішення полягає у можливості працювати з даними різних типів у межах єдиного аналітичного контуру, зберігаючи інформацію про їх походження та етапи оброблення.

Методи машинного навчання та штучного інтелекту застосовуються для автоматизації окремих операцій, які складно або ресурсомістко виконувати вручну. До них належать класифікація текстових матеріалів, пошук семантично подібних оголошень, групування інформаційних об’єктів за спільними ознаками та виявлення аномальних спостережень. Результат роботи алгоритму при цьому має розглядатися як аналітичний сигнал, що потребує змістовної перевірки. Кластеризація не підтверджує існування організованої групи, аномалія не означає протиправність, а автоматична класифікація не може самостійно визначати статус конкретної особи.

Геоінформаційні технології доповнюють аналіз просторовим і просторово-часовим виміром. GIS дає змогу зіставляти місця публікації або інші географічно прив’язані спостереження, досліджувати їх концентрацію, взаємне розташування та зміни у часі. Методи кластеризації, аналізу щільності та транспортної доступності можуть використовуватися для виявлення зон підвищеної концентрації модельних або реальних спостережень і перевірки гіпотез щодо просторових зв’язків. Водночас отримані «гарячі точки» або умовні

маршрутні зв’язки не повинні автоматично інтерпретуватися як встановлені місця злочинної активності чи фактичні маршрути переміщення постраждалих осіб.

Кібербезпековий компонент забезпечує захист даних і результатів аналітичної роботи на всіх етапах їх життєвого циклу. Хешування, фіксація часу, контроль доступу, журналювання операцій, резервне копіювання та використання *WORM*-сховищ можуть застосовуватися для контролю цілісності й простежуваності цифрових матеріалів. Засоби аналізу метаданих, виявлення повторного використання зображень та ознак синтетичного контенту допомагають оцінювати достовірність окремих цифрових об’єктів, але не повинні використовуватися як самодостатня підстава для висновку про фальсифікацію без додаткової перевірки.

Таким чином, інтегрований підхід формує послідовний аналітичний цикл: *відкрите джерело → структуровані дані → алгоритмічний аналіз → просторово-часова інтерпретація → експертна перевірка → захищене зберігання результатів.* Така модель дозволяє поєднати масштабованість автоматизованої обробки з необхідністю перевірюваності, правомірності та людиноцентричного контролю на етапі інтерпретації результатів.

4.1.3. Методологічні принципи

Методологія розроблення та апробації пілотних кейсів має ґрунтуватися на поєднанні технічної обґрунтованості, правомірності, організаційної реалізованості та захисту прав людини. Для сфери протидії торгівлі людьми це особливо важливо, оскільки ефективність аналітичних технологій не може оцінюватися окремо від якості даних, законності їх використання та можливих наслідків для постраждалих осіб.

Комплексність передбачає спільний розгляд технологічних, правових, організаційних та гуманітарних аспектів. Алгоритм, який демонструє прийнятну точність на тестових даних, не може вважатися готовим до практичного використання, якщо не визначено правові підстави оброблення інформації, модель доступу до даних, порядок відповідальності користувачів і механізми

захисту чутливих відомостей. Тому оцінювання пілотного рішення має охоплювати не лише його функціональність, а й умови безпечного та правомірного застосування.

Мультидисциплінарність необхідна через складність предметної області. Інтерпретація цифрових слідів потребує участі ІТ-фахівців і аналітиків, правова оцінка – юристів і представників правоохоронної практики, а робота з інформацією про постраждалих осіб – врахування соціальних, психологічних та етичних аспектів. Такий підхід зменшує ризик ситуації, коли технічно коректний результат отримує помилкову змістовну або правову інтерпретацію.

Масштабованість означає можливість розвитку рішення від обмеженого пілотного середовища до більш широкого рівня застосування без втрати керованості та якості. При цьому масштабування не повинно розумітися як просте збільшення обсягів даних. Перехід до регіонального чи національного рівня потребує повторної оцінки продуктивності, інформаційної безпеки, якості даних, прав доступу, навантаження на інфраструктуру та спроможності аналітиків перевіряти результати автоматизованої обробки.

Інтероперабельність передбачає здатність системи обмінюватися даними та результатами аналізу з іншими інформаційними середовищами у стандартизованому й контрольованому форматі. Для міжнародної взаємодії важливими є узгоджені структури даних, метадані, правила ідентифікації об’єктів, механізми контролю доступу та захищені канали обміну. Взаємодія з *Europol, Interpol, UNODC* та іншими міжнародними структурами має здійснюватися в межах їхніх повноважень, процедур доступу та чинних механізмів співробітництва, а не передбачати автоматичну технічну сумісність або безпосередній доступ до їхніх систем.

Прозорість і етичність вимагають, щоб походження даних, основні етапи їх оброблення та логіка формування аналітичного результату могли бути перевірені. Робота з персональними даними має здійснюватися з урахуванням вимог законодавства про їх захист, принципів мінімізації, пропорційності та обмеження мети. Особливого захисту потребують відомості про постраждалих

осіб: їх ідентифікація повинна бути обмежена випадками, коли це обґрунтовано необхідністю, а результати автоматизованого аналізу не можуть використовуватися для безумовного визначення статусу чи ролі конкретної людини.

Таким чином, методологічні принципи пілотування мають забезпечувати не лише технічну працездатність запропонованого рішення, а й його контрольованість, перевірюваність та безпечність. Практична цінність пілотного кейсу визначається тим, наскільки він дозволяє оцінити систему в реалістичних умовах, виявити її обмеження та встановити вимоги, необхідні для подальшого застосування без необґрунтованого ризику для прав і безпеки людини.

4.1.4. Очікувані результати

Реалізація практичних кейсів має продемонструвати, наскільки запропонований інтегрований підхід придатний для підтримки інформаційно-аналітичної діяльності у сфері протидії торгівлі людьми. Очікуваний ефект пов’язується передусім із більш швидким опрацюванням великих масивів інформації та автоматизованим виділенням об’єктів, зв’язків і нетипових спостережень, які потребують уваги аналітика. Це може скоротити час первинного аналізу, однак автоматично сформований сигнал не повинен підміняти його подальшу перевірку.

Важливим результатом є підвищення якості документування цифрових матеріалів**.** Фіксація походження даних, контроль їх цілісності, збереження метаданих, журналювання операцій та дотримання ланцюга збереження створюють умови для перевірюваності отриманих матеріалів і їх подальшого використання відповідно до вимог кримінального процесу. При цьому застосування технічних засобів саме по собі не визначає доказового статусу інформації, який встановлюється у передбаченому законодавством порядку.

Інтеграція даних і стандартизація аналітичних процедур можуть сприяти покращенню міжвідомчої та міжнародної взаємодії**.** Єдині правила опису інформаційних об’єктів, фіксації їх походження та обміну результатами аналізу зменшують ризик втрати контексту під час передавання інформації між

уповноваженими суб’єктами. Така взаємодія має здійснюватися відповідно до компетенції кожної установи, установлених процедур доступу та вимог щодо захисту персональних даних.

Окремим результатом пілотування може стати формування верифікованих і належним чином підготовлених наборів даних для подальших досліджень та вдосконалення алгоритмів машинного навчання. Для цього необхідні контроль якості, документування походження даних, коректне маркування, усунення дублювань і застосування псевдонімізації або анонімізації там, де це необхідно. Особливо важливо запобігати перенесенню помилкових або упереджених оцінок у навчальні вибірки, оскільки це може відтворювати такі помилки в роботі подальших моделей.

Таким чином, очікуваним результатом практичних кейсів є не автоматичне «виявлення злочинів», а підвищення керованості інформаційно-аналітичного процесу**:** скорочення обсягу даних, що потребують ручного первинного перегляду, покращення простежуваності цифрових матеріалів, підтримка обміну інформацією та створення основи для подальшої перевірки й удосконалення аналітичних моделей. Ступінь фактичної ефективності цих рішень має визначатися під час подальшої апробації на верифікованих даних із використанням кількісних показників якості та експертної оцінки.

4.1.5. Візуалізаційна складова

Для представлення результатів аналітичної обробки доцільно використовувати засоби візуалізації, які дозволяють швидко переходити від великих масивів даних до їх змістовної інтерпретації. Інтерактивні дашборди можуть об’єднувати ключові показники, фільтри, часові ряди, просторові дані та результати алгоритмічного аналізу в єдиному робочому середовищі для аналітика. Їх основне призначення полягає не у прийнятті автоматичних рішень, а у забезпеченні зручного доступу до структурованої інформації та підтримці подальшої перевірки виявлених сигналів.

Heatmaps і карти просторової концентрації можуть застосовуватися для відображення територіального розподілу спостережень і виявлення зон, у яких

певні інформаційні події трапляються частіше. Такі візуалізації допомагають порівнювати території та простежувати зміни у просторі й часі, однак виявлена концентрація даних не повинна автоматично трактуватися як підтвердження злочинної активності.

Графові моделі дозволяють представляти взаємозв'язки між акаунтами, контактними даними, оголошеннями, зображеннями, транзакційними ідентифікаторами та іншими інформаційними об'єктами. Вони дають змогу виділяти структурно значущі вузли, групи щільно пов'язаних елементів і повторювані зв'язки. Водночас структура графа відображає властивості досліджуваних даних і потребує додаткової перевірки перед формулюванням висновків щодо характеру взаємодії між конкретними особами.

Часові діаграми доцільно використовувати для аналізу динаміки появи оголошень, повторюваності контактів або інших подій. Вони дозволяють виявляти періоди підвищеної активності, сезонність і нетипові зміни інтенсивності інформаційних процесів. Кластеризаційні схеми, своєю чергою, можуть допомагати групувати оголошення, акаунти або повідомлення за подібними ознаками, спрощуючи подальше порівняння та експертний аналіз.

Загальна логіка запропонованого підходу передбачає поступове розгортання експериментальних і пілотних рішень із послідовною перевіркою їх технічної, організаційної, правової та етичної придатності. Апробація в контрольованих умовах, наближених до практичного середовища, дозволяє оцінити якість даних, стабільність алгоритмів, зручність інтерфейсів, рівень інформаційної безпеки та можливість інтеграції різних компонентів системи. Отримані результати створюють підстави для подальшого вдосконалення й масштабування рішень, але не є автоматичною гарантією їх ефективності у реальній правоохоронній діяльності.

Таким чином, практична цінність підходу визначається поєднанням *аналітичної наочності, перевірюваності результатів, правомірності використання даних і можливості поступового масштабування***.** Саме така модель дозволяє переходити від окремих експериментальних інструментів до

більш цілісної інформаційно-аналітичної системи без необґрунтованого завищення можливостей автоматизованих технологій.

4.2. OSINT-кейс: виявлення мережі оголошень про «роботу за кордоном»

4.2.1. Постановка завдання

Метою кейсу є демонстрація того, як OSINT-методи можуть використовуватися для первинного аналізу оголошень про роботу за кордоном та виявлення між ними можливих інформаційних зв’язків. Основна увага приділяється тексту оголошень, контактним даним, фотографіям і взаємозв’язкам між окремими інформаційними об’єктами.

Для аналізу використано набір із 500 оголошень, що містили текст, контактні дані та зображення. Такий набір дозволяє послідовно продемонструвати відбір повідомлень за текстовими ознаками, пошук повторюваних контактів, порівняння фотографій та побудову графа зв’язків. Виявлені збіги розглядаються як аналітичні сигнали для подальшої перевірки, а не як підтвердження факту вербування або іншої протиправної діяльності.

4.2.2. Аналіз текстів оголошень

На першому етапі здійснюється автоматизоване опрацювання текстів. Для цього застосовано представлення тексту за допомогою TF-IDF та логістичну регресію, що дозволяє розподілити оголошення за заданими ознаками. Додатково використовується нечітке зіставлення (*fuzzy matching*) для пошуку слів, у яких навмисно або випадково змінено окремі символи.

У вихідному наборі 428 оголошень було віднесено алгоритмом до нейтральної групи, а 72 – до групи підвищеної аналітичної уваги. Такий результат не означає, що 72 оголошення пов’язані з торгівлею людьми. Автоматична класифікація лише скорочує обсяг інформації, яку необхідно перевірити аналітику вручну.

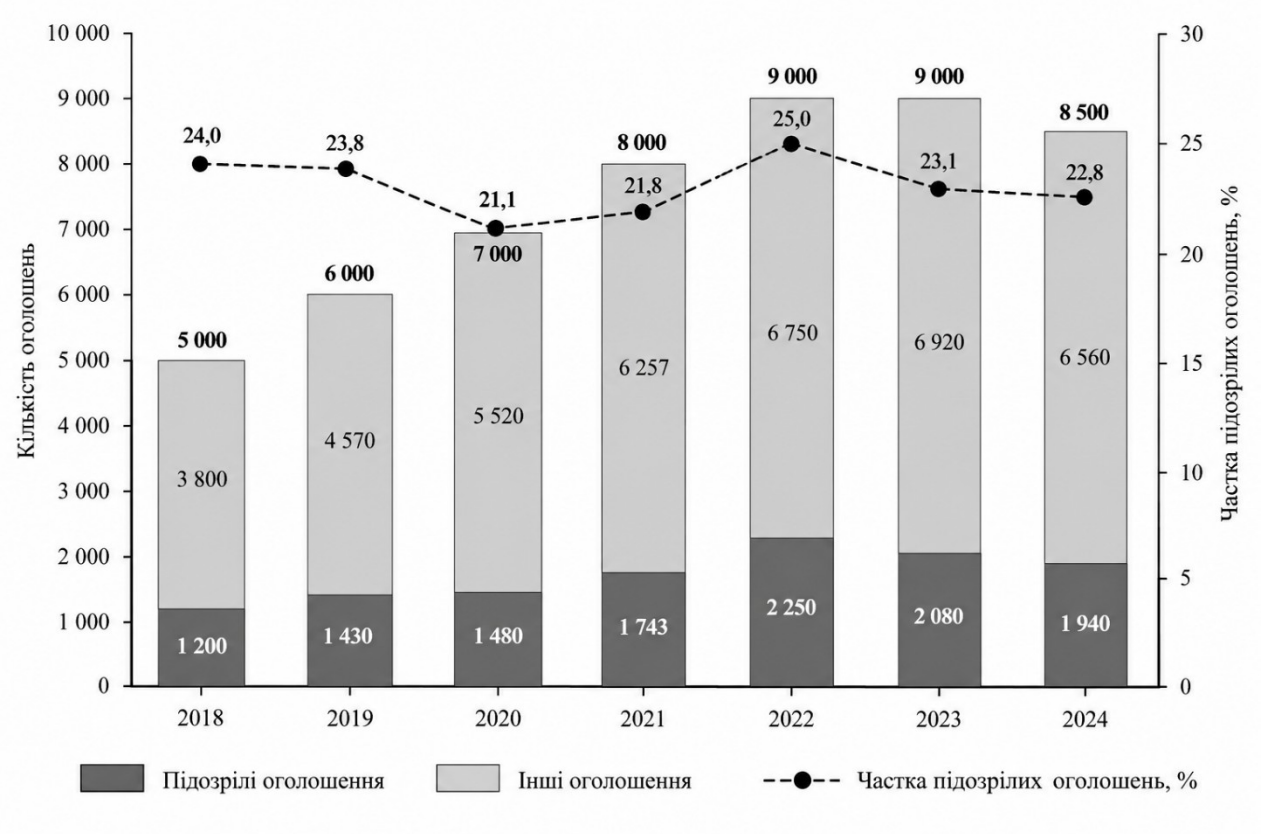


Рис. 4.1. Розподіл оголошень за результатами автоматизованої класифікації

4.2.3. Виявлення повторів контактних даних

Наступним етапом є зіставлення номерів телефонів та адрес електронної пошти, зазначених у різних оголошеннях. Повторне використання одного контакту дозволяє встановити можливий інформаційний зв’язок між публікаціями.

У досліджуваному наборі окремий номер телефону зустрічався у 24 публікаціях. Виявлено також адреси електронної пошти, які використовувалися в декількох оголошеннях. Такі повтори можуть бути пов’язані з централізованим розміщенням оголошень, діяльністю одного роботодавця, посередника або іншого суб’єкта. Тому сам факт повторення контакту не визначає характер діяльності, але створює підставу для зіставлення пов’язаних публікацій.

Домен електронної пошти також не повинен використовуватися як самостійний показник ризику. Його значення може оцінюватися лише разом з іншими характеристиками оголошення.

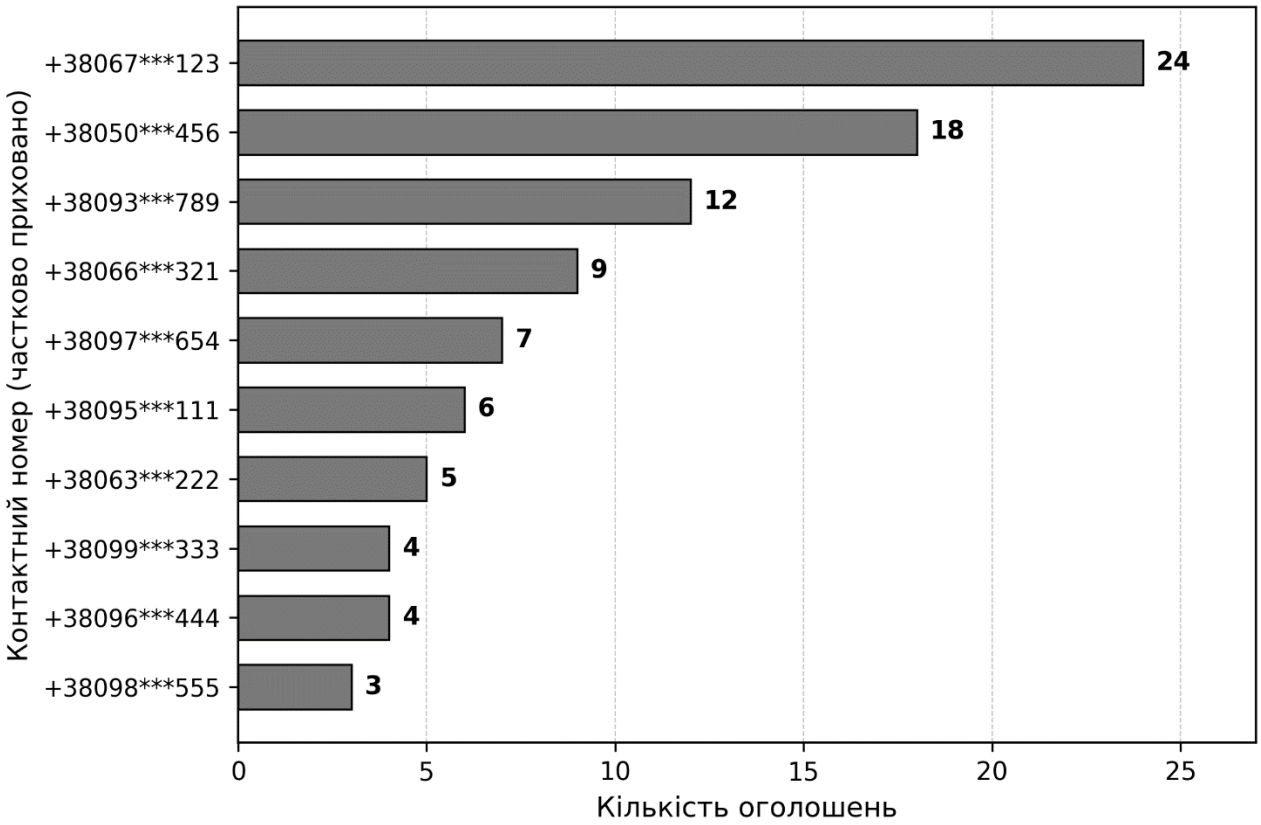


Рис. 4.2. Частота повторного використання контактних номерів у досліджуваному наборі оголошень.

4.2.4. Аналіз візуальних матеріалів

Для пошуку повторного використання фотографій застосовуються перцептивне хешування (*pHash*) та зворотний пошук зображень. На відміну від звичайного криптографічного хешування, pHash дозволяє знаходити візуально подібні зображення навіть після їх масштабування, обрізання або незначного редагування.

У наборі виявлено випадки використання однакових фотографій у різних оголошеннях із різними іменами. Додаткову інформацію може надати аналіз EXIF-метаданих, якщо вони збереглися у файлі. Невідповідність між заявленою інформацією та метаданими є підставою для додаткової перевірки, але не підтверджує автоматично факт фальсифікації.

Повторне використання фотографії також не означає, що всі відповідні оголошення створені однією особою або належать до єдиної мережі. Воно лише встановлює ще один інформаційний зв’язок, який має зіставлятися з контактними, текстовими та іншими даними.

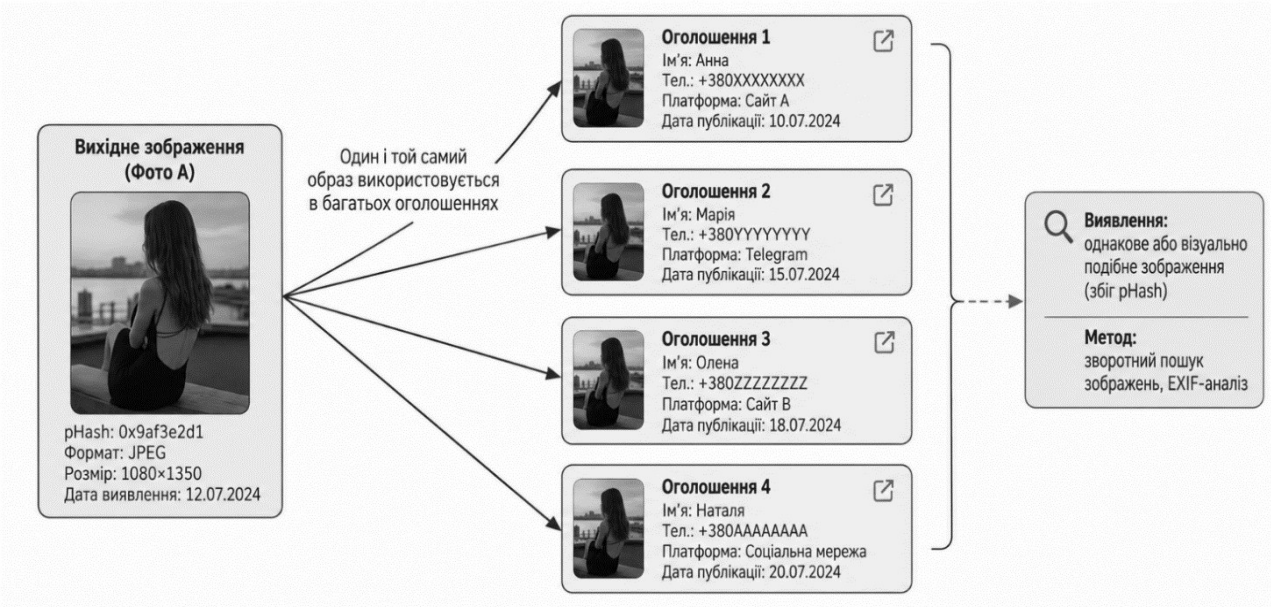


Рисунок 4.3. Приклад повторного використання однієї фотографії у різних анкетах

4.2.5. Графовий аналіз зв'язків

Після зіставлення текстів, контактів і зображень отримані зв'язки можуть бути представлені у вигляді графової моделі. Вузлами такого графа є інформаційні об'єкти – наприклад, контактні номери або оголошення, а ребрами – встановлені між ними зв'язки.

Графове представлення дозволяє побачити групи взаємопов'язаних публікацій та виділити вузли, через які проходить значна кількість зв'язків. Для цього можуть застосовуватися показники ступеня вузла та міжпосередницької центральності. Високе значення центральності свідчить про структурну значущість відповідного об'єкта у сформованому графі, але не дає підстав автоматично визначати його власника як «рекрутера», «координатора» або учасника злочинної групи.

У розглянутому прикладі один контактний вузол пов'язує три групи оголошень. Це дозволяє виділити його для подальшого аналізу та перевірити, чим пояснюється така кількість зв'язків.

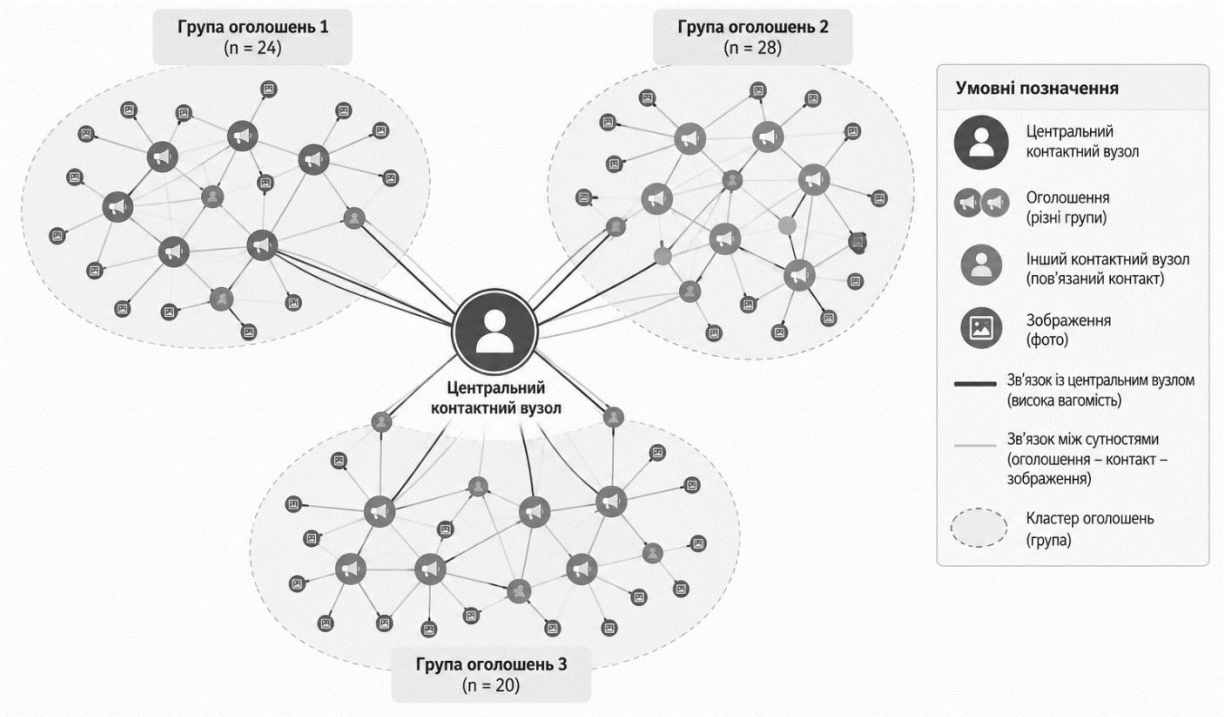


Рисунок 4.4. Графова модель зв'язків між контактним вузлом та групами оголошень. Центральний вузол характеризується високою структурною значущістю у сформованому графі.

4.2.6. Інтегрований результат і практичне значення

Поєднання декількох OSINT-методів дозволяє перейти від аналізу окремого оголошення до встановлення зв’язків між значною кількістю інформаційних об’єктів. Текстова класифікація скорочує масив для ручного перегляду, аналіз контактів виявляє повторювані ідентифікатори, порівняння фотографій встановлює повторне використання візуальних матеріалів, а графова модель наочно показує структуру виявлених зв’язків.

Практичне значення такого підходу полягає у *пріоритизації інформації для подальшої перевірки*. Чим більше незалежних ознак збігається – текст, номер телефону, електронна адреса, фотографія або інший ідентифікатор, – тим обґрунтованішою стає необхідність поглибленого аналізу відповідної групи публікацій. Разом із тим навіть сукупність таких збігів формує аналітичну гіпотезу, а не автоматичний висновок про наявність торгівлі людьми.

Отже, OSINT у межах цього кейсу виступає інструментом *пошуку, зіставлення та структурування цифрових слідів***.** Його результатом є не

встановлення винуватості конкретних осіб, а формування перевірюваних зв’язків та визначення інформаційних об’єктів, які можуть потребувати подальшої аналітичної, оперативної або процесуальної перевірки.

4.3. GIS-кейс: просторовий аналіз «гарячих точок»

4.3.1. Обґрунтування завдання

Просторовий аналіз дає можливість досліджувати, як окремі інформаційні спостереження розподіляються територіально та чи утворюють вони локальні зони підвищеної концентрації. У контексті протидії торгівлі людьми GIS доцільно використовувати не для автоматичного визначення «небезпечних територій», а для виявлення просторових закономірностей, які потребують подальшої перевірки.

Поєднання географічно прив’язаних оголошень із даними про транспортну інфраструктуру, адміністративні межі та пункти перетину державного кордону дозволяє оцінювати взаємне розташування інформаційних об’єктів і формувати гіпотези щодо можливих просторових зв’язків. При цьому концентрація оголошень біля транспортного вузла або прикордонної території сама по собі не свідчить про злочинну активність.

4.3.2. Вихідні дані

Для демонстрації можливостей GIS сформовано модельний набір із 150 спостережень, кожне з яких має умовну просторову прив’язку. До набору включено координати оголошень, отримані у вигляді GPS-міток, адрес або геотегів, а також відкриті шари транспортної інфраструктури, адміністративних меж і пунктів перетину державного кордону.

Використання модельних даних дозволяє продемонструвати роботу просторових методів без оброблення реальної інформації про постраждалих осіб. Тому отримані карти й кластери мають навчально-демонстраційний характер і не відображають фактичну географію торгівлі людьми.

4.3.3. Методологія

На першому етапі застосовано метод оцінювання щільності ядра – *Kernel Density Estimation (KDE).* Він перетворює набір окремих точок на безперервну поверхню щільності та дозволяє побачити території, де модельні спостереження розташовані найбільш концентровано. Чим більше точок знаходиться поблизу одна одної, тим вищим буде значення щільності на відповідній ділянці карти.

Kernel Density Estimation (KDE)

$$f(x) = \frac{1}{nh} \sum_{i=1}^{n} K\left(\frac{x - x_i}{h}\right) \quad (6)$$

де n – кількість точок (оголошень), h – ширина вікна, K – гаусове ядро. Результат: теплові карти, що показують зони з найбільшою концентрацією.

Другим методом є *DBSCAN*, який об'єднує просторово близькі точки у кластери. Основними параметрами алгоритму є максимальна відстань між сусідніми точками та мінімальна кількість точок, необхідна для утворення кластера. Перевагою *DBSCAN* є можливість знаходити групи довільної форми та відокремлювати поодинокі спостереження, які алгоритм визначає як «шум».

На третьому етапі результати *KDE* та *DBSCAN* накладаються на шари транспортної інфраструктури й адміністративних меж. Такий спосіб дозволяє перевірити, чи розташовані виявлені просторові концентрації поблизу транспортних вузлів, основних шляхів або прикордонних територій. Виявлений збіг розглядається лише як просторова асоціація, яка потребує пояснення за допомогою інших джерел інформації.

4.3.4. Результати модельного аналізу

У сформованому модельному наборі *KDE* виділив найбільш виражені зони концентрації спостережень у районах Києва, Львова та Одеси. Додаткові ділянки підвищеної щільності сформувалися поблизу окремих транспортних і прикордонних об'єктів. Цей результат демонструє здатність *KDE* швидко виділяти території, де кількість просторових спостережень вища порівняно з навколишніми районами.

Алгоритм *DBSCAN* у межах заданих параметрів сформував шість кластерів, серед яких найбільші розташувалися у західній частині модельної території. Частина кластерів знаходиться поблизу прикордонних районів. Такий результат не підтверджує транзитного характеру реальної діяльності, а лише демонструє, як алгоритм може виявляти локальні просторові скупчення у заданому наборі даних.

Для демонстрації можливостей маршрутного аналізу використано умовні сценарні напрямки *Київ – Львів – Польща, Одеса – південно-західний напрямок, Закарпаття – Угорщина та Чернівці – Румунія.* Вони застосовуються виключно як модельні траєкторії для перевірки взаємного розташування кластерів і транспортної мережі та не повинні інтерпретуватися як встановлені маршрути торгівлі людьми.

4.3.5. Ілюстративні матеріали

Теплова карта відображає територіальну інтенсивність розташування точок. Ділянки з вищою щільністю показують місця концентрації модельних спостережень, а не підтверджені осередки протиправної діяльності.

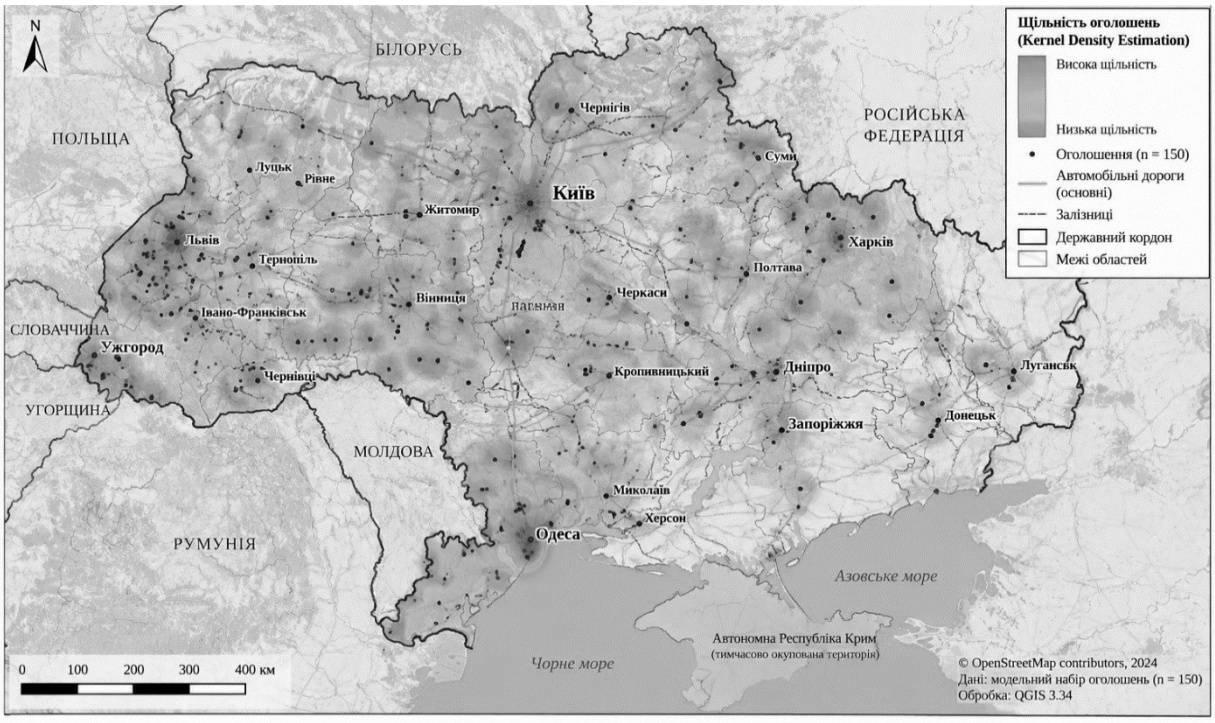


Рисунок 4.5. Теплова карта щільності модельних спостережень (KDE).

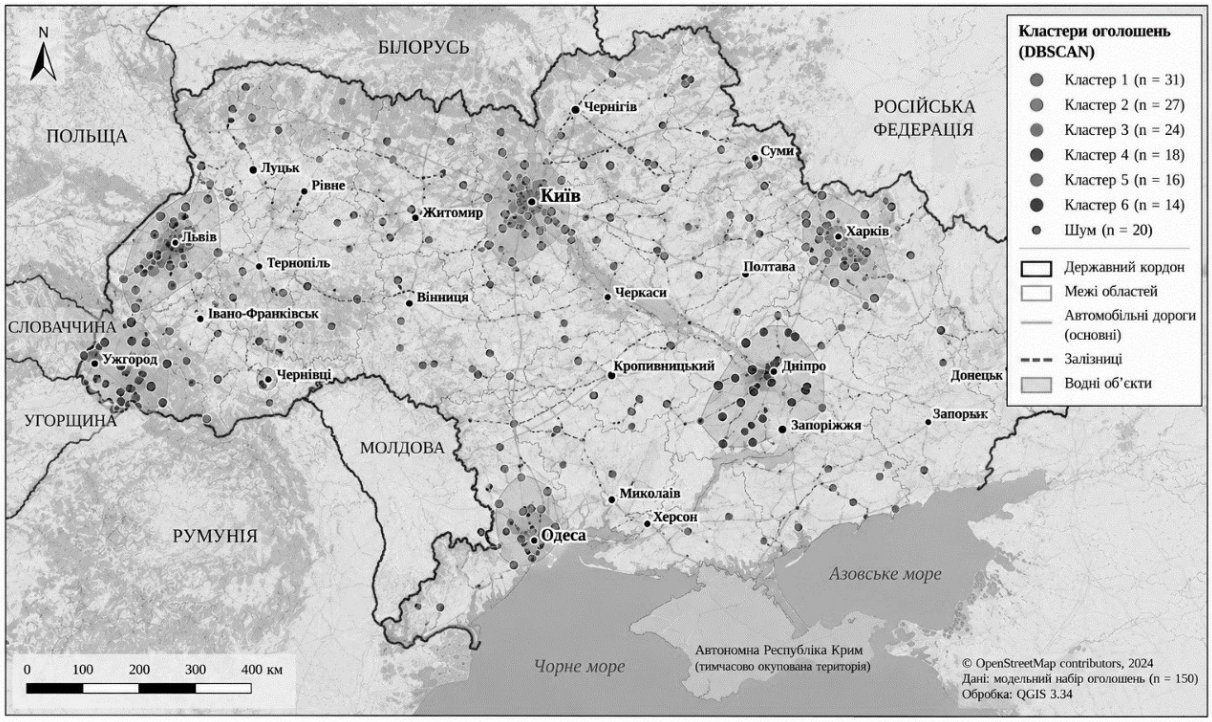


Рисунок 4.6. Просторові кластери модельних спостережень, сформовані методом DBSCAN.

Окремими кольорами відображаються групи просторово близьких точок, а поодинокі спостереження, які не відповідають установленим параметрам кластеризації, позначаються як «шум». Така візуалізація дозволяє порівнювати локальні групи та оцінювати їх просторову структуру.

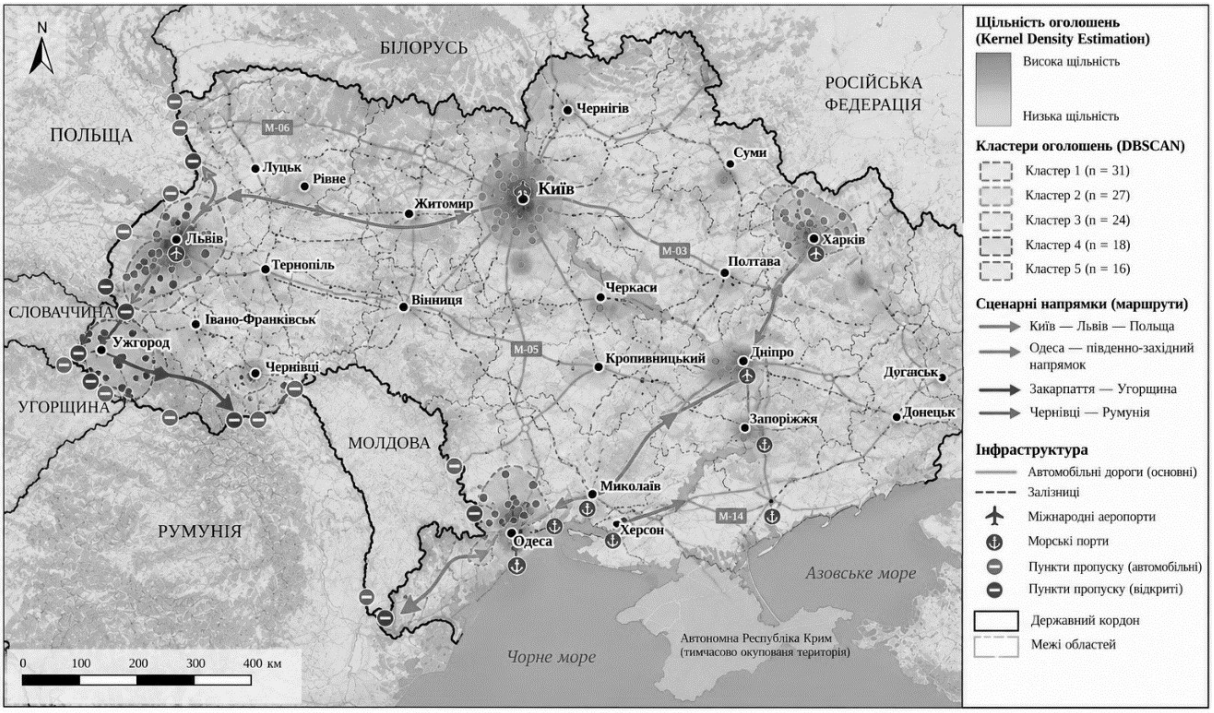


Рисунок 4.7. Схема просторового зіставлення модельних концентрацій із транспортною мережею.

Схема демонструє принцип накладання результатів просторового аналізу на транспортні та прикордонні об’єкти. Позначені напрямки мають сценарний характер і використовуються для демонстрації методики GIS-аналізу, а не для відображення фактичних маршрутів переміщення постраждалих осіб.

4.3.6. Практичне значення

Практична цінність GIS-підходу полягає у можливості перетворити великий масив географічно прив’язаних спостережень на зрозумілу просторову картину. Аналітик може визначити ділянки підвищеної концентрації даних, порівняти їх із транспортною інфраструктурою, виявити нетипові просторові групи та визначити, які з них потребують додаткової перевірки.

Для правоохоронних та інших уповноважених органів такі результати можуть використовуватися як додаткове джерело аналітичної інформації при плануванні перевірок, оцінюванні ситуації або зіставленні з іншими оперативними і статистичними даними. Вони не повинні бути самостійною підставою для посилення контролю щодо конкретної території, групи осіб або маршруту. В міжнародній взаємодії результати можуть передаватися у стандартизованому вигляді відповідно до встановлених процедур обміну інформацією.

4.3.7. Висновки

Проведений *GIS*-кейс демонструє, що поєднання *KDE, DBSCAN* та аналізу транспортної інфраструктури дозволяє досліджувати просторову структуру великих масивів географічно прив’язаних даних. *KDE* забезпечує загальне уявлення про щільність спостережень, *DBSCAN* виділяє локальні групи, а накладання на інші просторові шари допомагає оцінити можливі територіальні взаємозв’язки.

Разом із тим результати модельного кейсу не підтверджують фактичної територіальної концентрації вербування, існування реальних «гарячих точок» або маршрутів переміщення постраждалих осіб. Їх значення полягає у демонстрації методики формування та перевірки просторових гіпотез. Для

практичного використання такі результати мають зіставлятися з верифікованими даними, іншими незалежними джерелами та експертною оцінкою.

4.4. Big Data-кейс: інтеграція різнорідних даних

4.4.1. Постановка завдання

Однією з основних проблем інформаційно-аналітичної роботи у сфері протидії торгівлі людьми є розподіленість даних між різними джерелами та інформаційними системами. Текстові оголошення, контактні дані, зображення, географічні координати, відомості з відкритих реєстрів та інші цифрові об’єкти відрізняються за форматом, структурою і частотою оновлення. За наявності відповідних правових підстав до аналізу можуть також залучатися дані обмеженого доступу, зокрема фінансова або телекомунікаційна інформація.

Завдання кейсу полягає у демонстрації того, як різнорідні інформаційні потоки можуть бути приведені до єдиної структури, очищені, зіставлені та підготовлені для подальшого аналізу. Для цього використовується концепція *Data Lakehouse*, яка поєднує можливість зберігати великі обсяги різноформатних даних із засобами їх структурованої аналітичної обробки.

Реляційні бази даних при цьому не втрачають свого значення. Вони можуть залишатися ефективним компонентом системи, тоді як Lakehouse використовується як один із варіантів архітектури для інтеграції значних обсягів структурованих і неструктурованих даних.

4.4.2. Архітектура Lakehouse

Запропонована архітектура будується за багаторівневим принципом **Bronze – Silver – Gold**. Її логіка полягає у поступовому переході від первинних даних до підготовленої інформації, придатної для аналітики та візуалізації.

На рівні **Bronze** дані зберігаються максимально близько до їх початкового вигляду. Це можуть бути CSV- і Excel-файли, документи, результати OSINT-збору, записи інформаційних систем або інші цифрові об’єкти. Для кожного набору доцільно фіксувати джерело, час отримання, формат та інші метадані, необхідні для подальшої перевірки його походження.

На рівні **Silver** здійснюється очищення і нормалізація. Видаляються технічні дублікати, приводяться до єдиного формату номери телефонів, адреси електронної пошти, дати, географічні назви та інші ідентифікатори. Саме на цьому етапі створюються умови для коректного зіставлення відомостей, отриманих із різних джерел.

Рівень **Gold** містить підготовлені аналітичні набори даних. Вони можуть використовуватися для статистичного аналізу, *NLP*, кластеризації, побудови графових моделей, просторового аналізу, виявлення аномалій та формування візуалізацій.

Така структура дозволяє відокремити первинні дані від результатів їх оброблення та зберегти простежуваність переходу від вихідної інформації до аналітичного результату.

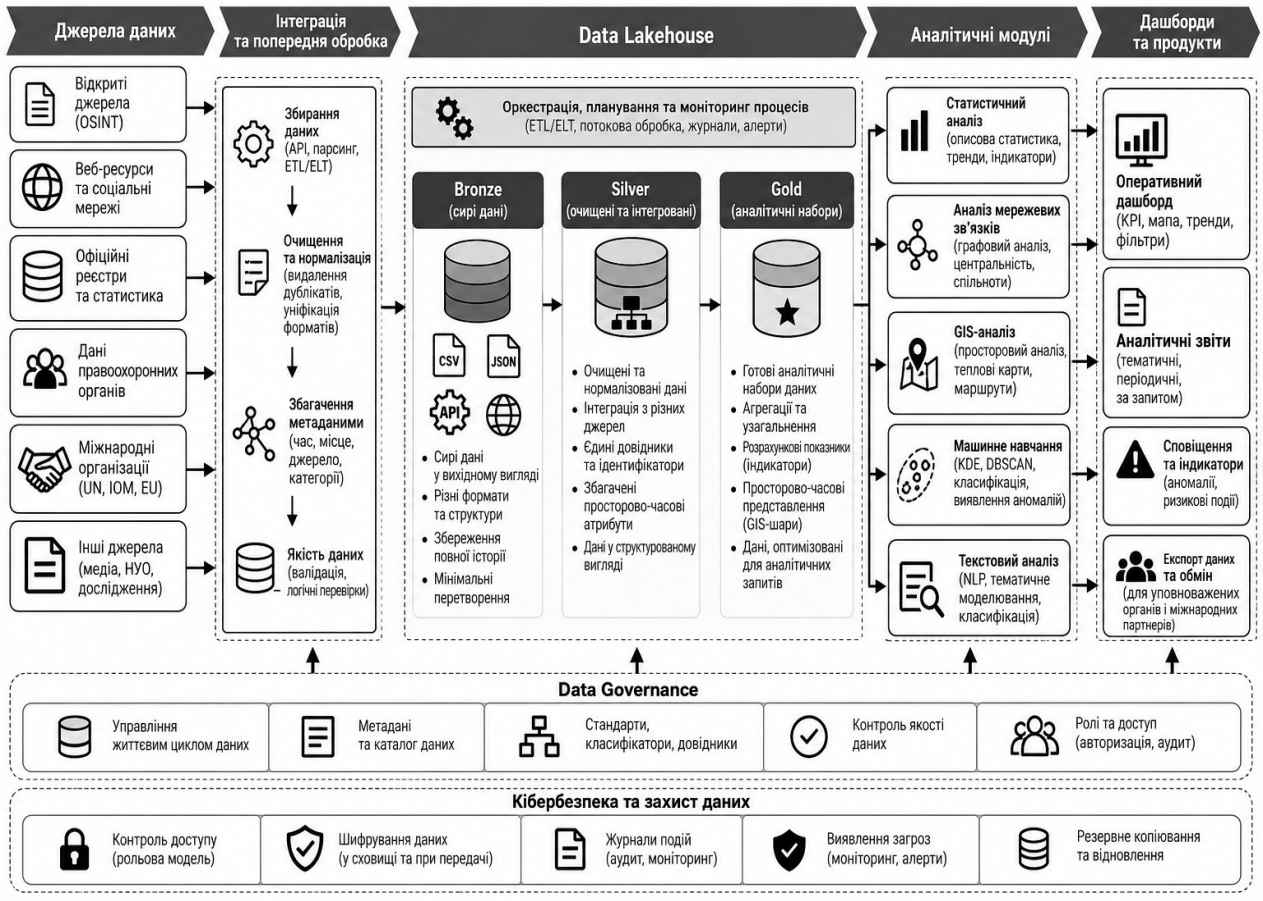


Рис. 4.8. Узагальнена архітектура Data Lakehouse: джерела даних → Bronze → Silver → Gold → аналітичні модулі та дашборди

4.4.3. Методи обробки

Після нормалізації даних можуть застосовуватися декілька взаємодоповнювальних методів. SQL-аналітика використовується для пошуку повторюваних номерів телефонів, адрес електронної пошти та інших ідентифікаторів. NLP-методи дають змогу порівнювати тексти, визначати їх семантичну подібність і групувати оголошення за змістовими характеристиками.

Графові моделі використовуються для представлення зв’язків між інформаційними об’єктами, наприклад між оголошенням, контактним номером, електронною адресою, обліковим записом або іншим цифровим ідентифікатором. Такий підхід дозволяє бачити не лише окремі збіги, а й структуру взаємозв’язків між ними. Вузли з високою кількістю зв’язків можуть отримувати підвищений аналітичний пріоритет, однак їхня структурна значущість не визначає автоматично роль конкретної особи.

Методи кластеризації можуть застосовуватися для групування оголошень за подібними текстовими, контактними, часовими або просторовими характеристиками. Аналіз часових рядів дозволяє виявляти періоди збільшення або зменшення інформаційної активності та нетипові стрибки кількості публікацій. Виявлена сезонність або аномалія при цьому розглядається як характеристика досліджуваного набору даних, а не як самостійне підтвердження зміни злочинної активності.

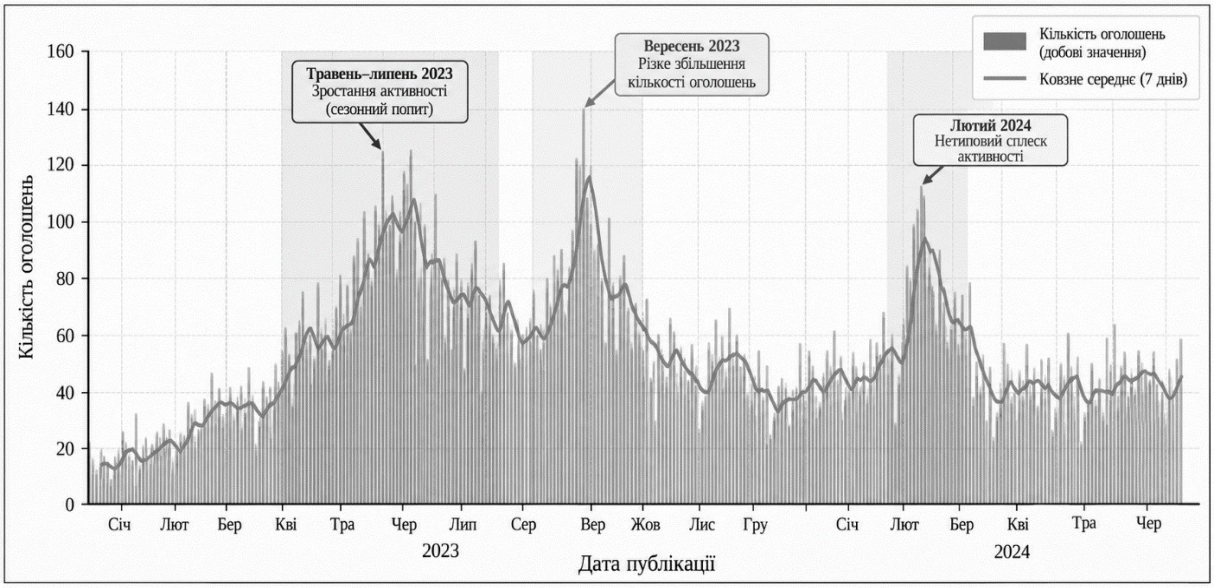


Рис. 4.9. Часова динаміка кількості оголошень у модельному наборі даних.

Часовий графік відображає зміну кількості публікацій упродовж досліджуваного періоду та дозволяє виділяти загальну тенденцію й окремі відхилення.

На схемі (Рис. 4.10.) різними групами представлено інформаційні об’єкти, подібні за вибраними характеристиками. Належність до одного кластера означає статистичну подібність об’єктів, але не підтверджує їх спільне походження або належність до однієї мережі.



Рис. 4.10. Приклад кластеризації оголошень за сукупністю ознак

4.4.4. Результати модельної апробації

У межах демонстраційного кейсу інтеграція різнорідних даних дозволила виявити повторювані контактні ідентифікатори, групи схожих оголошень, часові зміни активності та окремі нетипові спостереження. У модельному наборі понад 30 номерів телефонів повторювалися щонайменше у десяти оголошеннях, а одна адреса електронної пошти зустрічалася у 22 публікаціях на різних ресурсах.

Кластеризація розподілила тексти на декілька груп із подібною лексикою: оголошення, пов’язані з модельною сферою, сезонною роботою та короткими пропозиціями з мінімальним описом умов. Такий розподіл демонструє можливість автоматизованого структурування великих текстових масивів, однак назва або зміст кластера не визначає правомірності відповідних оголошень.

Аналіз часової складової показав періоди збільшення кількості публікацій і декілька різких відхилень від загальної динаміки. Їх доцільно розглядати як точки для додаткового аналізу причин зміни інформаційної активності.

В окремому демонстраційному фрагменті фінансових даних було виділено декілька транзакцій із повторюваним криптовалютним ідентифікатором отримувача. Подібний збіг може використовуватися для подальшого аналітичного зіставлення лише за умови законного доступу до відповідних даних. Сам факт повторного використання криптовалютної адреси або нетипової суми переказу не свідчить про злочинне походження коштів.

4.4.5. Практичне значення

Практична цінність Big Data-підходу полягає у можливості перейти від ізольованого аналізу окремих інформаційних об’єктів до їх системного зіставлення в межах єдиного аналітичного середовища. Це дозволяє скоротити обсяг ручної роботи, швидше знаходити повторювані ідентифікатори, групувати подібні матеріали та виділяти інформаційні об’єкти, які потребують подальшої перевірки.

Для аналітика результатом роботи системи можуть бути не «червоні списки», а переліки об’єктів із підвищеним аналітичним пріоритетом,

сформовані за прозорими критеріями. Такі переліки не повинні автоматично визначати осіб або контакти як пов’язані з протиправною діяльністю.

Просторові та часові результати можуть використовуватися разом з іншими верифікованими даними для оцінювання динаміки інформаційних процесів і формування робочих гіпотез. У міжвідомчій та міжнародній взаємодії доцільно використовувати стандартизовані формати обміну, узгоджені метадані та захищені канали відповідно до компетенції й процедур конкретних установ.

Таким чином, Data Lakehouse у межах запропонованого кейсу виступає не як самостійний «інструмент виявлення торгівлі людьми», а як *інфраструктура інтеграції, підготовки та аналітичного опрацювання різнорідних даних*. Її основна перевага полягає у можливості зберегти зв’язок між вихідними даними та результатами аналізу, поєднати різні методи оброблення й забезпечити масштабування інформаційно-аналітичного процесу. Практична ефективність такого рішення потребує окремої перевірки на верифікованих даних із урахуванням вимог інформаційної безпеки, правомірності доступу та якості вихідної інформації.

4.5. ML-кейс: виявлення аномалій у транзакціях

4.5.1. Постановка завдання

Аналіз великих масивів транзакційних даних ускладнюється тим, що більшість операцій відповідає типовій поведінці, тоді як окремі спостереження можуть істотно відрізнятися за сумою, частотою, часовими інтервалами або сукупністю інших характеристик. Ручний перегляд значної кількості операцій є ресурсомістким, тому методи статистичного аналізу та машинного навчання можуть використовуватися для автоматизованого виділення нетипових спостережень.

Завданням кейсу є демонстрація можливостей методів виявлення аномалій для первинної фільтрації транзакційного потоку. При цьому аномальна операція розглядається не як підтвердження протиправної діяльності, а як статистично нетипове спостереження, яке може потребувати додаткового аналізу.

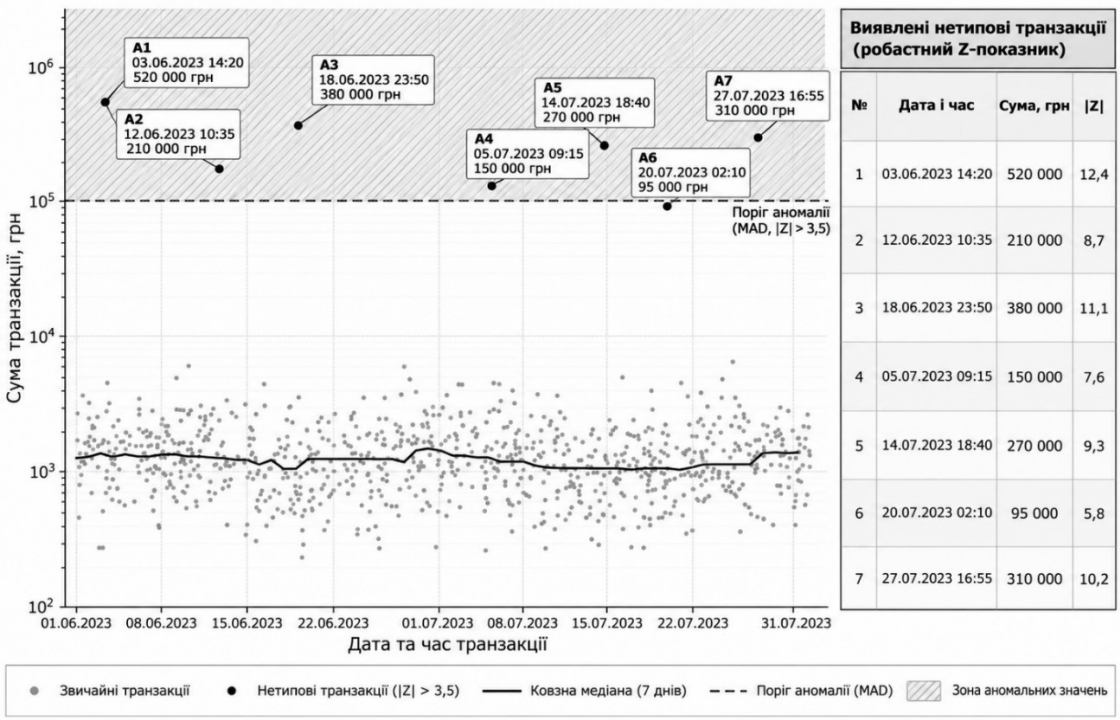
4.5.2. Характеристика даних

Для апробації використано синтетичний набір приблизно з 220 транзакцій. До основних характеристик включено суму переказу, часовий інтервал між операціями та тип каналу проведення транзакції. Для перевірки здатності алгоритмів знаходити нетипові спостереження до набору навмисно введено операції, що відрізнялися від основної сукупності за сумою, часовими параметрами або напрямком руху коштів.

Таким чином, набір має демонстраційний характер. Отримані на його основі результати характеризують роботу обраних методів у контрольованих умовах і не можуть безпосередньо переноситися на реальні фінансові потоки або використовуватися для оцінювання фактичної злочинної активності.

4.5.3. Методи виявлення аномалій

На першому етапі застосовано статистичний підхід на основі *робастної оцінки відхилення від медіани із використанням MAD (Median Absolute Deviation).* Для кожного спостереження визначається ступінь його віддаленості від типових значень. Спостереження, для яких модифікований Z-показник перевищує встановлений поріг, позначаються як потенційні аномалії.



Виявлені нетипові транзакції (робастний Z-показник)

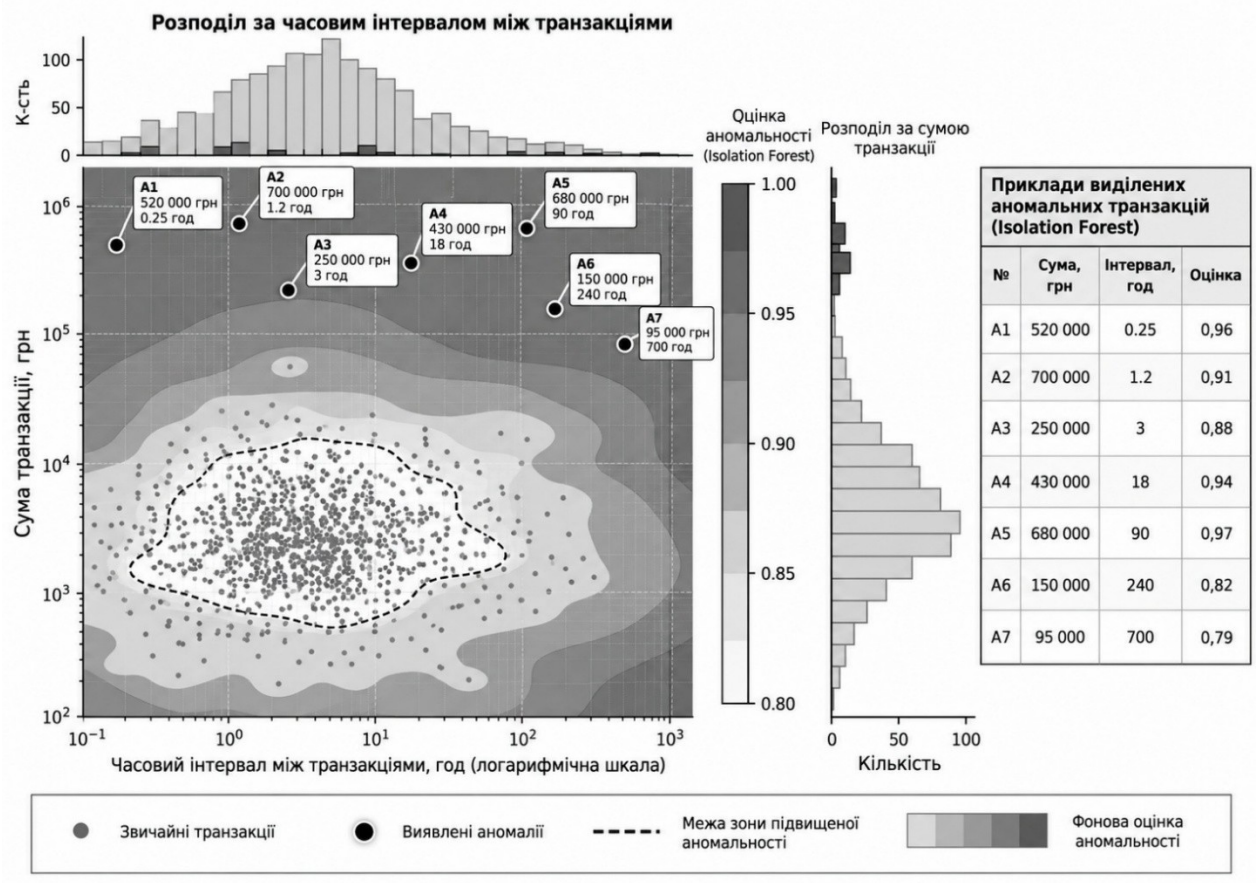
№	Дата і час	Сума, грн	|Z|
1	03.06.2023 14:20	520 000	12,4
2	12.06.2023 10:35	210 000	8,7
3	18.06.2023 23:50	380 000	11,1
4	05.07.2023 09:15	150 000	7,6
5	14.07.2023 18:40	270 000	9,3
6	20.07.2023 02:10	95 000	5,8
7	27.07.2023 16:55	310 000	10,2

Рис. 4.11. Виявлення нетипових транзакцій за допомогою робастного Z-

показника.

Перевагою такого підходу є простота та швидкість обчислення. Він добре підходить для первинного пошуку різких відхилень за окремою числовою ознакою, наприклад сумою операції. Водночас одновимірний статистичний критерій не враховує складні комбінації декількох параметрів.

На часовому графіку окремими маркерами доцільно виділити операції, які перевищують установлений статистичний поріг. Така візуалізація демонструє, як метод дозволяє швидко відокремити нетипові значення від основної маси спостережень.



Приклади виділених аномальних транзакцій (Isolation Forest)

№	Сума, грн	Інтервал, год	Оцінка
A1	520 000	0.25	0,96
A2	700 000	1.2	0,91
A3	250 000	3	0,88
A4	430 000	18	0,94
A5	680 000	90	0,97
A6	150 000	240	0,82
A7	95 000	700	0,79

Рис. 4.12. Виявлення аномалій методом Isolation Forest у просторі ознак «сума транзакції – часовий інтервал».

Для аналізу декількох характеристик одночасно застосовано алгоритм *Isolation Forest.* Його логіка полягає у багаторазовому випадковому поділі простору ознак. Спостереження, які суттєво відрізняються від основної сукупності, зазвичай відокремлюються швидше та отримують вищий показник аномальності.

У межах цього кейсу *Isolation Forest* дозволяє одночасно враховувати, наприклад, суму транзакції та часовий інтервал між операціями. За наявності ширшого набору даних до моделі можуть включатися й інші характеристики, якщо їх використання є методологічно та правомірно обґрунтованим.

Двовимірне представлення дозволяє наочно показати, що частина нетипових спостережень визначається не лише одним екстремальним значенням, а незвичайним поєднанням декількох параметрів.

Перспективним напрямом для складніших масивів даних є використання *автокодерів (Autoencoder)***.** Така нейромережева модель навчається відтворювати типові спостереження, а значне збільшення похибки реконструкції може використовуватися як ознака нетиповості. У межах цього кейсу автокодер розглядається як можливий напрям подальшого розвитку, а не як апробований метод.

4.5.4. Результати аналізу

За встановленого порогу робастний статистичний метод виділив у синтетичному наборі 7 транзакцій**,** що суттєво відрізнялися від основної сукупності. Isolation Forest додатково дозволив визначити спостереження, для яких нетиповість була пов’язана з поєднанням декількох характеристик, зокрема суми операції та тривалості інтервалу між подіями.

Отриманий результат демонструє різницю між одновимірним і багатовимірним аналізом. Статистичний метод ефективно виділяє явні відхилення за окремим показником, тоді як Isolation Forest дає змогу знаходити спостереження, які стають нетиповими лише внаслідок специфічного поєднання кількох ознак.

Оскільки використаний набір є синтетичним і не містить незалежно підтверджених класів «правомірна» та «протиправна» транзакція, за його результатами не можна робити висновок про фактичне зменшення кількості хибнопозитивних спрацювань. У межах кейсу можна оцінити насамперед здатність алгоритмів скорочувати кількість операцій, які потребують подальшого ручного аналізу.

4.5.5. Інтеграція у систему моніторингу

Методи виявлення аномалій можуть бути включені до раніше запропонованої архітектури Data Lakehouse. На рівні **Bronze** зберігаються первинні транзакційні записи разом із метаданими про їх походження. На рівні **Silver** здійснюються очищення, нормалізація форматів, приведення часових позначок і підготовка ознак. На рівні **Gold** формуються аналітичні набори, до яких застосовуються статистичні та ML-алгоритми.

Для оперативної первинної фільтрації можуть використовуватися прості статистичні критерії, а більш складні багатовимірні моделі – застосовуватися під час поглибленого пакетного аналізу. Результати доцільно відображати на аналітичному дашборді у вигляді кількості виявлених аномалій за період, динаміки показників та переліку операцій із підвищеним аналітичним пріоритетом.

Водночас автоматизоване сповіщення не повинно означати автоматичне блокування операції або визначення її учасника як причетного до протиправної діяльності. Результат алгоритму має передаватися уповноваженому фахівцю для подальшої перевірки з урахуванням контексту та інших доступних відомостей.

4.5.6. Практичне значення

Практичне значення методів виявлення аномалій полягає насамперед у *пріоритизації великого транзакційного масиву***.** Замість однакового аналізу всіх операцій система дозволяє виділити обмежену кількість спостережень із нетиповими характеристиками та спрямувати на них увагу аналітика.

Для фінансового моніторингу такі методи можуть використовуватися як додатковий механізм відбору операцій для подальшого аналізу. Для правоохоронної аналітики результати можуть мати значення лише у поєднанні з іншими законно отриманими та перевіреними відомостями. Аномалія за сумою, частотою, часовим інтервалом або іншими параметрами сама по собі не підтверджує відмивання коштів, фінансування вербування чи будь-яку іншу протиправну діяльність.

Поєднання статистичних і машинних методів дозволяє аналізувати як очевидні відхилення, так і складні багатовимірні комбінації характеристик. При цьому машинне навчання виконує функцію *інструмента аналітичного відбору***,** а не автоматичного механізму встановлення юридично значущих обставин.

Таким чином, ML-кейс демонструє можливість використання автоматизованого аналізу для пошуку нетипових транзакцій у великих інформаційних масивах. Його результатом є не виявлення «злочинних транзакцій», а *формування обґрунтованого переліку нетипових спостережень для подальшої експертної перевірки*. Оцінювання точності, рівня хибнопозитивних спрацювань і практичної ефективності такого підходу потребує окремої апробації на верифікованих даних із відомими контрольними класами.

Висновок до розділу 4

Результати апробації практичних кейсів показують, що найбільшу аналітичну цінність має не ізольоване застосування *OSINT, GIS, Big Data* або машинного навчання, а їх послідовне поєднання в межах єдиного інформаційно-аналітичного процесу. Кожен із розглянутих підходів вирішує окрему частину завдання: відкриті джерела забезпечують первинне інформаційне наповнення, просторовий аналіз додає географічний контекст, архітектура *Data Lakehouse* забезпечує інтеграцію та підготовку різнорідних даних, а алгоритмічні методи допомагають виділяти закономірності й нетипові спостереження.

OSINT-кейс продемонстрував можливість переходу від аналізу окремих оголошень до системного зіставлення текстів, контактних даних, зображень та інших цифрових ідентифікаторів. Основне значення такого підходу полягає у скороченні обсягу інформації, що потребує ручного перегляду, та формуванні перевірюваних аналітичних гіпотез. Повторюваний номер телефону, схоже зображення або текстова подібність не підтверджують самі по собі факту вербування чи належності до певної мережі, але їх сукупність дозволяє обґрунтовано визначати об’єкти для поглибленої перевірки.

GIS-кейс показав можливість дослідження просторової структури географічно прив’язаних даних. Поєднання *KDE, DBSCAN* і транспортних шарів дозволяє виділяти зони концентрації модельних спостережень, локальні просторові групи та їх розташування відносно інфраструктури. Водночас такі результати мають розглядатися як інструмент формування просторових гіпотез, а не як автоматичне визначення «гарячих точок» злочинної активності або фактичних маршрутів переміщення постраждалих осіб. Практична інтерпретація GIS-результатів потребує зіставлення з іншими незалежними та верифікованими даними.

Big Data-кейс засвідчив доцільність багаторівневої організації різнорідних інформаційних масивів. Архітектура *Data Lakehouse* дозволяє розділити первинні, очищені та аналітично підготовлені дані, зберігаючи їх походження і послідовність перетворень. Такий підхід важливий не лише для масштабування обчислень, а й для забезпечення простежуваності аналітичного процесу. Інтеграція текстових, контактних, просторових та інших ознак у єдиному середовищі створює умови для комплексного аналізу, але якість його результатів безпосередньо залежить від якості, повноти та правомірності використання вихідних даних.

ML-кейс продемонстрував можливість застосування статистичних і машинних методів для автоматизованого виділення нетипових транзакцій. Робастні статистичні показники ефективні для пошуку явних відхилень, тоді як *Isolation Forest* дозволяє враховувати комбінації декількох характеристик. Принципово важливо, що виявлена аномалія означає лише статистичну нетиповість, а не протиправний характер операції. Тому алгоритмічний результат повинен використовуватися для пріоритизації подальшої перевірки, а не для автоматичного формування висновку щодо конкретної транзакції або її учасників.

Спільною рисою всіх розглянутих кейсів є поступовий перехід від великого масиву слабко структурованої інформації до обмеженої кількості об’єктів, які потребують поглибленої аналітичної уваги. У такій моделі

автоматизація виконує функцію *фільтрації, структурування та пріоритизації*, тоді як змістовна оцінка результату залишається за фахівцем. Це дозволяє зменшити інформаційне навантаження без підміни професійного та процесуального рішення алгоритмічною оцінкою.

Водночас проведені кейси мають переважно демонстраційний характер і ґрунтуються на модельних або синтетичних наборах даних. Тому їх результати не можуть розглядатися як емпіричне підтвердження реальних масштабів, географії, фінансових механізмів або структури торгівлі людьми. Оцінювання практичної ефективності запропонованих підходів потребує подальшої апробації на верифікованих даних із використанням визначених показників якості, контролем хибнопозитивних і хибнонегативних результатів та експертною перевіркою.

Таким чином, практичні кейси підтверджують насамперед *функціональну сумісність і взаємодоповнюваність OSINT, GIS, Big Data* та *ML* у межах єдиного аналітичного контуру. Їх інтеграція створює основу для побудови систем підтримки аналітичної діяльності, у яких дані послідовно збираються, очищуються, зіставляються, просторово та алгоритмічно аналізуються, а результати проходять експертну верифікацію. Подальший розвиток такого підходу має ґрунтуватися на принципах правомірності, перевірюваності, інформаційної безпеки, пояснюваності алгоритмів і пріоритетного захисту прав та безпеки постраждалих осіб.

РОЗДІЛ 5. ПЕРСПЕКТИВИ РОЗВИТКУ ТА ІНТЕГРАЦІЯ В НАЦІОНАЛЬНУ СИСТЕМУ БЕЗПЕКИ

5.1. Необхідність інтеграції результатів у державну політику

5.1.1. Передумови

Результати апробації *OSINT, GIS, Big Data* та методів машинного навчання свідчать насамперед про їх потенціал як засобів підтримки інформаційно-аналітичної діяльності. Перехід від окремих експериментальних рішень до практичного використання потребує включення таких технологій у вже наявні організаційні, правові та інформаційні процеси державних органів, а не створення паралельної системи, що функціонуватиме відокремлено від них.

Необхідність такого підходу зумовлена насамперед фрагментарністю інформації. Дані, які можуть мати значення для протидії торгівлі людьми, формуються у різних середовищах, мають неоднакову структуру, рівень достовірності та правовий режим доступу. Частина відомостей є відкритою, інша може бути отримана лише уповноваженими суб’єктами відповідно до законодавства. Тому ключовим завданням державної політики має бути не максимальна централізація всіх доступних даних, а створення умов для їх правомірного, контрольованого та технологічно сумісного використання**.**

Інтеграція аналітичних технологій також пов’язана з необхідністю міжвідомчої взаємодії. Протидія торгівлі людьми охоплює правоохоронний, прикордонний, фінансовий, соціальний та міжнародний напрями, тому повна інформаційна картина не завжди може бути сформована в межах одного відомства. Водночас обмін даними має здійснюватися відповідно до компетенції кожного суб’єкта, установленої мети оброблення інформації та принципу мінімально необхідного доступу.

Базовим нормативним актом у цій сфері залишається Закон України «Про протидію торгівлі людьми», який визначає організаційно-правові засади державної політики у цій сфері. Стратегія національної безпеки України також

передбачає розвиток координації та інформаційно-аналітичних спроможностей держави.

5.1.2. Основні напрями інтеграції

Для системи МВС та Національної поліції перспективним є використання *OSINT* і автоматизованої аналітики як допоміжних засобів первинного опрацювання відкритих даних. Такі модулі можуть застосовуватися для пошуку повторюваних контактних ідентифікаторів, подібних публікацій, повторного використання зображень та інших інформаційних зв'язків. Їх результатом має бути не автоматичне визначення «підозрілих осіб», а формування переліку інформаційних об'єктів, що потребують перевірки аналітиком.

GIS-компонент може доповнювати таку систему просторовим контекстом. Карти щільності, кластеризація та зіставлення з транспортною інфраструктурою придатні для виявлення територіальних закономірностей у даних. Проте встановлена просторова концентрація не повинна безпосередньо перетворюватися на рішення щодо посилення контролю чи спрямування ресурсів без підтвердження іншими джерелами.

У діяльності Державної прикордонної служби просторово-часові аналітичні результати можуть використовуватися як один із додаткових інформаційних компонентів для оцінювання ситуації. Доцільнішим є зіставлення таких результатів із власними верифікованими даними ДПСУ, ніж автоматичне визначення «ризикових коридорів» лише за результатами *GIS*-моделей.

У сфері фінансового моніторингу методи статистичного аналізу та машинного навчання можуть застосовуватися для виділення операцій із нетиповими характеристиками. *Z-score, MAD, Isolation Forest* та інші алгоритми здатні зменшувати обсяг транзакційного масиву, що потребує поглибленого аналізу, однак аномальність операції не є підтвердженням її злочинного походження. Практичне використання таких методів повинно відбуватися лише уповноваженими суб'єктами та щодо даних, доступ до яких має належну правову підставу.

У сфері кібербезпеки й цифрової криміналістики інтеграція має забезпечувати контроль цілісності цифрових матеріалів, захист каналів передавання, журналювання операцій та розмежування доступу. Аналіз darknet-ресурсів, метаданих, повторного використання зображень або ознак синтетичного контенту доцільно розглядати як спеціалізовані аналітичні функції, результати яких потребують експертної перевірки.

Таким чином, державна інтеграція не повинна зводитися до створення одного універсального сховища, до якого всі відомства мають однаковий доступ. Більш обґрунтованою є *багаторівнева або федеративна модель*, за якої дані залишаються під контролем відповідних суб'єктів, а для спільного аналізу передаються лише необхідні відомості, аналітичні результати або стандартизовані інформаційні об'єкти.

5.1.3. Правові та стратегічні засади

Інтеграція інформаційно-аналітичних технологій у державну політику повинна здійснюватися в межах чинного законодавства, а не випереджати його. Закон України «Про протидію торгівлі людьми» встановлює базові організаційно-правові засади державної політики у цій сфері. Стратегія національної безпеки України визначає координацію державних органів, розвиток спроможностей та використання сучасних технологій як складові забезпечення національної стійкості.

У попередній редакції до правової основи було віднесено Доктрину інформаційної безпеки 2017 року. Для актуального викладу коректніше враховувати Стратегію інформаційної безпеки, затверджену Указом Президента України № 685/2021, яким відповідні положення Указу № 47/2017 про Доктрину інформаційної безпеки були визнані такими, що втратили чинність.

Правове забезпечення майбутньої інформаційно-аналітичної системи має охоплювати визначення мети оброблення даних, компетенції суб'єктів, правил міжвідомчого обміну, строків зберігання, процедур надання і припинення доступу, аудиту дій користувачів та порядку роботи з інформацією обмеженого доступу. Особливого значення набуває розмежування між відкритими даними,

відомчою інформацією та персональними даними, оскільки різний правовий режим не дозволяє механічно об’єднувати всі джерела в єдине доступне для всіх сховище.

Алгоритмічні рішення також повинні залишатися перевірюваними. Якщо система визначає інформаційний об’єкт як нетиповий або надає йому підвищений аналітичний пріоритет, користувач повинен мати можливість встановити, які дані та критерії вплинули на такий результат. Автоматизована оцінка не повинна самостійно визначати юридичний статус особи, факт злочину або необхідність застосування процесуальних заходів.

5.1.4. Організаційні умови та обмеження

Основним організаційним завданням є визначення чітких ролей між суб’єктами системи. Міжвідомча платформа не повинна дублювати функції Національної поліції, ДПСУ, СБУ, Держфінмоніторингу чи інших органів. Її доцільно розглядати як інфраструктуру для узгодженого аналітичного обміну, а компетенція щодо первинного отримання даних, їх перевірки та прийняття рішень має залишатися за відповідними уповноваженими органами.

Другим принциповим питанням є розмежування доступу. Користувач повинен отримувати не весь наявний масив, а лише ті категорії даних, які необхідні для виконання його функцій. Це потребує рольових моделей доступу, журналювання дій, періодичного перегляду повноважень і технічної можливості встановити історію роботи з конкретними даними.

Не менш важливим є кадровий компонент. Автоматизація не усуває потреби у фахівцеві, а змінює характер його роботи. Аналітик повинен уміти оцінювати якість вихідних даних, інтерпретувати статистичні й просторові результати, розуміти обмеження ML-моделей і відокремлювати алгоритмічний сигнал від встановленого факту. Тому підготовка персоналу має охоплювати одночасно інформаційні технології, аналітику, правові основи роботи з даними та питання захисту прав людини.

5.1.5. Очікуваний ефект інтеграції

Інтеграція може забезпечити більш послідовний інформаційно-аналітичний процес, у якому дані з різних джерел описуються за узгодженими правилами, а результати можуть бути простежені до вихідного джерела. Це зменшує втрату контексту під час міжвідомчої передачі та полегшує повторну перевірку аналітичних висновків.

Автоматизована попередня фільтрація здатна скорочувати обсяг інформації, що потребує ручного перегляду. Її ефект полягає не в усуненні аналітика, а в перенесенні його уваги з масового первинного перегляду на перевірку обмеженої кількості пріоритетних спостережень.

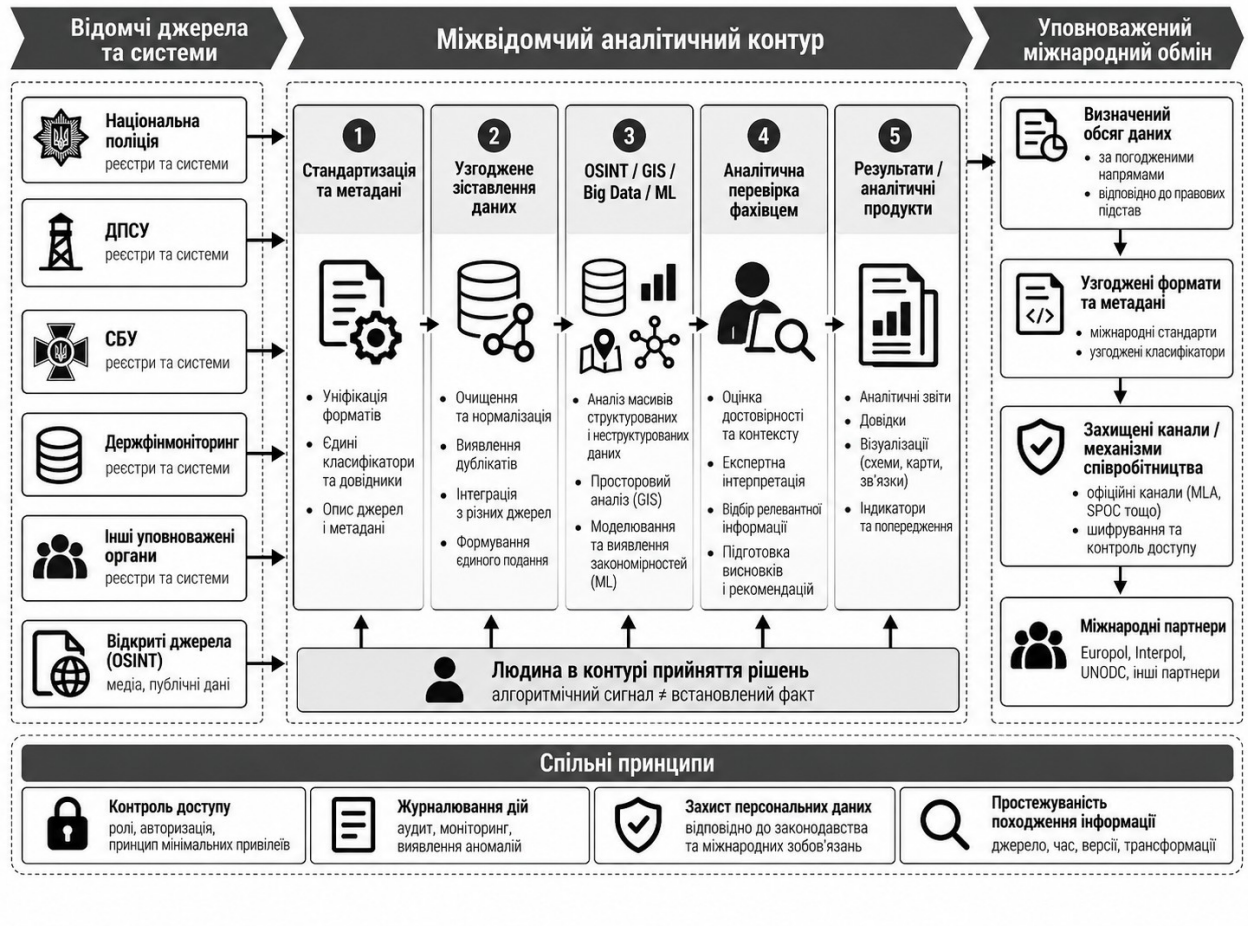


Рис. 5.1. Концептуальна схема інтеграції інформаційно-аналітичних технологій: відомчі джерела та системи → міжвідомчий аналітичний контур → уповноважений міжнародний обмін.

Додатковою перевагою є підвищення простежуваності роботи з даними. Реєстрація джерела, часу отримання, етапів перетворення та дій користувачів

дозволяє краще контролювати походження інформації й відтворювати логіку формування результату.

Міжнародна взаємодія також може бути спрощена за рахунок стандартизованого опису даних, метаданих і результатів аналізу. При цьому йдеться не про пряме підключення до інформаційних систем Europol, Interpol чи *UNODC,* а про використання передбачених механізмів співробітництва, узгоджених форматів і захищених каналів відповідно до компетенції сторін.

У такій моделі відомчий рівень відповідає за первинне формування та перевірку даних, міжвідомчий – за стандартизоване зіставлення й комплексний аналіз, а міжнародний – за передавання визначеного обсягу інформації через установлені механізми співробітництва. На всіх рівнях мають діяти спільні принципи контролю доступу, журналювання, захисту персональних даних і простежуваності походження інформації.

5.1.6. Висновки

Інтеграція результатів дослідження у державну політику доцільна не як одномоментне створення масштабної централізованої платформи, а як поетапний розвиток взаємодіючих інформаційно-аналітичних спроможностей**.** Початковим етапом має бути апробація окремих модулів у контрольованому середовищі, після чого можливі оцінювання їх ефективності, інформаційної безпеки, правомірності та організаційної сумісності.

Принципове значення має збереження людини в контурі прийняття рішень. OSINT, GIS, Big Data та ML повинні допомагати структурувати інформацію, знаходити зв’язки, просторові закономірності й нетипові спостереження, але не підміняти професійну оцінку аналітика, слідчого чи іншої уповноваженої особи.

Отже, інтеграція сучасних інформаційних технологій може підвищити керованість і масштабованість аналітичних процесів лише за умови одночасного забезпечення правомірності доступу до даних, міжвідомчого розмежування повноважень, інформаційної безпеки, пояснюваності алгоритмічних результатів та пріоритетного захисту прав постраждалих осіб**.** Саме така модель створює основу для переходу від окремих технологічних експериментів до стійкої

системи інформаційно-аналітичної підтримки державної політики у сфері протидії торгівлі людьми.

5.2. Технічні перспективи розвитку

Подальший розвиток інформаційно-аналітичного підходу до протидії торгівлі людьми пов’язаний не стільки з упровадженням окремих нових програмних продуктів, скільки з формуванням цілісної технологічної архітектури, здатної поєднувати різнорідні джерела даних, аналітичні модулі, GIS, засоби машинного навчання та механізми інформаційної безпеки. Така архітектура має залишатися модульною, масштабованою та придатною до поетапного впровадження, оскільки різні компоненти можуть мати неоднаковий рівень готовності, правові обмеження та вимоги до доступу.

5.2.1. Розвиток Data Lakehouse як інтеграційного ядра

Одним із перспективних напрямів є розвиток *Data Lakehouse* як середовища для накопичення, підготовки та аналітичного використання різнорідних даних. Його призначення полягає у поєднанні переваг сховищ неструктурованих даних із можливостями структурованої аналітики.

На рівні державної або міжвідомчої системи така архітектура не обов’язково повинна означати фізичне зосередження всіх даних в одному сховищі. Доцільнішою є модель, у якій *Data Lakehouse* виконує роль спільного аналітичного контуру, а первинні дані можуть залишатися у відомчих системах відповідно до компетенції та правового режиму доступу.

Архітектура може будуватися за вже розглянутим принципом **Bronze – Silver – Gold**. Рівень Bronze забезпечує збереження первинних даних разом із метаданими про джерело та час отримання. На рівні Silver здійснюються очищення, нормалізація, дедуплікація та приведення ідентифікаторів до уніфікованого формату. Gold-рівень містить аналітично підготовлені набори для SQL-запитів, GIS, NLP, графового аналізу, машинного навчання та візуалізації.

Для оброблення великих потоків можуть використовуватися технології потокової та пакетної обробки, зокрема Kafka, Flink, Spark або функціонально

аналогічні рішення. Вибір конкретного технологічного стеку має визначатися обсягом даних, швидкістю їх надходження, вимогами до відмовостійкості та можливостями наявної державної інфраструктури, а не необхідністю застосування конкретного програмного продукту.

Принциповим елементом архітектури повинна залишатися простежуваність: від аналітичного результату має бути можливість повернутися до вихідного джерела та встановити, які операції були виконані з даними на кожному етапі.

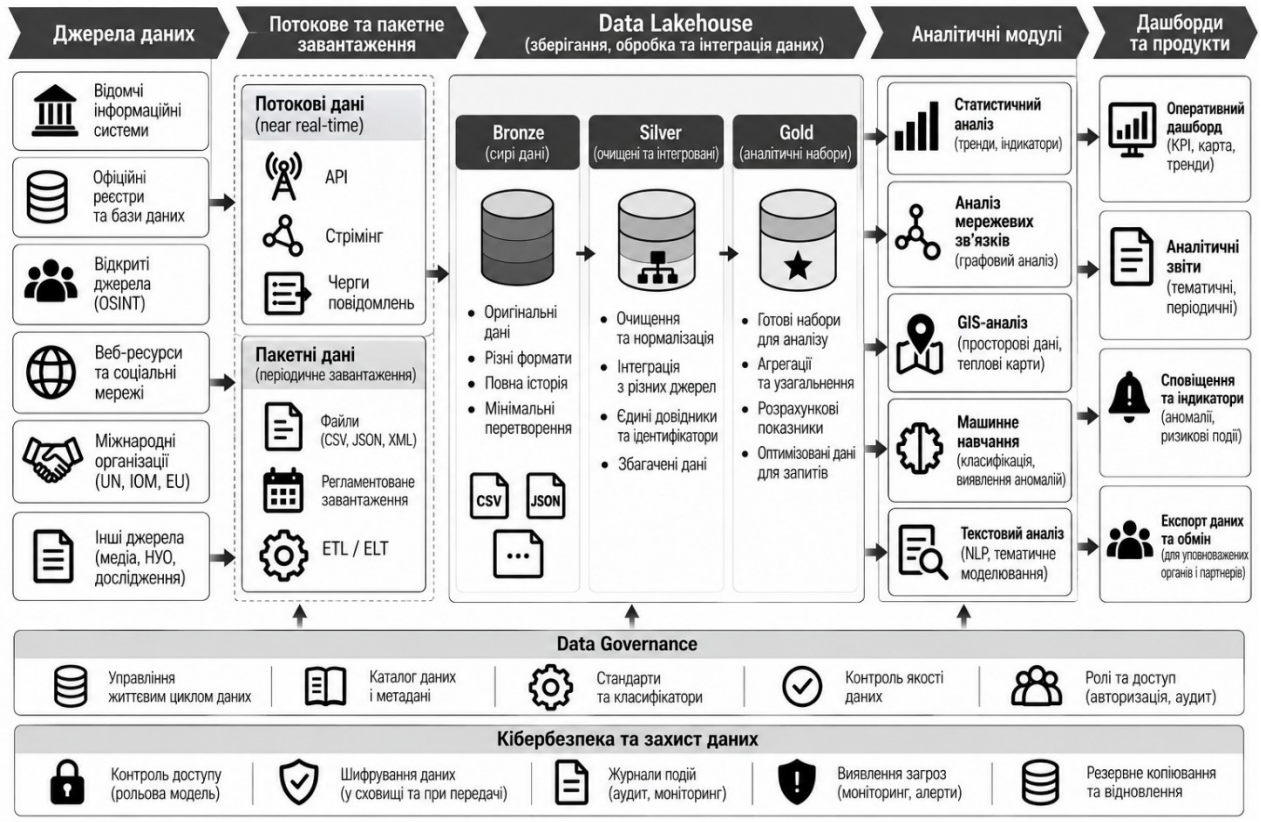


Рис. 5.2. Перспективна архітектура Data Lakehouse: джерела даних → потокове та пакетне завантаження → Bronze → Silver → Gold → аналітичні модулі та дашборди.

5.2.2. Розвиток засобів штучного інтелекту та машинного навчання

Штучний інтелект доцільно розглядати як аналітичний шар, що працює поверх підготовлених і контрольованих наборів даних. Його основним призначенням є автоматизація операцій, які складно виконувати вручну у великих інформаційних масивах.

Для текстових даних перспективними є *NLP*-моделі, що дозволяють визначати семантичну подібність оголошень, виділяти сутності, групувати повідомлення за тематикою та знаходити повторювані мовні конструкції. При цьому окремі слова або словосполучення не повинні використовуватися як автоматичні ознаки протиправної діяльності: значення має їх контекст і поєднання з іншими перевіреними даними.

Методи виявлення аномалій, зокрема *Isolation Forest* та автокодери, можуть застосовуватися до багатовимірних наборів для пошуку нетипових спостережень. Для часових рядів перспективним є використання моделей прогнозування та детекції змін динаміки, однак прогноз повинен супроводжуватися оцінкою невизначеності й не трактуватися як передбачення конкретної злочинної події.

Для графових даних можуть досліджуватися алгоритми машинного навчання, включаючи *Graph Neural Networks*. Їх призначенням може бути аналіз складних структур взаємозв'язків, класифікація типів вузлів або прогнозування можливих зв'язків. При цьому модель не повинна автоматично визначати «злочинну мережу» або роль конкретної особи лише на підставі структури графа.

Обов'язковою вимогою до майбутніх *AI*-модулів має бути пояснюваність результату. Методи *XAI*, зокрема *SHAP* та інші засоби інтерпретації, можуть допомагати визначити, які ознаки найбільше вплинули на алгоритмічну оцінку. Пояснюваність підвищує можливість експертної перевірки, але не замінює правову оцінку та не надає алгоритмічному результату самостійної доказової сили.

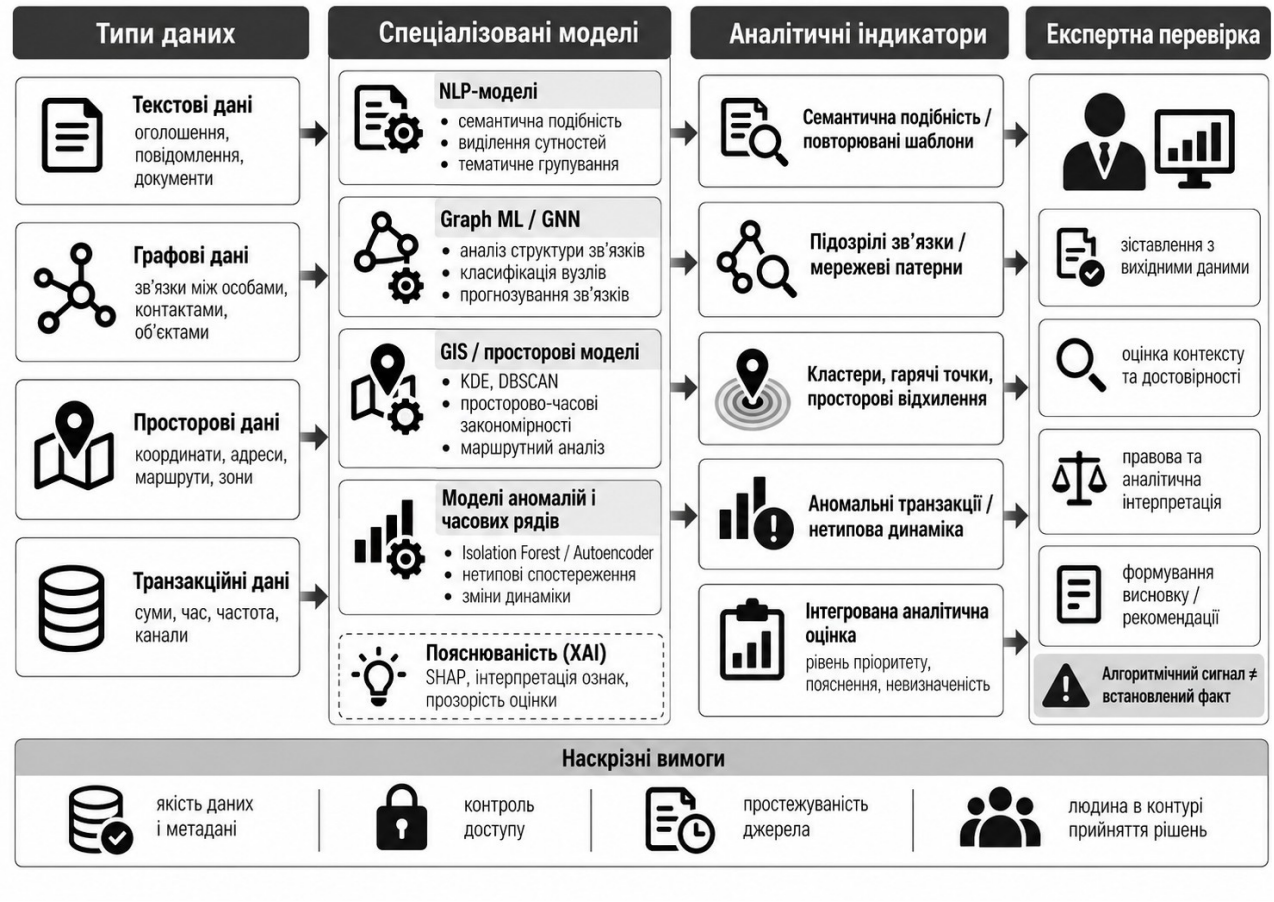


Рис. 5.3. Концептуальна структура AI/ML-модулів: текстові, графові, просторові та транзакційні дані → спеціалізовані моделі → аналітичні індикатори → експертна перевірка.

5.2.3. Розвиток GIS-компонента

GIS-компонент має забезпечувати просторовий і просторово-часовий вимір аналітики. Його функції доцільно розвивати від простої картографічної візуалізації до комплексного аналізу взаємного розташування інформаційних об'єктів, транспортної інфраструктури та інших тематичних шарів.

KDE може використовуватися для оцінювання щільності спостережень, а *DBSCAN* – для пошуку локальних просторових груп. Маршрутний аналіз на основі мережевих алгоритмів може допомагати оцінювати транспортну доступність, можливі сценарні напрямки переміщення або взаємозв'язок між точками. Водночас найкоротший або оптимальний маршрут, розрахований *GIS*, не є фактичним маршрутом переміщення конкретної людини.

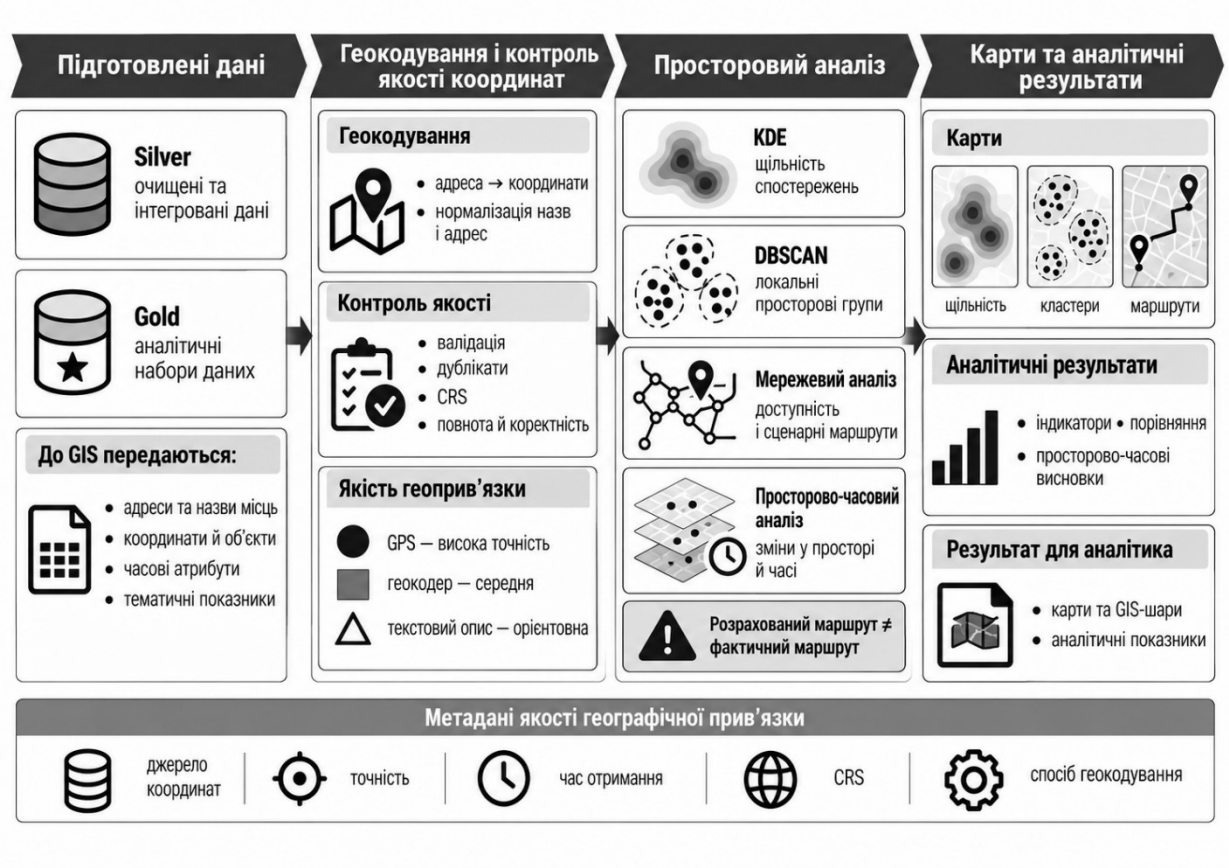


Рис. 5.4. Взаємодія Data Lakehouse та GIS: підготовлені дані → геокодування й контроль якості координат → просторовий аналіз → карти та аналітичні результати.

Перспективним є безпосередній зв'язок *GIS* із рівнями *Silver і Gold Data Lakehouse*. Після геокодування адрес, перевірки координат і нормалізації просторових даних вони можуть використовуватися для побудови карт щільності, кластерів, часових карт та інших просторових моделей.

Важливою умовою є збереження інформації про якість географічної прив'язки. Координати, отримані безпосередньо з *GPS*, адреси, автоматично перетворені геокодером, і приблизна локація, визначена з текстового опису, мають різний рівень точності та не повинні аналізуватися як рівнозначні.

5.2.4. Кіберзахист і стійкість платформи

Розширення аналітичних можливостей неминуче збільшує вимоги до інформаційної безпеки. Система, яка об'єднує значні обсяги даних і використовується декількома установами, сама стає критичним об'єктом захисту.

Захист мережевого периметра може включати *WAF, IDS/IPS* та інші засоби виявлення й блокування атак. На рівні користувачів доцільно застосовувати багатофакторну автентифікацію, *RBAC* або *ABAC* та принцип найменших необхідних привілеїв. Підхід *Zero Trust* передбачає, що сам факт перебування користувача або пристрою у внутрішній мережі не є достатньою підставою для довіри.

Дані під час передавання повинні захищатися сучасними криптографічними протоколами, а під час зберігання – шифруванням і належним керуванням ключами. Перспективним напрямом є забезпечення криптографічної гнучкості (*crypto-agility*), що дозволятиме надалі переходити на постквантові алгоритми у міру їх стандартизації та необхідності.

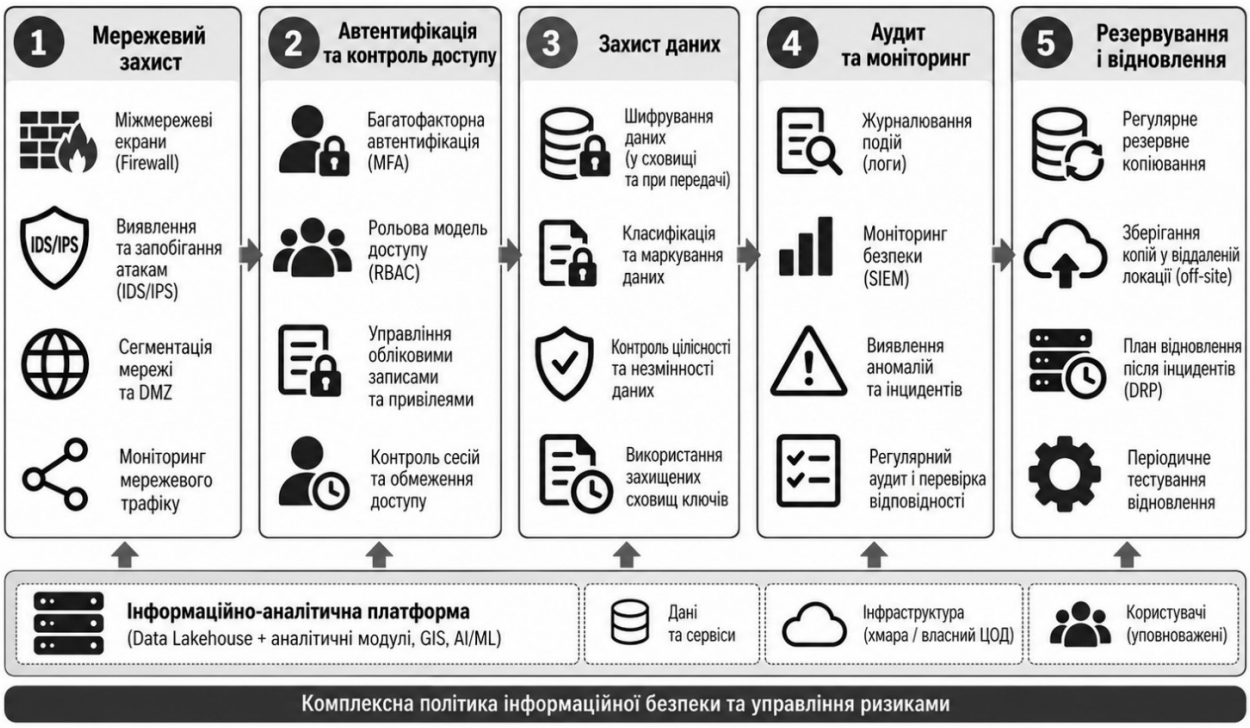


Рис. 5.5. Багаторівнева модель кіберзахисту аналітичної платформи: мережевий захист → автентифікація та контроль доступу → захист даних → аудит → резервування і відновлення.

Для збереження цілісності та простежуваності доцільно використовувати незмінювані журнали аудиту, криптографічне хешування та *WORM*-механізми там, де це виправдано характером даних. Застосування блокчейн-технологій не є обов’язковою умовою такого захисту.

Стійкість має забезпечуватися резервним копіюванням, географічним резервуванням критичних компонентів, планами відновлення після аварій та регулярною перевіркою працездатності резервних копій.

5.2.5. Інтероперабельність та API

Модульність системи передбачає використання програмних інтерфейсів для обміну даними між окремими компонентами. Внутрішні API можуть забезпечувати взаємодію Data Lakehouse, OSINT, GIS, графових та ML-модулів.

API повинні передавати не лише основні значення, а й метадані про джерело, час отримання, якість і рівень доступу до інформації. Це необхідно для того, щоб під час переходу між системами не втрачався контекст даних.

Для різних типів інформації можуть застосовуватися стандартні структуровані формати, зокрема JSON, GeoJSON або JSON-LD. Спеціалізовані стандарти на кшталт STIX 2.1 доцільні лише для тих категорій даних, для яких вони були розроблені, і не повинні використовуватися як універсальний формат усієї правоохоронної інформації.

Взаємодія з міжнародними інформаційними системами має здійснюватися через передбачені відповідними організаціями захищені механізми обміну. Наявність API у внутрішній платформі не означає автоматичної можливості прямого підключення до систем Interpol, Europol чи інших міжнародних структур.

Інтерфейси для Power BI, Grafana, Superset та інших BI-засобів можуть використовуватися для формування дашбордів і звітів, якщо це відповідає вимогам до захисту відповідної категорії даних.

5.2.6. Хмарні та контейнерні технології

Перспективним напрямом масштабування є використання гібридної інфраструктури, у якій державні або відомчі обчислювальні ресурси можуть поєднуватися з хмарними сервісами.

Використання публічної хмари не повинно розглядатися як універсальне рішення для всіх категорій інформації. Місце розміщення даних, модель хмарного сервісу та перелік допустимих операцій мають визначатися відповідно

до правового режиму інформації, вимог кібербезпеки та політики конкретного державного органу.

Контейнеризація за допомогою Docker та Kubernetes або функціонально аналогічних технологій може спростити розгортання окремих модулів, забезпечити кероване масштабування та ізоляцію сервісів. Це особливо корисно для архітектури, у якій OSINT, GIS, ETL, машинне навчання та візуалізація функціонують як окремі компоненти.

Serverless-підхід може використовуватися для короткочасних подієвих операцій, наприклад запуску окремої функції після надходження нового запису або формування технічного сповіщення. Водночас критичні аналітичні процеси повинні залишатися контрольованими, відтворюваними та придатними до аудиту незалежно від моделі розгортання.

5.2.7. Висновки

Технічний розвиток запропонованої системи доцільно будувати як поєднання кількох взаємозалежних рівнів: *Data Lakehouse забезпечує інтеграцію й підготовку інформації; AI/ML – автоматизований пошук закономірностей і нетипових спостережень; GIS – просторову інтерпретацію; API – взаємодію компонентів; кіберзахист – конфіденційність, цілісність, доступність і простежуваність даних.*

Перспективність такої архітектури визначається не кількістю впроваджених технологій, а можливістю їх контрольованої взаємодії. Кожен компонент повинен мати визначене призначення, джерела даних, правила доступу, процедури перевірки результатів та механізми аудиту.

Подальший розвиток має здійснюватися модульно: від апробації окремих сервісів до їх інтеграції у міжвідомчий аналітичний контур. Це дозволяє перевіряти масштабованість, надійність і безпеку до переходу на ширший рівень використання та уникати ситуації, коли технічна складність системи випереджає її організаційну й правову готовність.

5.3. Організаційні аспекти впровадження

Технічна готовність інформаційно-аналітичної платформи сама по собі не забезпечує її практичного застосування. Результативність системи залежить від чіткого розподілу повноважень, узгоджених процедур обміну даними, підготовки персоналу та визначення відповідальності за використання аналітичних результатів.

5.3.1. Міжвідомча координація

Протидія торгівлі людьми потребує взаємодії органів, які працюють із різними видами інформації: правоохоронними, прикордонними, фінансовими, кібербезпековими та соціальними даними. Тому доцільно передбачити *міжвідомчий координаційний механізм***,** який забезпечуватиме узгоджені правила інформаційного обміну без необґрунтованого дублювання баз даних і функцій.

Національна поліція може використовувати результати OSINT, графового та просторового аналізу в межах своїх повноважень; ДПСУ – зіставляти просторово-часові індикатори з власними даними; Держфінмоніторинг – аналізувати фінансові ознаки відповідно до встановлених процедур. Інші компетентні органи залучаються в межах визначених законом функцій. Обмін повинен стосуватися лише інформації, необхідної для конкретного завдання.

5.3.2. Розподіл ролей і відповідальності

Організаційна модель має чітко розмежовувати адміністрування системи, аналітичну роботу, технічне обслуговування та прийняття рішень. Адміністратор забезпечує функціонування платформи, контроль доступу й журналювання; аналітичні підрозділи формують запити, перевіряють результати та готують аналітичні матеріали; технічні фахівці відповідають за працездатність і кіберзахист інфраструктури.

Принциповим є те, що *аналітична платформа підтримує діяльність уповноважених посадових осіб, але не перебирає на себе їхні повноваження***.** Алгоритмічна оцінка, кластер або сигнал аномалії повинні проходити перевірку людиною перед подальшим використанням.

5.3.3. Кадрове забезпечення

Практичне впровадження потребує фахівців, які поєднують компетентності у сфері аналізу даних, OSINT, GIS, інформаційної безпеки та правових основ роботи з інформацією. До необхідних навичок належать робота з базами даних і мовами аналітичної обробки, використання GIS та графових інструментів, перевірка відкритих джерел і критична інтерпретація результатів AI/ML-моделей.

Підготовка такого фахівця повинна бути орієнтована не лише на володіння програмними засобами, а й на розуміння обмежень автоматизованої аналітики, правил роботи з персональними даними та необхідності експертної перевірки отриманих результатів.

5.3.4. Правові та етичні умови

Доступ до даних має визначатися службовими повноваженнями та принципом мінімально необхідного доступу. Система повинна забезпечувати розмежування ролей, журналювання операцій, захист персональних даних і можливість встановити, хто та з якою інформацією працював.

Окремої уваги потребує ризик помилкової алгоритмічної оцінки. Результати машинного навчання повинні бути достатньо пояснюваними для перевірки аналітиком, а автоматизовані моделі не можуть самостійно визначати правовий статус людини або її причетність до протиправної діяльності.

5.3.5. Очікуваний результат організаційного впровадження

Організаційна інтеграція має забезпечити не створення єдиної безмежної бази даних, а *керований міжвідомчий обмін інформацією та аналітичними результатами.* Це дозволяє зменшити дублювання операцій, прискорити перевірку міжвідомчих запитів, забезпечити простежуваність використання даних і сформувати узгоджений порядок роботи з результатами OSINT, GIS, Big Data та ML.

Таким чином, організаційна модель повинна ґрунтуватися на *розмежуванні компетенцій, мінімально необхідному доступі до даних, персональній відповідальності користувачів та обов'язковій експертній*

перевірці алгоритмічних результатів. Це створює умови для практичного використання аналітичної платформи без надмірної централізації даних і підміни професійних рішень автоматизованими оцінками.

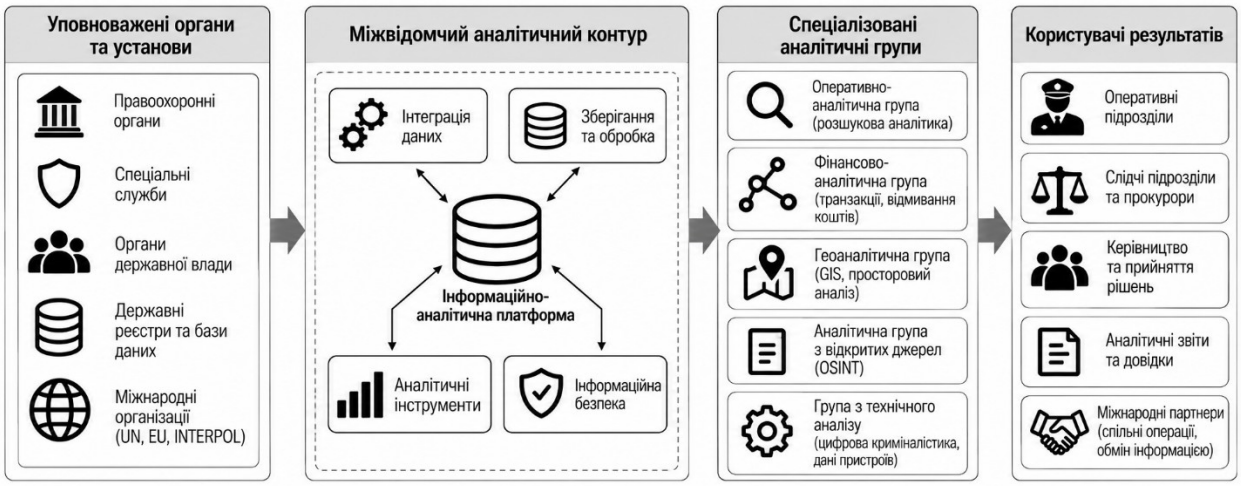


Рис. 5.6. Організаційна модель міжвідомчої взаємодії: уповноважені органи → міжвідомчий аналітичний контур → спеціалізовані аналітичні групи → користувачі результатів.

5.4. Міжнародна співпраця та інтеграція

5.4.1. Необхідність міжнародної інтеграції

Торгівля людьми часто має транскордонний характер: окремі етапи вербування, переміщення, експлуатації, фінансових розрахунків і цифрової комунікації можуть відбуватися у різних державах. Відповідні цифрові сліди також розподіляються між різними юрисдикціями та інформаційними системами. За таких умов ефективність національної аналітики залежить від можливості своєчасно отримувати, перевіряти та зіставляти інформацію з міжнародними партнерами.

Міжнародна інтеграція повинна розглядатися не як створення необмеженого транскордонного доступу до даних, а як **контрольований обмін визначеним обсягом інформації** через установлені правові та правоохоронні механізми. Особливого значення набувають уніфікація опису інформаційних об’єктів, захист персональних даних, фіксація походження інформації та збереження можливості її перевірки.

5.4.2. Основні напрями міжнародної співпраці

Важливими партнерами України у протидії транснаціональній злочинності є **Europol, Interpol та UNODC**. Europol забезпечує європейську правоохоронну взаємодію та захищений інформаційний обмін, зокрема через SIENA. Interpol забезпечує глобальну правоохоронну комунікацію через мережу I-24/7 і доступ до спеціалізованих міжнародних інформаційних ресурсів. UNODC виконує передусім нормативно-методичну, аналітичну та координаційну функції у сфері протидії транснаціональній організованій злочинності та торгівлі людьми.

Окремим напрямом є фінансова взаємодія між компетентними органами та підрозділами фінансової розвідки. Її значення полягає у можливості зіставляти транскордонні фінансові індикатори з іншими відомостями за умови належних правових підстав та дотримання режиму доступу.

5.4.3. Технічні принципи інтеграції

Міжнародний обмін потребує стандартизованого представлення даних і метаданих. Для окремих категорій інформації можуть застосовуватися JSON, JSON-LD, GeoJSON та спеціалізовані формати. STIX/TAXII доцільно використовувати у тих випадках, коли йдеться про структурований обмін інформацією про кіберзагрози та відповідні індикатори, а не як універсальний формат усіх матеріалів правоохоронної діяльності.

Технічна інтероперабельність має забезпечуватися захищеними каналами, автентифікацією користувачів, рольовим розмежуванням доступу та журналюванням операцій. Водночас взаємодія з Europol, Interpol чи іншими структурами повинна здійснюватися через доступні Україні офіційні механізми співробітництва. Наявність внутрішнього API національної платформи не означає автоматичної можливості прямого підключення до міжнародних інформаційних систем.

Багатомовні NLP-моделі можуть додатково використовуватися для перекладу, семантичного пошуку та порівняння текстових матеріалів різними мовами. Їх результати повинні перевірятися фахівцем, особливо коли від точності перекладу залежить зміст аналітичного висновку.

5.4.4. Очікуваний ефект

Практична цінність міжнародної інтеграції полягає у можливості зіставляти інформацію, яка в межах однієї держави виглядає фрагментарною. Повторюваний контакт, цифровий ідентифікатор, фінансова операція або пов’язаний обліковий запис можуть набувати додаткового аналітичного значення після порівняння з інформацією іншої юрисдикції.

Стандартизація обміну також зменшує втрату контексту та полегшує використання матеріалів різними компетентними органами. При цьому технічна сумісність формату не визначає процесуальної допустимості інформації: її правовий статус залежить від способу отримання, документування та вимог відповідного законодавства.

5.4.5. Модель міжнародної інтеграції

Для запропонованої інформаційно-аналітичної платформи доцільною є модель, у якій міжнародний рівень є зовнішнім контуром національної системи. Аналітичні результати спочатку формуються та перевіряються уповноваженими українськими органами, після чого визначений обсяг інформації може передаватися міжнародному партнеру через передбачений механізм співробітництва.

Зворотний інформаційний потік будується аналогічно: отримані від партнерів відомості інтегруються до відповідного аналітичного контексту лише після перевірки їх походження, правового режиму та можливості використання.

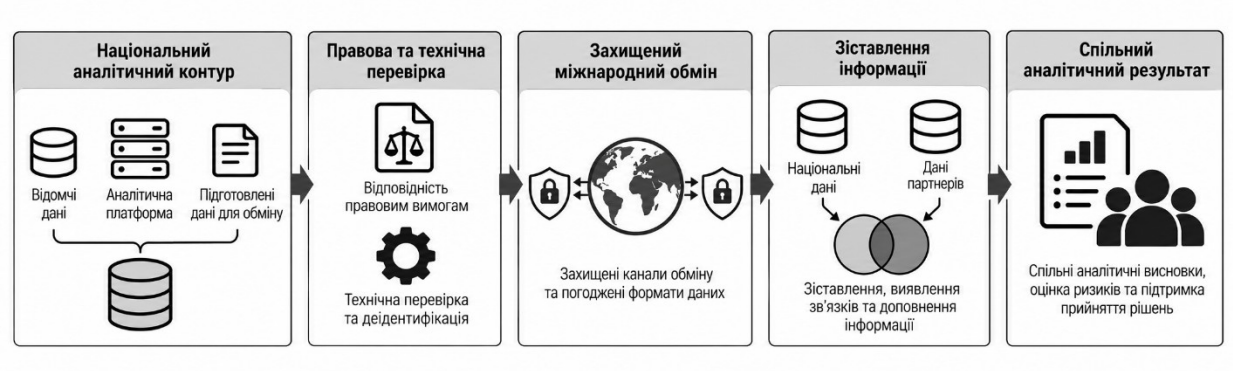


Рис. 5.7. Модель міжнародної інтеграції аналітичної платформи.

Таким чином, міжнародна інтеграція має забезпечувати Такий підхід дозволяє доповнювати національну аналітику транскордонним контекстом, не порушуючи принципів компетенції, пропорційності та захисту персональних даних.

5.5. Перспективи для науки та освіти

Розвиток інформаційно-аналітичних технологій у сфері протидії торгівлі людьми потребує відповідного кадрового та наукового забезпечення. Практичне використання OSINT, GIS, Big Data, машинного навчання та цифрової криміналістики вимагає від фахівця не лише технічних навичок, а й розуміння правових обмежень, принципів захисту персональних даних та особливостей роботи з чутливою інформацією.

5.5.1. Формування професійних компетентностей

Підготовка аналітиків для правоохоронної та безпекової сфери має мати міждисциплінарний характер. До основних компетентностей належать робота з базами даних і засобами програмного аналізу, використання GIS, OSINT та графових моделей, розуміння принципів машинного навчання, а також здатність перевіряти походження, якість і достовірність інформації.

Не менш важливими є знання кримінального процесу, правил поводження з цифровими матеріалами, захисту персональних даних і принципів людиноцентричного використання аналітичних технологій. Технічний результат повинен оцінюватися критично: алгоритмічний сигнал, кластер або аномалія не можуть автоматично перетворюватися на висновок щодо конкретної особи.

5.5.2. Освітня складова

Перспективним є включення до освітніх програм з інформаційних технологій і правоохоронної діяльності навчальних компонентів із OSINT, GIS, кримінальної аналітики, цифрової криміналістики, аналізу даних та застосування AI/ML у безпековій сфері. Окремий напрям становлять програми підвищення кваліфікації для працівників правоохоронних та інших уповноважених органів.

Практична підготовка має здійснюватися переважно на **синтетичних, модельних або належним чином анонімізованих даних**. Це дозволяє відпрацьовувати повний цикл аналітичної роботи – від отримання та перевірки інформації до її просторового, графового й алгоритмічного аналізу – без необґрунтованого використання персональних даних реальних постраждалих осіб.

5.5.3. Перспективні напрями наукових досліджень

Науковий розвиток доцільно спрямувати на міждисциплінарні дослідження, що поєднують інформаційні технології, кримінальну аналітику, GIS, цифрову криміналістику та захист прав людини. Перспективними є дослідження методів виявлення аномалій, аналізу великих графів, просторово-часових закономірностей, автоматизованої обробки відкритих джерел та оцінювання пояснюваності AI-моделей.

Особливого значення набуває оцінювання не лише точності алгоритмів, а й частоти хибнопозитивних і хибнонегативних результатів, стійкості моделей до зміни даних та можливості експертної перевірки висновків. Для досліджень і навчання доцільно формувати верифіковані анонімізовані або синтетичні набори даних із чітко задокументованим походженням і структурою.

5.5.4. Очікуваний результат

Поєднання освіти, практичної підготовки та прикладних досліджень має сприяти формуванню фахівців, здатних працювати на межі інформаційних технологій і правоохоронної аналітики. Йдеться не про створення окремої універсальної професії, а про розвиток компетентностей аналітиків, цифрових криміналістів, GIS-фахівців та спеціалістів із даних, які можуть ефективно працювати у міждисциплінарних командах.



Рис. 5.8. Модель підготовки фахівців з інформаційно-аналітичного забезпечення.

Науково-освітнє середовище при цьому виконує подвійну функцію: забезпечує підготовку кадрів для практичного застосування технологій та створює умови для незалежної перевірки й удосконалення аналітичних методів.

Таким чином, розвиток кадрового й наукового потенціалу є необхідною умовою сталого впровадження запропонованої інформаційно-аналітичної системи. Технології можуть підвищувати швидкість і масштаб аналітичної роботи, однак якість кінцевого результату визначатиметься насамперед *компетентністю фахівця, якістю даних, критичною перевіркою алгоритмічних результатів та дотриманням прав людини.*

5.6. Етичні та правові аспекти розвитку платформи

Ефективність інформаційно-аналітичної платформи визначається не лише її технічними можливостями, а й правомірністю оброблення даних, прозорістю алгоритмічних процедур та здатністю мінімізувати ризики для прав людини. У сфері протидії торгівлі людьми це має особливе значення через оброблення персональних, комунікаційних, просторових та інших чутливих даних.

5.6.1. Правові основи

Збирання, зберігання, аналіз і передавання інформації повинні здійснюватися відповідно до законодавства України, зокрема вимог щодо захисту персональних даних, інформаційної безпеки та повноважень відповідних державних органів. Для міжнародного обміну додатково враховуються правові режими та стандарти сторін, між якими здійснюється передавання інформації.

Наявність даних у відкритому доступі не означає необмеженої можливості їх накопичення та подальшого використання. Оброблення має відповідати визначеній законній меті, бути необхідним і пропорційним, а для інформації обмеженого доступу – ґрунтуватися на відповідних повноваженнях.

5.6.2. Основні етичні ризики

Ключовими ризиками є надмірне збирання персональних даних, помилкові алгоритмічні оцінки, упередженість моделей та непропорційне використання засобів моніторингу. Особливо небезпечним є автоматичне перенесення алгоритмічного результату на оцінку конкретної людини. Аномалія, кластер або високий показник ризику є лише аналітичним сигналом і не визначає причетності особи до протиправної діяльності.

Тому робота платформи повинна будуватися за принципом *Human-in-the-Loop:* алгоритм допомагає знайти та структурувати інформацію, а змістовна перевірка і прийняття рішення залишаються за уповноваженим фахівцем.

5.6.3. Практичні механізми захисту

Основою відповідального використання даних має бути система *Data Governance,* яка визначає правила отримання, зберігання, використання, передавання та видалення інформації. Для зменшення ризиків доцільно застосовувати мінімізацію даних, псевдонімізацію або анонімізацію, рольове та атрибутне розмежування доступу (RBAC/ABAC), журналювання дій користувачів і регулярний аудит.

Для AI/ML-модулів необхідно забезпечити можливість перевірки того, які дані та ознаки вплинули на результат. Explainable AI у цьому випадку виконує функцію підтримки прозорості й контролю, але не замінює експертної оцінки.

5.6.4. Баланс ефективності та прав людини

Розширення можливостей OSINT, Big Data, GIS та ML не повинно автоматично означати збільшення обсягу даних, що збираються про громадян. Принциповим є підхід, за якого кожен додатковий вид інформації або аналітична процедура мають бути обґрунтовані конкретною метою та очікуваною користю.

Тому баланс між ефективністю та правами людини забезпечується не зменшенням функціональності системи, а *обмеженням надмірного втручання*: мінімізацією даних, розмежуванням доступу, експертною перевіркою, прозорістю алгоритмів і можливістю аудиту.

5.6.5. Багаторівнева модель Data Governance

Для запропонованої платформи доцільною є багаторівнева модель Data Governance, що об'єднує *правовий, етичний, технічний та організаційний рівні.* Правовий рівень визначає допустимі межі роботи з інформацією; етичний – принципи пропорційності, недискримінації та захисту людини; технічний – засоби контролю доступу, шифрування, журналювання та захисту даних; організаційний – розподіл відповідальності, аудит і підготовку персоналу.

Ці рівні повинні функціонувати як єдина система. Правові та етичні вимоги визначають обмеження для технологій, технічні засоби забезпечують їх практичне виконання, а організаційні процедури підтримують постійний контроль і відповідальність.

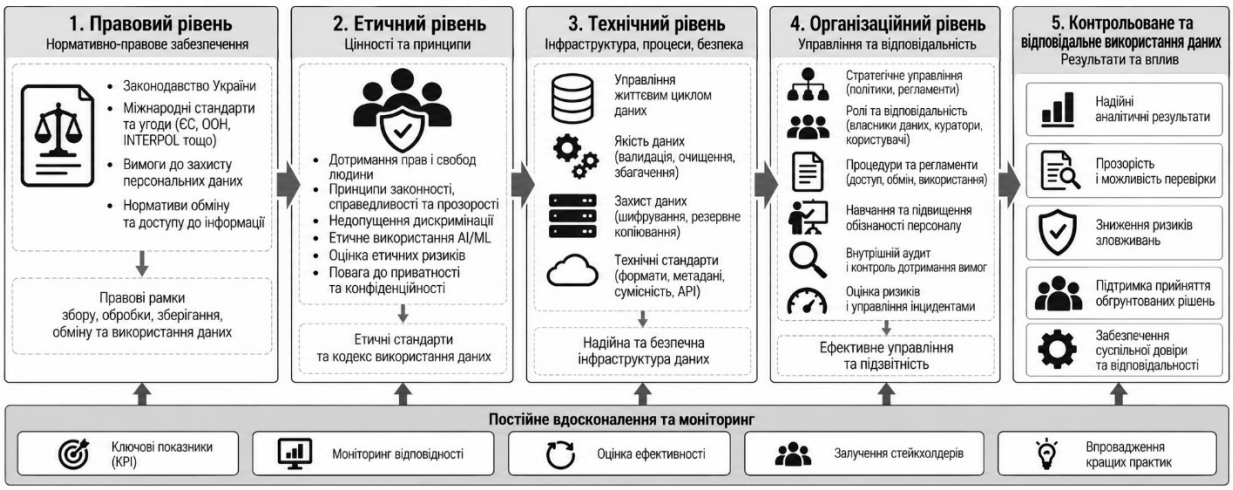


Рис. 5.9. Багаторівнева модель Data Governance аналітичної платформи: правовий рівень → етичний рівень → технічний рівень → організаційний рівень → контрольоване та відповідальне використання даних.

Таким чином, етична та правова стійкість платформи має забезпечуватися ще на етапі її проєктування. Принципи *privacy by design, data minimization, Human-in-the-Loop, Explainable AI, контроль доступу та простежуваність*

операцій повинні бути вбудованими характеристиками системи. Це дозволяє поєднати аналітичну ефективність із захистом приватності, гідності та інших прав людини.

Висновки до розділу 5

Перспективи розвитку інформаційно-аналітичного забезпечення протидії торгівлі людьми визначаються не стільки впровадженням окремих цифрових інструментів, скільки здатністю об'єднати технологічні, організаційні, правові, кадрові та міжнародні компоненти в узгоджену систему. Результати дослідження свідчать, що перехід від експериментальних *OSINT-, GIS-, Big Data- та ML*-рішень до практичного використання має здійснюватися поетапно, із перевіркою їх функціональності, безпеки, правомірності та сумісності з наявними інформаційними процесами державних органів.

Оптимальною видається не модель необмеженого централізованого накопичення інформації, а *керований міжвідомчий аналітичний контур***,** у якому первинні дані можуть залишатися під контролем відповідних установ, а для спільного аналізу передаються лише необхідні відомості та аналітичні результати. Такий підхід дозволяє поєднати потребу у комплексному аналізі з принципами розмежування повноважень, мінімізації даних і персональної відповідальності за їх використання.

Технологічною основою такого контуру може бути модульна *Data Lakehouse*-архітектура, пов'язана з *GIS, OSINT*, графовим аналізом, засобами машинного навчання та візуалізації. Її практична цінність полягає у забезпеченні простежуваного переходу від первинних даних до аналітичного результату. Водночас автоматизація повинна виконувати функції структурування, пошуку закономірностей і пріоритизації інформації, а не підміняти професійну оцінку. Тому принцип *Human-in-the-Loop* є необхідною складовою використання AI/ML у правоохоронній аналітиці.

Подальше масштабування системи безпосередньо залежить від її кіберстійкості. Розмежування доступу, шифрування, журналювання операцій, резервування, контроль цілісності та можливість відновлення після інцидентів

мають бути закладені в архітектуру платформи від початку. Не менш важливою є простежуваність усіх операцій із даними, оскільки саме вона забезпечує можливість перевірити походження інформації, послідовність її оброблення та обґрунтованість сформованого результату.

Міжнародний характер торгівлі людьми робить зовнішній інформаційний обмін необхідним компонентом системи. Проте міжнародна інтеграція повинна розумітися не як прямий доступ до зовнішніх баз даних, а як використання встановлених механізмів співробітництва, захищених каналів та узгоджених форматів обміну. Це дозволяє доповнювати національну аналітику транскордонним контекстом без втрати контролю за походженням, правовим режимом і подальшим використанням інформації.

Стійкість запропонованої моделі значною мірою залежить від кадрового та наукового забезпечення. Фахівець, який працює з такими системами, повинен поєднувати навички роботи з даними, GIS, OSINT, цифровою криміналістикою та AI/ML із розумінням правових обмежень і ризиків алгоритмічної помилки. Тому розвиток освітніх програм, практичних навчальних середовищ і прикладних досліджень є не допоміжним, а системоутворювальним елементом подальшого впровадження.

Ключовою умовою функціонування всієї моделі є *Data Governance*, що поєднує правовий, етичний, технічний та організаційний рівні. Законність оброблення, пропорційність, мінімізація даних, пояснюваність алгоритмів, захист постраждалих осіб, розмежування доступу та аудит мають діяти як взаємопов’язані механізми. Це дозволяє уникнути ситуації, коли підвищення технічних можливостей системи супроводжується необґрунтованим розширенням контролю або ризиком порушення прав людини.

Отже, подальший розвиток запропонованого підходу доцільно здійснювати як *поетапне формування модульної, міжвідомчої та контрольованої інформаційно-аналітичної системи*, у якій технології підтримують роботу фахівця, а не замінюють її. Її результативність визначатиметься не лише швидкістю оброблення даних або складністю

алгоритмів, а здатністю забезпечити одночасно аналітичну корисність, перевірюваність результатів, кіберстійкість, міжнародну взаємодію та належний захист прав і безпеки людини.

РОЗДІЛ 6. КРИМІНОЛОГІЧНИЙ АНАЛІЗ ТА МОДЕЛЮВАННЯ РИЗИКІВ ТОРГІВЛІ ЛЮДЬМИ В ЦИФРОВОМУ СЕРЕДОВИЩІ

6.1. Кримінологічна характеристика сучасної торгівлі людьми

Торгівля людьми належить до найбільш небезпечних форм організованої злочинної діяльності, оскільки посягає на особисту свободу, гідність, фізичну та психічну недоторканність людини, а в окремих випадках – на її життя і здоров'я. Специфіка цього кримінального явища полягає в тому, що людина стає об'єктом злочинної діяльності, спрямованої на отримання матеріальної або іншої вигоди шляхом її вербування, переміщення, переховування, передачі або одержання з метою подальшої експлуатації.

Відповідно до Закону України «Про протидію торгівлі людьми» торгівля людьми охоплює здійснення незаконної угоди, об'єктом якої є людина, а також вербування, переміщення, переховування, передачу або одержання людини, вчинені з метою експлуатації із використанням обману, шахрайства, шантажу, уразливого стану людини, насильства, службового становища, матеріальної чи іншої залежності [6]. Кримінально-правова характеристика відповідного діяння закріплена у ст. 149 Кримінального кодексу України, яка передбачає відповідальність за торгівлю людиною, а також за вербування, переміщення, переховування, передачу або одержання людини з метою експлуатації із застосуванням передбачених законом способів впливу [2].

Міжнародно–правове розуміння торгівлі людьми сформульовано у «Протоколі про запобігання і припинення торгівлі людьми, особливо жінками і дітьми, та покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності». Відповідно до ст. 3 Протоколу торгівля людьми включає вербування, перевезення, передачу, переховування або одержання осіб із використанням певних способів впливу з метою експлуатації; при цьому експлуатація охоплює, щонайменше, сексуальну експлуатацію, примусову працю або послуги, рабство та подібні до рабства практики,

підневільний стан і вилучення органів [1]. Європейський підхід до протидії цьому явищу додатково закріплено у «Конвенції Ради Європи про заходи щодо протидії торгівлі людьми», яка орієнтує держави не лише на кримінальне переслідування, а й на запобігання торгівлі людьми та захист її жертв [59].

З кримінологічної точки зору торгівля людьми не є однорідним злочинним явищем, що реалізується за єдиною схемою. Її сучасна специфіка визначається різноманітністю форм експлуатації, гнучкістю злочинних моделей, використанням економічної та соціальної вразливості потерпілих, мобільністю злочинців і потерпілих, транснаціональним характером окремих злочинних мереж, а також дедалі ширшим використанням інформаційно-комунікаційних технологій.

Водночас офіційно зареєстровані показники не можуть розглядатися як точний показник фактичного масштабу торгівлі людьми. Виявлення залежить від ефективності правоохоронних органів, механізмів ідентифікації потерпілих, готовності самих потерпілих повідомляти про злочини та інших факторів. Тому статистичні дані міжнародних організацій характеризують передусім виявлену частину явища.

За даними «Глобального звіту Управління ООН з наркотиків і злочинності про торгівлю людьми за 2024 рік», підготовленого на основі інформації зі 156 держав та аналізу виявлених випадків за 2020–2023 рр., у досліджуваному масиві було зафіксовано 202 478 потерпілих. Серед них 62 % становили дорослі та 38 % – діти. За встановленими цілями експлуатації 42 % виявлених потерпілих припадали на примусову працю, 36 % – на сексуальну експлуатацію, 8 % – на примусову злочинну діяльність, 8 % – на змішані форми експлуатації; інші категорії становили меншу частку [60]. Наведені показники слід інтерпретувати саме як характеристики виявлених випадків, а не як оцінку фактичної глобальної структури торгівлі людьми.

6.1.1. Основні форми та способи вчинення торгівлі людьми

Форми сучасної торгівлі людьми доцільно розглядати передусім крізь призму мети експлуатації. Міжнародні документи виділяють сексуальну

експлуатацію, примусову працю або послуги, рабство та подібні до рабства практики, підневільний стан, вилучення органів та інші форми експлуатаційного використання людини [61; 62].

Однією з найбільш поширених форм залишається сексуальна експлуатація. Її механізм може передбачати вербування особи під приводом працевлаштування, модельної діяльності, туристичних послуг, особистих стосунків або іншої діяльності з подальшим примушуванням до надання сексуальних послуг. У сучасних умовах частина комунікації між злочинцем і потенційною жертвою переноситься у цифрове середовище, що дозволяє встановлювати первинний контакт без безпосередньої фізичної взаємодії [64].

Значне місце посідає трудова експлуатація. Вона може реалізовуватися у сільському господарстві, будівництві, виробництві, сфері побутових послуг, домашній праці, логістиці та інших секторах. Особливістю такої моделі є те, що злочинна діяльність нерідко маскується під звичайні трудові відносини. Потенційному потерпілому пропонують працевлаштування, заробітну плату та прийнятні умови проживання, однак після його прибуття до місця роботи відбувається зміна домовленостей, обмеження свободи пересування, контроль над документами або доходами, застосування погроз, насильства чи інших форм примусу.

Окремого значення набуває торгівля людьми з метою примусової злочинної діяльності. У Глобальному звіті UNODC 2024 року така форма становила 8 % серед виявлених потерпілих у досліджуваному масиві [60]. Йдеться про ситуації, коли особу експлуатують шляхом примушування до вчинення кримінальних правопорушень для отримання доходу торговцями або іншими експлуататорами. Зростання значення цієї моделі пов’язане, зокрема, із розвитком цифрових шахрайських операцій та інших видів злочинної діяльності, що можуть здійснюватися дистанційно.

До інших форм експлуатації належать примусове жебрацтво, примусовий шлюб та змішані форми експлуатації. За даними UNODC, у глобальному масиві виявлених випадків 2020–2023 рр. частка потерпілих від примусового жебрацтва

становила 1 %, а від примусових шлюбів – також 1 % [60]. Водночас низькі показники окремих категорій не означають відсутності відповідних форм злочинної діяльності, оскільки вони можуть характеризуватися значною латентністю та неоднаковою практикою їх виявлення у різних державах.

Способи вчинення торгівлі людьми охоплюють обман, шахрайство, шантаж, погрози, фізичне та психологічне насильство, використання уразливого стану, матеріальної або іншої залежності та інші форми впливу, визначені кримінальним законодавством [1; 2]. Важливою тенденцією є поєднання кількох способів впливу на потерпілого. Наприклад, первинний обман може надалі доповнюватися психологічним тиском, позбавленням доступу до коштів і документів, погрозами або насильством.

Сучасні моделі характеризуються також поступовим переходом від переважно фізичного примусу до складніших механізмів контролю. Злочинці можуть створювати фінансову залежність, формувати боргові зобов'язання, ізолювати потерпілого від соціального оточення, погрожувати розголошенням персональної інформації або використовувати залежність, пов'язану з міграційним чи соціальним статусом особи.

Таким чином, сучасна торгівля людьми характеризується не відмовою від традиційних способів примусу, а їх комбінуванням із соціально–психологічними, економічними та технологічними механізмами впливу.

6.1.2. Суб'єкти та структура злочинної діяльності

Суб'єктний склад торгівлі людьми може бути як відносно простим, так і складним. В окремому випадку одна особа може одночасно здійснювати пошук потенційної жертви, її вербування та подальшу експлуатацію. В інших випадках між кількома учасниками розподіляються функції щодо вербування, переміщення, забезпечення документами та транспортом, безпосередньої експлуатації, фінансового обслуговування та приховування злочинної діяльності.

За даними UNODC, у глобальному масиві, проаналізованому для Глобального звіту 2024 року, 70 % торговців людьми діяли в межах

організованих груп із бізнесовою або управлінською структурою, тоді як 28 % діяли індивідуально або у взаємодії з іншими особами без встановлення такої організованої структури [60]. Наведені показники свідчать про значну роль організованих форм злочинної діяльності, але одночасно підтверджують, що торгівля людьми не завжди здійснюється великими ієрархічно побудованими злочинними організаціями.

Функціональна структура злочинної діяльності може передбачати наявність вербувальників, посередників, осіб, відповідальних за переміщення та логістику, безпосередніх експлуататорів, фінансових посередників та інших учасників. При цьому такий розподіл не є універсальним: одна особа може виконувати декілька функцій, а окремі учасники можуть залучатися лише на певному етапі злочинної діяльності.

Особливістю сучасних мереж є їхня гнучкість. Замість постійної вертикальної структури може функціонувати мережа контактів, у межах якої окремі особи залучаються для виконання конкретних завдань. Такий характер взаємодії ускладнює встановлення всіх учасників злочинної діяльності та доказування зв’язків між ними.

Окремого значення набувають фінансові механізми забезпечення злочинної діяльності. Отримані від експлуатації кошти можуть переміщуватися через різні рахунки, платіжні сервіси та інші фінансові інструменти. У сучасних умовах додаткові ризики пов’язані з використанням віртуальних активів та інших цифрових фінансових інструментів, що здатні полегшувати транскордонне переміщення коштів [62].

Водночас дослідження UNODC щодо організованої злочинності в Україні в умовах війни показує, що торгівля людьми в Україні не зводиться до діяльності великих централізованих злочинних організацій. У дослідженні зафіксовано, зокрема, моделі експлуатації внутрішньо переміщених осіб, що виникають на тлі їхньої підвищеної уразливості [62].

Отже, структура сучасної злочинної діяльності у сфері торгівлі людьми має гібридний характер і може поєднувати традиційні міжособистісні зв’язки,

організовані злочинні групи, тимчасових посередників, легальні комерційні структури та цифрову інфраструктуру.

6.1.3. Типові моделі вербування, переміщення та експлуатації

Механізм торгівлі людьми доцільно розглядати як сукупність взаємопов'язаних дій, спрямованих на виявлення потенційної жертви, встановлення контакту, її вербування, переміщення або передачу, встановлення контролю та подальшу експлуатацію.

На етапі вербування злочинці використовують різні способи формування мотивації потенційної жертви. Найбільш поширеною є пропозиція роботи або іншої діяльності, яка не відповідає реальним умовам. Також можуть використовуватися пропозиції допомоги, навчання, проживання, особистих стосунків або іншої соціально привабливої взаємодії. Важливим фактором є використання уразливого стану людини, який відповідно до міжнародного та національного законодавства може бути одним із засобів вчинення торгівлі людьми [1–3].

Особливого значення в сучасних умовах набуває цифрове вербування. Злочинці можуть використовувати соціальні мережі, сайти пошуку роботи, месенджери, платформи знайомств та інші цифрові ресурси. ОБСЄ зазначає, що соціальні мережі використовуються для аналізу інформації, яку потенційні потерпілі публікують про себе, виявлення ознак уразливості, формування довіри, створення псевдоінтимних відносин і подальшого обману або психологічного контролю [6].

Окремим різновидом є використання неправдивих вакансій. У такому випадку злочинці можуть створювати оголошення про роботу, що не відповідають фактичним умовам, або маскувати шахрайську пропозицію під діяльність реально існуючої компанії. Цифрове середовище дає змогу швидко поширювати такі оголошення серед значної кількості потенційних жертв [5; 6].

Переміщення потерпілих може бути внутрішнім або транскордонним. Водночас фізичне переміщення не є необхідною умовою існування кожної сучасної моделі торгівлі людьми. Експлуатація може здійснюватися за

відсутності значного територіального переміщення, а окремі елементи злочинної діяльності – зокрема вербування, координація, контроль та фінансове забезпечення – можуть здійснюватися дистанційно.

Після потрапляння потерпілого у середовище експлуатації можуть застосовуватися фізичне насильство, погрози, шантаж, обмеження доступу до коштів і документів, ізоляція, психологічний тиск, створення боргової залежності та інші форми контролю [59–61].

Важливим є розмежування первинної згоди особи та реальних умов її подальшого перебування. Згода особи на працевлаштування, поїздку або іншу діяльність не виключає можливості торгівлі людьми, якщо для її залучення або подальшої експлуатації були використані передбачені законом способи впливу. Особливий підхід застосовується до дітей: відповідно до міжнародного визначення торгівлі дітьми використання таких засобів впливу для встановлення факту торгівлі не є необхідним [1].

Для України особливого значення набувають моделі, пов’язані з вимушеним переміщенням населення. Дослідження UNODC 2025 року, присвячене динаміці організованої злочинності в Україні в умовах війни, містить окремий розділ про торгівлю людьми та наводить, зокрема, випадок експлуатації внутрішньо переміщених осіб у Львівській області. У дослідженні також розглядається проблема вербування дітей у контексті збройного конфлікту [62].

Отже, типова модель торгівлі людьми може бути представлена як послідовність «уразливість – встановлення контакту – вербування – переміщення або передача – встановлення контролю – експлуатація», однак на практиці окремі етапи можуть поєднуватися, змінювати порядок або реалізовуватися паралельно.

6.1.4. Транснаціональний характер злочинних мереж

Торгівля людьми має значний транснаціональний потенціал. У межах однієї злочинної схеми можуть взаємодіяти особи, які перебувають у різних державах, а країна походження потерпілого, країна його транзиту та країна експлуатації можуть не збігатися. Саме транснаціональний характер є однією з

причин включення «Протоколу про торгівлю людьми» до системи міжнародно–правових інструментів, що доповнюють Конвенцію ООН проти транснаціональної організованої злочинності [1].

Транскордонний характер діяльності створює для злочинців додаткові можливості приховування слідів злочину, використання відмінностей у законодавстві різних держав, ускладнення доступу правоохоронних органів до доказів та переміщення незаконних доходів.

Для потерпілої особи перетин державного кордону може посилювати залежність від експлуататора через незнання мови, відсутність соціальних контактів, невизначеність правового статусу, відсутність документів та страх перед державними органами.

Разом із тим транснаціональний характер не слід ототожнювати виключно з фізичним переміщенням потерпілих через державний кордон. Сучасні цифрові технології дозволяють організаторам, вербувальникам, посередникам та експлуататорам перебувати в різних юрисдикціях і координувати злочинну діяльність дистанційно [61; 63].

Таким чином, окремі елементи злочинної діяльності можуть бути географічно розосереджені: потенційних потерпілих знаходять в одній державі, вербування здійснюється з іншої, експлуатація організовується у третій, а фінансові операції проходять через декілька юрисдикцій.

Для України ця проблема набула особливої гостроти після початку повномасштабної збройної агресії російської федерації. Масове вимушене переміщення населення створило нові умови для злочинної експлуатації осіб, які опинилися у залежному або вразливому становищі. Дослідження UNODC щодо організованої злочинності в Україні в умовах війни прямо розглядає торгівлю людьми як один із напрямів злочинної діяльності, що адаптується до умов воєнного часу [62].

Транснаціональна структура сучасних мереж дедалі більше доповнюється цифровим виміром. Інтернет і цифрові платформи дають можливість здійснювати вербування в одній країні, координувати переміщення з іншої,

організовувати експлуатацію у третій та одночасно управляти фінансовими потоками через декілька юрисдикцій [61; 63].

Саме тому протидія транснаціональній торгівлі людьми потребує міжнародного обміну інформацією, спільних розслідувань, фінансової розвідки, оперативної взаємодії правоохоронних органів та ефективного механізму отримання електронних доказів із різних юрисдикцій.

6.1.5. Цифрова трансформація механізмів торгівлі людьми

Однією з найбільш істотних характеристик сучасної торгівлі людьми є цифрова трансформація способів її вчинення. Водночас цифровізацію не слід розглядати як самостійну причину торгівлі людьми. Як наголошує ОБСЄ, технології є інструментом, який може використовуватися злочинцями для вербування, реклами, контролю потерпілих, організації експлуатації та переміщення незаконних доходів [61].

Першим напрямом цифрової трансформації є вербування. Соціальні мережі, сайти пошуку роботи, месенджери, платформи знайомств та інші цифрові ресурси дають можливість встановлювати контакт із потенційними потерпілими без безпосереднього фізичного контакту. Це розширює географію пошуку та дозволяє злочинцям одночасно комунікувати з великою кількістю осіб [61; 63].

Особливу небезпеку становить можливість використання інформації, яку користувачі самостійно розміщують у соціальних мережах. Відомості про матеріальне становище, сімейні обставини, пошук роботи, міграційні плани або інші життєві труднощі можуть використовуватися злочинцями для визначення потенційної уразливості та персоналізації способу впливу [61].

Другим напрямом є використання цифрових технологій для формування довіри та психологічного контролю. Комунікація через месенджери і соціальні мережі дозволяє підтримувати постійний контакт із потерпілим, здійснювати психологічний тиск, погрожувати поширенням персональної інформації та контролювати поведінку особи.

Третій напрям пов’язаний із цифровізацією самої експлуатації. Окремі форми сексуальної експлуатації можуть реалізовуватися через цифрові платформи та онлайн-трансляції, що дозволяє фізично віддаленим особам брати участь у злочинній діяльності. У таких випадках організатори, експлуататори та споживачі незаконного контенту можуть перебувати у різних державах.

Четвертим напрямом є використання технологій для фінансового забезпечення злочинної діяльності. Електронні платежі, цифрові фінансові сервіси та віртуальні активи можуть використовуватися для переміщення доходів, отриманих від експлуатації. У зв’язку з цим фінансове розслідування сучасної торгівлі людьми дедалі більше потребує аналізу цифрових транзакцій та інших електронних фінансових слідів [61; 64].

Окремого значення набуває використання технологій штучного інтелекту. У сучасних матеріалах ОБСЄ зазначається, що AI-інструменти можуть використовуватися для створення переконливого неправдивого контенту, імітації особи, автоматизації комунікації та масштабування процесів вербування. У 2026 році ОБСЄ окремо звернула увагу на ризики AI-опосередкованого вербування, цифрового грумінгу, імперсонації та використання синтетичного контенту [65].

Для України цифровий компонент має особливе значення у зв’язку з війною та масовим вимушеним переміщенням населення. ОБСЄ зазначає, що переміщені особи активно використовують цифрові платформи для пошуку роботи, освіти, соціальних послуг та підтримки, що одночасно створює додаткові можливості для злочинців здійснювати технологічно опосередковане вербування [65].

Водночас цифрове середовище створює не лише нові можливості для злочинців, а й нові інструменти для правоохоронної діяльності. Електронне листування, метадані, цифрові оголошення, інформація про облікові записи, платіжні операції, дані цифрових платформ та інші електронні сліди можуть використовуватися для встановлення зв’язків між учасниками злочинної

діяльності, ідентифікації потерпілих та документування окремих елементів злочинного механізму [61; 63].

ОБСЄ розглядає технології саме у подвійному контексті: з одного боку, вони створюють нові можливості для торгівців людьми, а з іншого – можуть використовуватися правоохоронними органами та громадянським суспільством для виявлення злочинів, ідентифікації потерпілих та протидії злочинним мережам [61].

Таким чином, цифрова трансформація не створила принципово нового соціального явища торгівлі людьми, але істотно змінила механізми його реалізації. Її основними проявами є цифровізація вербування, дистанційна комунікація з потерпілими, використання цифрових інструментів контролю, перенесення окремих форм експлуатації в онлайн–середовище, застосування електронних платіжних інструментів та використання штучного інтелекту для масштабування окремих злочинних практик [61; 63; 68].

Отже, сучасну торгівлю людьми доцільно розглядати як динамічне кримінальне явище, що поєднує традиційні механізми вербування, переміщення та експлуатації з мережевими, транскордонними та цифровими способами організації злочинної діяльності. Її кримінологічна специфіка визначається не лише різноманітністю форм експлуатації, а й здатністю злочинців адаптувати механізми впливу до соціальних криз, міграційних процесів, збройних конфліктів та технологічних змін. Для України ця характеристика набуває особливого значення в умовах повномасштабної війни, масового переміщення населення та зростання ролі цифрового середовища у працевлаштуванні, комунікації та отриманні соціальних послуг.

6.2. Фактори та індикатори ризику

Кримінологічне дослідження торгівлі людьми передбачає не лише аналіз уже вчинених кримінальних правопорушень, а й визначення обставин, за яких підвищується ймовірність втягнення людини в експлуатаційні відносини. У цьому контексті особливого значення набуває категорія ризику торгівлі людьми, яка характеризує наявність сукупності соціальних, економічних, міграційних,

поведінкових, цифрових, просторових та інших обставин, що можуть підвищувати уразливість особи або створювати сприятливе середовище для діяльності торговців людьми.

При цьому фактор ризику та індикатор ризику не є тотожними поняттями. Фактор ризику являє собою обставину, процес або умову, які можуть збільшувати уразливість особи чи сприяти виникненню ситуації експлуатації. Індикатором є конкретна ознака або сукупність ознак, доступних для спостереження, виявлення чи документування, які можуть свідчити про наявність підвищеного ризику. Таке розмежування має принципове значення для правоохоронної та превентивної діяльності, оскільки сама наявність певного фактора або індикатора не означає, що особа є потерпілою від торгівлі людьми або що відповідне кримінальне правопорушення вже вчинено.

Торгівля людьми виникає внаслідок взаємодії попиту на дешеву або контрольовану працю, сексуальні послуги чи інші форми експлуатації з уразливістю потенційних потерпілих та можливостями, які створює для злочинців конкретне соціальне середовище. У цьому сенсі ризик торгівлі людьми має багатофакторний характер і не може бути пояснений виключно бідністю, міграцією, безробіттям або використанням цифрових технологій.

Важливість такого підходу зумовлена також значною латентністю торгівлі людьми. Особа може перебувати в ситуації експлуатації тривалий час, не звертаючись по допомогу або не ідентифікуючи себе як потерпілу. Причинами можуть бути страх перед експлуататором, психологічна залежність, погрози, економічна залежність, незнання своїх прав, недовіра до державних органів або відсутність доступу до допомоги. Тому система ризик-індикаторів має бути спрямована не на механічну класифікацію людей, а на своєчасне виявлення ситуацій, які потребують додаткової уваги та перевірки.

6.2.1. Соціально–економічні фактори

Соціально–економічні фактори формують одну з базових груп умов, які можуть підвищувати уразливість людини до торгівлі людьми. До них належать бідність, безробіття, нестабільна зайнятість, низький рівень доходів, відсутність

житла, боргові зобов’язання, соціальна ізоляція, обмежений доступ до освіти та професійної підготовки, а також відсутність ефективної системи соціальної підтримки.

Водночас науково некоректно ототожнювати бідність із неминучим ризиком торгівлі людьми. Економічна нестабільність є лише одним із факторів, який у поєднанні з іншими обставинами може підвищувати уразливість. Наприклад, особа, яка втратила роботу, одночасно має значні боргові зобов’язання, не має стабільного житла та отримує неправдиву пропозицію роботи за кордоном, перебуває у принципово іншій ситуації ризику, ніж особа, яка також шукає роботу, але має стабільне житло, соціальну підтримку та можливість перевірити роботодавця.

Примусова праця може характеризуватися сукупністю індикаторів, серед яких обмеження свободи пересування, утримання заробітної плати, боргова залежність, обман щодо умов праці, зловживання уразливістю, залякування та погрози, а також надмірна залежність працівника від роботодавця. Частина цих ознак одночасно може розглядатися як індикатори переходу від потенційного ризику до фактичної експлуатації.

Економічна залежність може формуватися поступово. Спочатку особі пропонується робота із привабливими умовами, після чого створюється борг за проїзд, проживання, харчування або інші послуги. Надалі цей борг використовується для обмеження можливості особи залишити місце роботи. У такому випадку економічний механізм перетворюється на інструмент контролю.

Соціальна ізоляція також є важливим фактором. Відсутність сімейних або соціальних зв’язків, перебування далеко від звичного місця проживання, незнання мови чи місцевих правил можуть зменшувати можливість потерпілого отримати сторонню допомогу. Особливо це характерно для осіб, які перебувають за межами держави свого громадянства.

В умовах України до соціально-економічних факторів можуть додаватися наслідки війни: втрата житла або роботи, переміщення, розрив соціальних зв’язків, залежність від гуманітарної допомоги та необхідність термінового

пошуку доходу. Дослідження UNODC щодо організованої злочинності в Україні в умовах війни звертає увагу на використання злочинцями уразливості внутрішньо переміщених осіб [62].

Таким чином, до основних соціально–економічних факторів ризику доцільно відносити не окремий показник матеріального становища, а комплекс взаємопов'язаних характеристик: економічну нестабільність, відсутність безпечного житла, залежність від інших осіб, нестабільну зайнятість, боргові зобов'язання, соціальну ізоляцію та обмежений доступ до допомоги.

6.2.2. Міграційні та геополітичні фактори

Міграційні процеси самі по собі не є причиною торгівлі людьми. Водночас міграція може створювати умови, у яких особа стає більш залежною від посередників або роботодавців та має менше можливостей для захисту своїх прав.

Особливо значущими факторами є нерегулярний або невизначений міграційний статус, відсутність документів, недостатнє знання законодавства держави перебування, мовний бар'єр, залежність від посередника при працевлаштуванні, відсутність доступу до офіційних каналів працевлаштування та соціальна ізоляція.

Торгівля людьми може виникати як у межах внутрішньої міграції, так і внаслідок транскордонного переміщення. При цьому переміщення через державний кордон не є необхідною умовою торгівлі людьми. Відповідно до міжнародного визначення та українського законодавства кримінальне правопорушення може бути вчинене і без перетинання державного кордону [1; 6].

Для України особливого значення набуває фактор вимушеного переміщення населення внаслідок повномасштабної війни. Мільйони людей були змушені залишити свої домівки, частина перемістилася в межах України, інші – за кордон. Така ситуація створює середовище підвищеної уразливості, оскільки людина може одночасно втратити житло, роботу, звичне соціальне оточення та доступ до сталих джерел доходу [62].

Окремий ризик становить переміщення дітей без належного супроводу або перебування дітей у ситуації розриву сімейних і соціальних зв'язків. Дитячий вік сам по собі є фактором особливої уразливості, що обумовлює необхідність застосування спеціальних механізмів захисту [1; 6].

Геополітичні кризи, збройні конфлікти, гуманітарні катастрофи та масштабні переміщення населення можуть змінювати структуру попиту і пропозиції на незаконні експлуатаційні послуги, створювати дефіцит безпечного працевлаштування та послаблювати соціальні механізми захисту. У таких умовах злочинці можуть використовувати інформаційний хаос, невизначеність та нагальну потребу людей у житлі, роботі або транспорті.

Для правоохоронної діяльності важливо враховувати, що міграційний статус або факт перетину кордону не можуть використовуватися як самостійний критерій ризику. Оцінювання має здійснюватися за сукупністю обставин, зокрема характером працевлаштування, умовами проживання, залежністю від посередників, доступом до документів, можливістю вільно залишити місце роботи та наявністю ознак примусу або обману.

6.2.3. Цифрові фактори ризику

Цифровізація суспільних відносин сформувала нову групу факторів, які можуть сприяти виникненню або маскуванню ситуацій торгівлі людьми. Соціальні мережі, месенджери, платформи пошуку роботи, сервіси знайомств та інші цифрові ресурси використовуються не лише для комунікації, а й для пошуку потенційних потерпілих, формування довіри, розміщення неправдивих оголошень та організації експлуатації [61].

Одним із ключових цифрових факторів є відсутність можливості або навичок перевірити достовірність інформації про роботодавця, посередника чи запропоновану діяльність. Особа може отримати привабливу пропозицію роботи через соціальну мережу або месенджер, не маючи достатньої інформації про суб'єкта, який її розмістив.

Іншим фактором є надмірна відкритість персональної інформації. Публічні відомості про сімейний стан, місце проживання, пошук роботи, матеріальні

труднощі, плани щодо виїзду за кордон або інші життєві обставини можуть бути використані злочинцями для персоналізованого впливу [61].

Значний ризик становлять фальшиві профілі та імперсонація. Злочинець може створити цифрову ідентичність, яка створює враження легітимного роботодавця, представника компанії, знайомого або потенційного партнера. Використання штучного інтелекту додатково розширює можливості створення синтетичного тексту, зображень, аудіо та відео, які можуть підвищувати переконливість неправдивої комунікації [66].

Цифровим фактором ризику є також комунікація виключно через анонімні або важко ідентифіковані облікові записи, вимога перейти на зашифровані або інші канали зв'язку, відмова надати перевірювані відомості про роботодавця чи умови праці, а також вимога передати персональні документи або фінансову інформацію до початку офіційних трудових відносин.

Разом із тим цифрова активність людини сама по собі не може вважатися ознакою ризику торгівлі людьми. Використання соціальних мереж, месенджерів або онлайн-сервісів є звичайною поведінкою сучасної людини. Кримінологічне значення має саме поєднання цифрових обставин з іншими факторами уразливості або ознаками експлуатаційного контролю.

6.2.4. Поведінкові індикатори

Поведінкові індикатори мають особливе значення для первинного виявлення можливих потерпілих, оскільки вони можуть бути безпосередньо спостережуваними працівниками правоохоронних органів, соціальних служб, прикордонниками, медичними працівниками, працівниками громадських організацій або іншими суб'єктами, які контактують із потенційними потерпілими.

До таких індикаторів можуть належати страх перед спілкуванням із представниками державних органів, небажання відповідати на запитання про роботу або місце проживання, суперечності між розповіддю особи та очевидними обставинами її перебування, ознаки психологічного тиску, надмірна

залежність від іншої особи під час спілкування, відсутність контролю над власними документами або фінансовими ресурсами.

Міжнародна організація праці серед індикаторів примусової праці називає, зокрема, обмеження свободи пересування, ізоляцію, утримання документів, утримання заробітної плати, боргову залежність, погрози, залякування, фізичне або сексуальне насильство, а також обман щодо характеру та умов роботи [67].

Важливим індикатором є контроль іншої особи над поведінкою потенційного потерпілого. Наприклад, особа може не мати можливості самостійно відповідати на запитання, постійно узгоджувати свої відповіді з іншою людиною або демонструвати очевидний страх залишитися без супроводу.

Певне значення має також невідповідність між заявленою метою перебування та фактичними умовами. Наприклад, особа повідомляє про працевлаштування, однак не має інформації про роботодавця, не знає умов договору, не отримує обіцяну оплату або не має можливості самостійно залишити місце роботи.

Однак жоден із зазначених індикаторів не може використовуватися ізольовано. Страх, нервозність, відсутність документів чи небажання спілкуватися з правоохоронцями можуть бути зумовлені багатьма причинами. Тому поведінкові індикатори мають використовуватися як підстава для делікатного додаткового з’ясування обставин, а не як автоматична підстава для висновку про наявність торгівлі людьми.

6.2.5. Просторові та часові фактори

Ризик торгівлі людьми має також просторовий і часовий вимір. Злочинна діяльність не розподіляється рівномірно у просторі, а її інтенсивність може залежати від особливостей конкретного середовища.

До потенційно значущих просторових факторів належать місця концентрації міграційних потоків, транспортні вузли, прикордонні райони, місця тимчасового проживання переміщених осіб, райони концентрації сезонних працівників, окремі сектори неформальної зайнятості, місця надання

сексуальних послуг, а також цифрово опосередковані середовища, які не мають чіткої фізичної локалізації.

При цьому сам факт перебування особи у транспортному вузлі, на кордоні або в районі концентрації мігрантів не свідчить про ризик торгівлі людьми. Просторовий фактор набуває кримінологічного значення лише у взаємозв'язку з іншими характеристиками середовища та поведінки.

Часовий вимір пов'язаний із періодами, коли збільшується мобільність населення, попит на сезонну працю або кількість осіб, які шукають тимчасову зайнятість. Додаткові ризики можуть виникати під час криз, надзвичайних ситуацій, масових переміщень населення та інших періодів соціальної нестабільності.

Для України особливо значущим часовим фактором є тривалість повномасштабної війни та пов'язані з нею зміни структури міграції, зайнятості та соціальної підтримки. Водночас кримінологічний аналіз має уникати спрощеного причинно-наслідкового зв'язку між війною та торгівлею людьми: війна створює або посилює окремі фактори уразливості, але сама по собі не означає виникнення торгівлі людьми [62].

Перспективним напрямом є поєднання просторового та часового аналізу з геоінформаційними системами. Накладання даних про виявлені випадки, маршрути переміщення, місця розміщення потенційно уразливих груп, транспортну інфраструктуру та інші фактори може використовуватися для визначення територій і періодів підвищеного ризику. Такий підхід повинен ґрунтуватися на агрегованих даних і дотриманні вимог щодо захисту персональної інформації.

6.2.6. Фінансові індикатори

Фінансові індикатори набувають дедалі більшого значення у виявленні торгівлі людьми, оскільки експлуатація людини, як правило, має економічну мотивацію. Аналіз фінансових потоків може дозволити виявити зв'язки між учасниками злочинної діяльності, встановити джерела незаконних доходів та ідентифікувати механізми їх переміщення.

До потенційно значущих фінансових індикаторів належать систематичні платежі між особами, пов’язаними з вербуванням, транспортуванням та експлуатацією; отримання коштів за посередницькі послуги, які фактично супроводжуються контролем над потерпілими; невідповідність офіційних доходів характеру здійснюваної діяльності; використання значної кількості рахунків або платіжних інструментів для розподілу коштів; а також транзакції, пов’язані з діяльністю, що має ознаки експлуатації.

Важливим індикатором може бути рух коштів, пов’язаний із вербуванням і переміщенням потерпілих. Наприклад, витрати на придбання квитків, оплату проживання, трансфери або інші логістичні послуги можуть у сукупності з іншими даними дозволити реконструювати механізм злочинної діяльності.

Окрему групу становлять операції з віртуальними активами. Цифрові фінансові інструменти можуть використовуватися для переміщення доходів через державні кордони, а особливості окремих криптовалютних операцій можуть ускладнювати традиційні механізми фінансового моніторингу. ОБСЄ звертає увагу на необхідність посилення спроможності компетентних органів відстежувати фінансові потоки, пов’язані з торгівлею людьми, включно з операціями з віртуальними активами [68].

Водночас окремий фінансовий індикатор не може розглядатися як доказ торгівлі людьми. Його значення виникає внаслідок поєднання з іншими даними – інформацією про вербування, переміщення, комунікацію, умови праці, контроль над потерпілими та характер отримуваних доходів.

Фінансовий аналіз тому повинен бути інтегрованим із кримінальним аналізом інших даних. Зіставлення фінансових транзакцій із цифровими комунікаціями, транспортними даними, відомостями про перетин кордону та інформацією про трудові відносини може істотно підвищувати ефективність виявлення злочинних мереж.

6.2.7. Комплексна система індикаторів ризику

Розглянуті фактори свідчать, що ефективне виявлення ризику торгівлі людьми неможливе на основі одного критерію. Бідність, міграція, користування

соціальними мережами, відсутність документів або незвичайна поведінка окремо не дають достатніх підстав для висновку про наявність ситуації торгівлі людьми. Відповідно, перспективним є формування комплексної системи індикаторів, у якій окремі ознаки оцінюються у взаємозв'язку.

Таку систему доцільно будувати за сімома взаємопов'язаними групами: соціально-економічними, міграційними та геополітичними, цифровими, поведінковими, просторово-часовими та фінансовими індикаторами. При цьому окремо має враховуватися контекст конкретної ситуації та особливості потенційного потерпілого.

Соціально-економічний блок може охоплювати безробіття, відсутність стабільного доходу, житлову нестабільність, боргову залежність, соціальну ізоляцію та інші обставини уразливості. Міграційний блок – залежність від посередників, невизначений статус, відсутність документів, мовні бар'єри, незнання прав та інші фактори, пов'язані з переміщенням. Цифровий блок – сумнівні онлайн-пропозиції, фальшиві профілі, неможливість перевірити роботодавця, використання анонімних каналів зв'язку та інші ознаки технологічно опосередкованого вербування.

Поведінковий блок має включати ознаки контролю іншої особи, страх, ізоляцію, небажання або неможливість самостійно спілкуватися, відсутність контролю над документами чи фінансовими ресурсами, а також суперечності між заявленими та фактичними умовами праці. Просторово-часовий блок може враховувати місце та час виникнення ситуації, особливості міграційних потоків, транспортної інфраструктури та кризових процесів. Фінансовий блок – характер і напрям руху коштів, платежі між учасниками, ознаки отримання доходів від експлуатації та використання цифрових фінансових інструментів.

Для практичної діяльності доцільно розглядати систему індикаторів не як жорстку шкалу, яка автоматично визначає наявність або відсутність торгівлі людьми, а як інструмент **первинного ризик-орієнтованого виявлення**. У цьому випадку оцінювання може здійснюватися за трьома рівнями: низький ризик, підвищений ризик та високий ризик. Така градація повинна

використовуватися виключно для визначення необхідності подальшої перевірки та надання допомоги, а не для автоматичної кваліфікації поведінки особи або визначення її статусу.

Принциповим є застосування контекстного підходу. Наприклад, наявність пропозиції роботи через соціальну мережу сама по собі не свідчить про торгівлю людьми. Однак якщо одночасно встановлено відсутність інформації про роботодавця, вимогу передати документи, оплатити значний «борг» за працевлаштування, обмеження зв'язку з родичами та неможливість самостійно залишити місце роботи, сукупність таких ознак формує значно вищий рівень ризику та потребує невідкладного реагування.

Перспективним є застосування у правоохоронній діяльності ризик-орієнтованих аналітичних моделей, які дозволяють об'єднувати різні типи даних. За умови належних правових підстав та дотримання вимог щодо захисту персональних даних можуть аналізуватися відомості про оголошення, цифрові комунікації, транспортні маршрути, фінансові операції, кримінальні провадження та інші релевантні джерела інформації. Особливого значення тут набуває не максимізація кількості зібраних даних, а їх релевантність, достовірність і законність отримання.

Комплексна система індикаторів повинна також передбачати механізм постійного оновлення. Способи торгівлі людьми змінюються під впливом соціальних, економічних, воєнних і технологічних процесів. Тому перелік індикаторів не може бути раз і назавжди визначеним. Нові способи цифрового вербування, зміни міграційних маршрутів, поява нових форм експлуатації та фінансових інструментів потребують регулярного перегляду відповідних моделей ризику.

Таким чином, кримінологічно обґрунтована система оцінювання ризику торгівлі людьми повинна базуватися на поєднанні факторів уразливості, характеристик середовища та безпосередніх індикаторів експлуатаційного контролю. Її призначення полягає не у встановленні вини чи автоматичному визначенні потерпілого, а у своєчасному виявленні ситуацій, які потребують

додаткової перевірки, захисту потенційної жертви та, за наявності відповідних підстав, початку кримінального розслідування.

Узагальнюючи, можна констатувати, що сучасний ризик торгівлі людьми формується на перетині декількох груп чинників: **уразливості особи, експлуатаційного середовища, можливостей злочинців та доступності механізмів контролю**. Саме тому найбільш перспективною є не статична система окремих ознак, а динамічна ризик-орієнтована модель, здатна враховувати взаємозв'язки між соціально-економічними, міграційними, цифровими, поведінковими, просторово-часовими та фінансовими характеристиками.

6.3. Моделювання злочинних мереж

Сучасна торгівля людьми дедалі частіше реалізується не як ізольована діяльність окремого правопорушника, а як сукупність взаємопов'язаних дій декількох осіб, між якими існують функціональні, комунікаційні, фінансові, транспортні та інші зв'язки. За таких умов традиційне дослідження кожного учасника окремо не завжди дозволяє встановити повну структуру злочинної діяльності. Одним із перспективних інструментів її аналізу є моделювання у формі мережі.

Мережевий підхід ґрунтується на представленні досліджуваної системи як сукупності об'єктів та зв'язків між ними. У теорії графів така система може бути представлена графом (G=(V,E)), де (V) – множина вузлів, а (E) – множина ребер, що відображають встановлені або припущені зв'язки між вузлами. У контексті кримінального аналізу вузлами можуть виступати фізичні особи, юридичні особи, телефонні номери, облікові записи, банківські рахунки, транспортні засоби, адреси, цифрові ідентифікатори або інші об'єкти, щодо яких наявна релевантна інформація. Ребра можуть відображати спільне використання ресурсу, комунікацію, фінансову операцію, родинний або діловий зв'язок, спільне переміщення, оренду майна чи іншу документально встановлену взаємодію.

Такий підхід відповідає сучасній концепції intelligence–led policing, у межах якої аналітична інформація використовується для визначення структур злочинності, ключових суб'єктів та пріоритетів правоохоронної діяльності [68]. Мережевий аналіз при цьому не замінює доказування, оперативну роботу або процесуальне розслідування, а є інструментом упорядкування та аналізу інформації.

Особливість мережевого моделювання торгівлі людьми полягає в необхідності врахування багаторівневого характеру відповідної злочинної діяльності. Один і той самий учасник може одночасно виконувати декілька функцій, а один зв'язок може мати кілька характеристик. Наприклад, дві особи можуть бути пов'язані одночасно телефонними контактами, спільними фінансовими операціями та переміщенням потерпілих. Тому для практичного кримінального аналізу доцільно використовувати не лише прості графи, а й атрибутовані, зважені та, за потреби, мультиграфові моделі.

Важливим є також розмежування встановлених і припущених зв'язків. Якщо факт телефонного контакту підтверджений даними оператора, відповідне ребро може мати статус підтвердженого. Якщо зв'язок лише передбачається на підставі непрямих ознак, він повинен мати інший статус і не може ототожнюватися з доведеним фактом участі у злочинній діяльності. Такий підхід дозволяє уникати однієї з основних небезпек автоматизованого мережевого аналізу – перетворення статистичної або аналітичної кореляції на твердження про кримінальну причетність.

6.3.1. Графове представлення злочинної діяльності

Графове представлення дозволяє перетворити розрізнені відомості про учасників та події на формальну структуру, придатну для подальшого аналізу. У найпростішій моделі вузли відповідають особам, а ребра – встановленим зв'язкам між ними. Однак для аналізу торгівлі людьми така модель є недостатньою, оскільки злочинна діяльність включає значну кількість об'єктів, які не є безпосередніми учасниками.

Тому доцільним є формування гетерогенної мережі, у якій можуть бути представлені різні типи вузлів: особи, організації, телефонні номери, електронні адреси, акаунти соціальних мереж, банківські рахунки, транспортні засоби, адреси, оголошення, документи, події та інші об’єкти. Зв’язки між ними також можуть бути різного типу: «спілкується», «володіє», «використовує», «отримує кошти від», «перераховує кошти», «переміщується разом із», «розміщує оголошення», «пов’язаний з адресою» тощо.

Таке представлення відповідає підходам до аналізу зв’язків між різними типами сутностей, що застосовуються в кримінальному аналізі та intelligence analysis. На практиці воно дозволяє перейти від запитання «хто контактував із ким?» до складнішого питання «яким чином різні об’єкти та події пов’язані між собою?» [68; 69].

Наприклад, інформація про неправдиве оголошення щодо працевлаштування може бути представлена як зв’язок між конкретним цифровим акаунтом, номером телефону, особою, платіжним інструментом та адресою, де фактично перебувала потенційна жертва. Якщо аналогічний номер телефону або рахунок зустрічається в інших епізодах, граф дозволяє виявити спільний елемент між ними.

Для підвищення аналітичної цінності граф може бути зваженим. Вага ребра може відображати кількість контактів, частоту транзакцій, тривалість взаємодії або інший обґрунтований параметр. Водночас вибір ваги повинен відповідати природі конкретного зв’язку. Наприклад, велика кількість телефонних контактів свідчить про інтенсивність комунікації, але сама по собі не доводить характеру цієї комунікації.

Доцільним є також використання часових атрибутів. Кожен зв’язок або подія може мати дату початку, дату завершення або часовий інтервал. Це дозволяє досліджувати не лише структуру мережі в певний момент, а й послідовність її формування та зміни.

Графове представлення має особливе значення у випадках, коли інформація надходить із різних джерел. Дані кримінального провадження,

OSINT, фінансового аналізу, інформаційних систем, результатів допитів та цифрової криміналістики можуть бути представлені в єдиній аналітичній моделі. При цьому джерело кожного зв'язку повинно зберігатися як окремий атрибут, що дозволяє оцінювати його надійність та перевірюваність.

Таким чином, графова модель виконує функцію своєрідного «каркаса» кримінального аналізу, на якому можуть поєднуватися різні типи інформації. Її перевагою є можливість одночасного аналізу великої кількості об'єктів і зв'язків, які складно простежити при лінійному опрацюванні інформації.

6.3.2. Виявлення ключових учасників мережі

Одним із основних завдань мережевого аналізу є визначення вузлів, які займають особливе положення у структурі мережі. При цьому поняття «ключовий учасник» не повинно автоматично ототожнюватися з найбільш активною або найбільш пов'язаною особою. У різних мережевих моделях ключовість може визначатися різними властивостями.

Одним із базових показників є ступінь вузла (degree), тобто кількість його безпосередніх зв'язків. Високе значення degree може свідчити про те, що особа або інший об'єкт має значну кількість контактів. У контексті торгівлі людьми такий показник може допомогти визначити осіб, які контактують із великою кількістю учасників або пов'язані з численними епізодами.

Водночас високий ступінь не означає автоматично високої злочинної ролі. Наприклад, транспортний диспетчер, оператор сервісу або адміністратор легальної організації може мати велику кількість зв'язків, не будучи учасником злочинної діяльності. Тому показник degree повинен розглядатися лише в контексті інших характеристик.

Іншим важливим показником є betweenness centrality – центральність посередництва. Вона характеризує, наскільки часто певний вузол розташований на найкоротших шляхах між іншими вузлами мережі [71]. У кримінальному аналізі цей показник може бути корисним для пошуку осіб або об'єктів, які виконують функцію посередників між окремими частинами мережі.

Наприклад, одна особа може підтримувати зв’язок між вербувальниками в одній групі та особами, які безпосередньо здійснюють експлуатацію в іншій. Навіть за відносно невеликої кількості власних контактів така особа може мати високу структурну значущість через своє положення між підгрупами.

Closeness centrality характеризує близькість вузла до інших вузлів за довжиною найкоротших шляхів, а eigenvector centrality враховує не лише кількість зв’язків, а й значущість вузлів, із якими здійснюється взаємодія [71]. Використання декількох показників дозволяє отримати більш об’єктивне уявлення про структурну роль окремого вузла.

Окремого значення набуває PageRank та споріднені методи оцінювання структурної значущості вузлів. Однак їх використання в кримінальному аналізі має здійснюватися з урахуванням природи даних та поставленого завдання. Алгоритмічно високий рейтинг вузла не означає його кримінальної вини.

Доцільним є формування комплексного профілю вузла, який може включати кількість та тип зв’язків, центральність, часову активність, зв’язки з іншими значущими вузлами, фінансові характеристики та інші релевантні атрибути. Такий підхід дозволяє перейти від пошуку «найбільш підозрілої особи» до визначення вузлів, які є найбільш значущими для функціонування конкретної мережі.

Для практичних цілей можна використовувати матрицю, у якій кожному вузлу відповідають значення кількох показників центральності. Наприклад, особа з високим degree може бути комунікаційним центром, особа з високим betweenness – посередником, а особа з високим eigenvector centrality – вузлом, пов’язаним з іншими структурно значущими учасниками.

Таким чином, мережевий аналіз дозволяє встановлювати не лише найбільш активних учасників, а й тих, хто займає стратегічно важливе положення у структурі злочинної діяльності.

6.3.3. Виявлення прихованих зв’язків

Однією з найбільш складних задач кримінального аналізу є виявлення зв’язків, які безпосередньо не зафіксовані в інформаційних джерелах.

Прихований зв’язок у цьому контексті не означає доведений факт таємної взаємодії. Йдеться про структурну або аналітичну гіпотезу про можливий зв’язок, яка потребує подальшої перевірки.

Підставою для формування такої гіпотези може бути наявність спільних атрибутів. Наприклад, різні особи можуть використовувати той самий номер телефону, електронну адресу, банківський рахунок, транспортний засіб, IP–адресу, адресу проживання або цифровий акаунт. Сукупність таких збігів може свідчити про потенційний зв’язок, але кожен із них повинен оцінюватися з урахуванням можливості законного або випадкового збігу.

Іншим підходом є аналіз довших шляхів у мережі. Якщо два вузли не мають прямого зв’язку, але через декілька проміжних вузлів пов’язані з однією групою об’єктів, це може бути підставою для перевірки можливого функціонального зв’язку між ними.

Особливе значення має аналіз двочасткових і багатошарових мереж. Наприклад, у мережі «особа – телефонний номер» два різних учасники можуть бути пов’язані спільним номером. У мережі «особа – фінансовий рахунок» спільний рахунок може створювати зв’язок між особами, які безпосередньо між собою не контактували. У мережі «особа – місце» спільне використання одного об’єкта нерухомості або адреси може виявити додаткову структурну залежність.

Для виявлення прихованих зв’язків можуть використовуватися алгоритми пошуку спільних сусідів, коефіцієнти подібності, аналіз коротких шляхів та методи link prediction. Останні використовуються для прогнозування потенційних зв’язків між вузлами на основі структури вже відомої мережі.

Однак у кримінальному аналізі особливо важливо розмежовувати **прогнозований зв’язок** та **встановлений зв’язок**. Результат алгоритму link prediction є лише аналітичною гіпотезою. Він не може самостійно використовуватися як доказ існування фактичної взаємодії або кримінальної причетності особи.

Додатковим джерелом прихованих зв’язків може бути часовий аналіз. Саме створення часової лінії може дозволити зрозуміти послідовність подій та

виявити приховані зв’язки [72, с. 173]. Наприклад, повторювані збіги між перебуванням різних осіб у конкретних місцях, синхронність телефонної активності, послідовність фінансових транзакцій та переміщення потерпілих можуть утворювати часовий патерн. Саме поєднання просторової, часової та мережевої інформації часто має більшу аналітичну цінність, ніж кожен вид даних окремо.

Важливим є також аналіз цифрової ідентичності. Одна фізична особа може використовувати декілька цифрових акаунтів, номерів телефонів або інших ідентифікаторів. Встановлення належності таких ідентифікаторів одній особі може істотно змінити структуру графа. Водночас відповідні висновки повинні ґрунтуватися на перевірюваних даних, а не лише на схожості імен, фотографій чи стилю поведінки.

Отже, виявлення прихованих зв’язків є процесом формування та перевірки аналітичних гіпотез. Його результативність залежить не лише від алгоритму, а й від якості первинних даних, їхньої повноти, точності і незалежного підтвердження.

6.3.4. Аналіз підгруп та ієрархії злочинних мереж

Злочинна мережа може складатися з декількох функціональних підгруп, між якими існують різні за інтенсивністю та характером зв’язки. Виявлення таких підгруп дозволяє перейти від аналізу окремих учасників до дослідження організаційної структури мережі.

Одним із найбільш поширених підходів є community detection – автоматизоване виявлення груп вузлів, між якими зв’язки є більш щільними, ніж із рештою мережі. Для цього можуть використовуватися різні алгоритми, зокрема метод Louvain та його модифікації, Leiden, методи на основі спектрального аналізу та інші алгоритми виявлення спільнот [73].

Результат community detection не слід автоматично трактувати як встановлену злочинну групу. Алгоритм визначає структурно щільну частину графа за заданим критерієм. Така спільнота може відповідати реальній

організаційній підгрупі, але може також виникнути через особливості комунікації, спільне використання ресурсів або неповноту даних.

У мережі торгівлі людьми потенційні підгрупи можуть функціонально відповідати різним елементам злочинного механізму. Наприклад, одна група може бути пов’язана з пошуком і вербуванням, інша – з транспортним забезпеченням, третя – з безпосередньою експлуатацією, четверта – з фінансовими операціями. Проте така інтерпретація повинна здійснюватися лише після зіставлення результатів алгоритмічного аналізу з іншими джерелами інформації.

Для дослідження ієрархії важливим є аналіз не лише щільності зв’язків, а й їхньої спрямованості. У спрямованому графі ребро може відображати напрям передавання інформації, коштів або управлінської команди. Це дозволяє досліджувати потенційні ланцюги управління та посередництва.

У зважених графах додатково може аналізуватися інтенсивність зв’язків. Наприклад, систематичне передавання коштів або регулярна комунікація може мати більшу вагу, ніж одинична взаємодія. Однак значення ваги повинно бути обґрунтованим, оскільки механічне надання більшої ваги частішим контактам може спотворювати структуру мережі.

Важливо також враховувати, що злочинні мережі не обов’язково мають класичну вертикальну ієрархію. Сучасні організовані злочинні структури можуть характеризуватися децентралізованістю, тимчасовим залученням учасників та функціональним розподілом ролей. Саме тому мережеве моделювання є корисним доповненням до традиційного організаційного аналізу.

Порівняння щільності внутрішніх та зовнішніх зв’язків підгруп дозволяє визначити так звані структурні «мости» між ними. Такі вузли можуть мати особливе значення для розуміння того, як функціонально різні частини мережі взаємодіють між собою.

У практичному плані результати аналізу підгруп можуть використовуватися для визначення пріоритетів подальшої перевірки: які учасники мають найбільше зв’язків між підгрупами, які ресурси

використовуються кількома групами, які цифрові або фінансові ідентифікатори об’єднують різні епізоди та які структурні елементи залишаються недостатньо дослідженими.

Таким чином, community detection і споріднені методи доцільно використовувати не для автоматичного встановлення організованої злочинної групи, а як інструмент структурного аналізу, що дозволяє формувати та перевіряти гіпотези щодо функціональної організації мережі.

6.3.5. Динамічне моделювання мереж

Статичне представлення мережі відображає її структуру лише у певний момент часу. Для торгівлі людьми цього часто недостатньо, оскільки злочинна діяльність має процесуальний характер: учасники встановлюють нові контакти, змінюють засоби комунікації, залучають нових посередників, переміщують потерпілих, створюють нові цифрові акаунти та змінюють фінансові маршрути.

Тому доцільним є використання часових, або динамічних, мереж. У такій моделі граф характеризує стан мережі у певний момент або часовий інтервал. Порівняння послідовних станів дозволяє визначати появу та зникнення вузлів, формування нових зв’язків, припинення взаємодії, зміну центральності окремих учасників та перебудову підгруп.

Динамічний аналіз може здійснюватися шляхом побудови послідовності часових зрізів. Наприклад, мережа може аналізуватися за днями, тижнями або місяцями залежно від характеру даних. Для кожного зрізу визначаються її основні характеристики, після чого порівнюються зміни.

Особливе значення має аналіз моментів різкої зміни структури. Раптове виникнення значної кількості нових зв’язків, поява нового центрального вузла або швидке переміщення частини мережі до іншого цифрового ресурсу можуть бути підставою для додаткового аналізу. Проте самі по собі такі зміни не свідчать про злочинність – вони лише визначають аномалію або структурну зміну, яку необхідно пояснити.

Динамічне моделювання може використовуватися також для реконструкції послідовності подій. Наприклад, аналіз часових зв’язків між появою оголошення

про роботу, встановленням контакту з потенційним потерпілим, придбанням транспортних квитків, переміщенням особи, фінансовими операціями та подальшою комунікацією може дозволити побудувати хронологічну модель відповідного епізоду.

Особливе значення має поєднання динамічної мережі з географічною інформацією. У такому випадку кожен вузол або подія може мати просторову координату, а переміщення між місцями – часову характеристику. Це дозволяє досліджувати не лише структуру зв'язків, а й маршрути функціонування злочинної діяльності.

Динамічна модель також дає змогу досліджувати стійкість мережі. Наприклад, можна аналізувати, як зміна або видалення окремих вузлів впливає на зв'язність мережі. Такий підхід використовується в мережевій науці для дослідження стійкості та вразливості складних систем [74]. У кримінальному аналізі його потенційно можна застосовувати для моделювання різних сценаріїв припинення діяльності мережі. Однак результати такого моделювання слід розглядати як аналітичні сценарії, а не як гарантований прогноз поведінки злочинців.

Динамічний підхід особливо важливий для протидії цифровізованій торгівлі людьми. Цифрові мережі можуть змінюватися значно швидше, ніж традиційні соціальні зв'язки: можуть створюватися нові акаунти, змінюватися номери телефонів, видалятися оголошення, переходити комунікації між платформами. Тому аналіз лише одного інформаційного зрізу може не відображати реальної структури взаємодії [61].

Важливою умовою динамічного моделювання є точна фіксація часу отримання та актуальності інформації. Дані, які не мають достовірної часової прив'язки, можуть призвести до помилкової реконструкції послідовності подій. Саме тому кожен зв'язок у часовій моделі повинен, наскільки це можливо, супроводжуватися інформацією про джерело, час його встановлення та рівень достовірності.

Узагальнення результатів графового та динамічного аналізу дозволяє сформувати багатовимірну модель злочинної мережі, яка характеризує її структурну будову, учасників, функціональні підгрупи, комунікаційні та фінансові зв’язки, просторове розміщення і часову динаміку. Така модель може використовуватися для підтримки прийняття рішень у кримінальному аналізі, визначення напрямів подальшої перевірки та виявлення зв’язків, які залишаються непомітними при аналізі окремих інформаційних масивів.

Таким чином, моделювання злочинних мереж є перспективним інструментом дослідження сучасної торгівлі людьми, оскільки дозволяє перейти від аналізу ізольованих фактів до дослідження системи взаємопов’язаних осіб, ресурсів, подій та комунікацій. Його найбільша цінність полягає у можливості інтегрувати гетерогенні дані, визначати структурно значущі вузли, виявляти потенційні приховані зв’язки, аналізувати підгрупи та простежувати трансформацію мережі в часі.

Водночас графова модель не повинна розглядатися як автоматизований засіб встановлення вини. Результати network analysis, community detection, link prediction або оцінювання центральності є передусім **аналітичними результатами**, які потребують незалежної перевірки. Для кримінального провадження вони набувають доказового значення лише в межах передбачених законодавством процедур отримання, перевірки та оцінки відповідної інформації. Саме поєднання мережевого аналізу з OSINT, цифровою криміналістикою, фінансовим аналізом, просторовим аналізом та традиційними методами кримінального розслідування дозволяє сформувати більш повну картину злочинної діяльності.

6.4. Прогнозування ризиків торгівлі людьми

Розвиток аналітичних технологій створює можливості не лише для виявлення вже сформованих випадків торгівлі людьми, а й для прогнозування змін у криміногенному середовищі. На відміну від традиційного ретроспективного аналізу, прогнозний підхід орієнтований на визначення ймовірних тенденцій, територій, часових періодів, способів вербування та інших

характеристик, які можуть бути пов’язані з підвищенням ризику торгівлі людьми.

Прогнозування у цьому контексті доцільно розуміти як процес формування обґрунтованих припущень щодо майбутнього стану або розвитку явища на основі історичних та актуальних даних. Воно може стосуватися як кількісних показників – наприклад, очікуваної кількості повідомлень чи виявлених випадків, – так і просторового розподілу ризику, зміни способів вербування, трансформації злочинних мереж та появи нових каналів комунікації.

Необхідність такого підходу зумовлена динамічністю самої торгівлі людьми. Злочинці адаптують способи вербування до змін у соціальному середовищі, міграційних процесах, цифрових платформах та економічній ситуації. UNODC у глобальному звіті про торгівлю людьми наголошує на різноманітності форм експлуатації та регіональних відмінностях у характері виявлених випадків, що обумовлює необхідність аналізу не лише абсолютної кількості випадків, а й структури та тенденцій явища [60].

Водночас прогнозування ризиків не повинно ототожнюватися з передбаченням того, що конкретна особа обов’язково стане потерпілою або що конкретна особа вчинить кримінальне правопорушення. Прогнозний результат має характеризувати **ймовірність виникнення певної ситуації або зміни певного процесу**, а не встановлювати юридичний статус людини.

Саме тому об’єктом прогнозування доцільніше визначати часові, просторові, інформаційні, комунікаційні та мережеві характеристики торгівлі людьми. Такий підхід відповідає принципам ризик–орієнтованого аналізу та дозволяє використовувати прогнозування як інструмент підтримки прийняття рішень, а не як механізм автоматизованого кримінального профілювання.

Прогнозна модель може бути представлена як прогнозне значення часового ряду на h періодів уперед, сформоване на основі інформації, доступної на момент t:

$$\hat{Y}_{t+h|t},$$

де t – момент формування прогнозу, h – прогнозний горизонт, а символ |t вказує, що для отримання прогнозу використовується інформація, доступна до моменту t [75].

Залежно від завдання (Y) може бути кількісним показником, категорією ризику, просторовою оцінкою або ймовірністю виникнення певної події. При цьому якість прогнозу визначається не складністю алгоритму, а насамперед якістю даних, правильністю формулювання прогнозного завдання, репрезентативністю навчальної вибірки та належною валідацією результатів.

6.4.1. Прогнозування часової активності

Часовий аналіз дозволяє встановлювати закономірності зміни інтенсивності торгівлі людьми в різні періоди. Його основою є часові ряди – послідовності спостережень, упорядкованих відповідно до моменту або періоду їх виникнення.

Для кримінологічного аналізу такими спостереженнями можуть бути кількість зареєстрованих повідомлень, виявлених потерпілих, кримінальних правопорушень, встановлених фактів вербування, оголошень, пов’язаних із потенційно ризиковою діяльністю, або інших показників, за якими існують достатньо тривалі та порівнювані часові ряди.

Найпростішим способом аналізу часової активності є визначення тренду. Якщо кількість спостережуваних подій послідовно збільшується або зменшується, це може свідчити про відповідну тенденцію. Однак прямолінійне перенесення минулої тенденції в майбутнє не завжди є коректним. На кількість виявлених випадків можуть впливати зміни законодавства, правоохоронної практики, доступності допомоги потерпілим, методів реєстрації та інших чинників.

Важливим елементом часової моделі є сезонність. Певні форми експлуатації можуть бути пов’язані з сезонною зайнятістю, туристичними потоками, зміною попиту на працю або іншими циклічними процесами. Виявлення повторюваних часових закономірностей дозволяє визначити періоди, у які доцільно посилювати превентивні заходи.

Для цього можуть застосовуватися класичні статистичні методи аналізу часових рядів, зокрема ковзні середні, експоненційне згладжування, регресійні моделі та ARIMA–подібні підходи. За наявності достатнього обсягу якісних даних можливе використання методів машинного навчання для прогнозування нелінійних залежностей.

Однак у кримінологічних даних часто виникає проблема неповного спостереження. Зареєстровані випадки не є тотожними реальній кількості випадків торгівлі людьми. На статистику впливають латентність злочинності, готовність потерпілих звертатися по допомогу та спроможність компетентних органів виявляти відповідні правопорушення. Тому прогнозування на основі офіційної статистики фактично прогнозує **спостережуваний показник**, а не обов'язково реальний масштаб явища.

Особливої уваги потребує вплив різких зовнішніх подій. Війна, масштабні міграційні переміщення, економічні кризи, зміни міграційного законодавства або поява нових цифрових платформ можуть створювати структурні розриви у часових рядах. У таких випадках модель, побудована виключно на попередній статистичній закономірності, може давати систематично помилковий прогноз.

Тому часовий прогноз повинен супроводжуватися оцінюванням невизначеності. Доцільно використовувати не лише точкове прогнозне значення, а й прогнозний інтервал, який показує діапазон можливих значень. Це дозволяє уникати хибної точності та коректніше представляти результати аналітичної роботи.

6.4.2. Просторове прогнозування

Просторове прогнозування спрямоване на визначення територій, де за наявними даними може спостерігатися підвищений ризик виникнення або поширення певних форм торгівлі людьми. Його основою можуть бути географічно прив'язані дані про виявлені випадки, міграційні потоки, транспортну інфраструктуру, економічні характеристики територій, місця тимчасового розміщення переміщених осіб та інші релевантні показники.

Одним із базових інструментів є картографування просторового розподілу подій. Уже саме відображення випадків на карті може дозволити виявити концентрації, просторові кластери та території, які відрізняються від загальної структури розподілу.

Для кількісної оцінки можуть використовуватися методи просторової статистики та геоінформаційного аналізу. Зокрема, аналіз просторової автокореляції дозволяє оцінювати, чи мають близько розташовані території схожі значення певного показника. Методи кластеризації можуть використовуватися для виявлення територіальних концентрацій подій.

Просторове прогнозування може бути реалізоване через побудову поверхні ризику, де кожній територіальній одиниці відповідає певне значення прогнозованого показника. Така поверхня не повинна трактуватися як карта «злочинності» конкретних районів або населених пунктів. Вона відображає лише статистично або аналітично визначену концентрацію факторів ризику.

Особливо важливим є врахування різної щільності населення. Абсолютна кількість випадків у великому місті природно може бути більшою, ніж у невеликому населеному пункті. Тому порівняння територій часто доцільно здійснювати з використанням нормованих показників, наприклад кількості подій на певну кількість населення.

Для торгівлі людьми перспективним є поєднання просторового прогнозування з аналізом транспортних і міграційних маршрутів. Території можуть аналізуватися не лише як адміністративні одиниці, а як елементи просторової мережі, між якими переміщуються люди, ресурси та інформація.

Однак просторовий прогноз має суттєве обмеження: територіальна концентрація зареєстрованих випадків може відображати не лише реальну концентрацію злочинності, а й різницю в ефективності її виявлення. Територія з більшою кількістю зареєстрованих випадків може мати кращу систему виявлення, а не обов’язково вищу реальну інтенсивність торгівлі людьми.

Тому просторові моделі повинні враховувати як характеристики криміногенного середовища, так і характеристики спостереження. Це дозволяє зменшити ризик помилкової інтерпретації статистичних даних.

6.4.3. Прогнозування нових каналів вербування

Зміна способів вербування є одним із найбільш складних напрямів прогнозування, оскільки нові канали можуть виникати швидше, ніж формується достатня статистична база для їх кількісного моделювання.

Цифрові платформи створюють особливі умови для такої трансформації. Соціальні мережі, месенджери, платформи пошуку роботи та інші онлайн–середовища можуть використовуватися для пошуку потенційних потерпілих, встановлення контакту, формування довіри та подальшого контролю. OSCE прямо вказує, що цифрові технології використовуються для онлайн–вербування, контролю потерпілих, переміщення незаконних доходів і розширення злочинних мереж.

Прогнозування нових каналів тому має відрізнятися від класичного прогнозування часових рядів. Його завданням є не стільки визначення конкретної майбутньої платформи, скільки виявлення **ранніх сигналів трансформації способу вербування**.

Такими сигналами можуть бути поява нових типів оголошень, зміна лексики та візуального оформлення пропозицій, переміщення комунікації між платформами, поява нових способів приховування контактної інформації, зміна способів платежів або використання нових цифрових інструментів.

Для їх виявлення можуть застосовуватися методи аналізу тексту, кластеризації, тематичного моделювання, аналізу часових змін та виявлення аномалій. Наприклад, систематична поява нової групи оголошень зі схожими характеристиками може бути сигналом формування нового способу вербування.

Особливого значення набуває аналіз семантичних змін. Текст оголошень може змінюватися з метою обходу автоматизованої модерації або адаптації до поведінки користувачів. Тому простий пошук за ключовими словами може бути

недостатнім. Перспективними є методи обробки природної мови, які дозволяють аналізувати контекст, семантичну близькість текстів та їх трансформацію у часі.

Окремим фактором є розвиток генеративного штучного інтелекту. OSCE та Bali Process у спільному аналітичному матеріалі 2024 року звернули увагу на потенційну здатність генеративного AI посилювати масштаби та складність торгівлі людьми, зокрема через автоматизацію окремих елементів злочинної діяльності.

Тому прогнозування нових каналів вербування має включати технологічний моніторинг. Його завданням є виявлення не конкретного «злочинного застосунку», а змін у технологічному середовищі, які можуть знижувати витрати на вербування, підвищувати анонімність або збільшувати масштаб комунікації.

При цьому прогноз повинен залишатися гіпотезою. Якщо нова платформа або технологія має характеристики, які потенційно можуть бути використані для торгівлі людьми, це ще не означає, що вона фактично використовується з такою метою. Відповідні висновки повинні підтверджуватися емпіричними даними.

6.4.4. Моделі ризик–скорингу

Ризик-скоринг передбачає формування числової оцінки ризику на основі сукупності визначених факторів. Одним із поширених підходів є використання зваженої лінійної комбінації показників:

$$R = \sum_{i=1}^{n} w_i x_i$$

де R - інтегральний показник ризику, x_i - значення і-го індикатора, а w_i - його вага. Такий підхід передбачає агрегування окремих факторів шляхом множення їхніх значень на відповідні вагові коефіцієнти та підсумовування отриманих величин [76].

Така модель може бути зрозумілою для користувача та відносно легкою для аудиту. Наприклад, окремі показники можуть характеризувати наявність сумнівної пропозиції роботи, відсутність інформації про роботодавця, залежність від посередника, утримання документів, фінансову залежність або

інші обставини. Однак сам факт включення показника до моделі не означає, що він є універсальним або однаково значущим у всіх ситуаціях.

Більш складним підходом є логістична регресія, яка дозволяє оцінювати ймовірність належності спостереження до певного класу. За достатньої кількості якісних даних можуть використовуватися дерева рішень, random forest, gradient boosting та інші методи машинного навчання.

Для протидії торгівлі людьми ризик–скоринг доцільно орієнтувати на **ситуацію, подію, оголошення, територію або інший об'єкт аналізу**, а не на визначення «небезпечної» особи за її персональними характеристиками.

Це принципово важливе обмеження. Використання скорингової моделі для твердження, що конкретна людина має високу ймовірність бути злочинцем лише через її соціальні або особистісні характеристики, створює значні ризики дискримінації та помилкової класифікації. У правовому регулюванні ЄС цей ризик отримав безпосереднє нормативне відображення: AI Act забороняє використання AI для прогнозування ризику вчинення особою кримінального правопорушення, якщо таке прогнозування ґрунтується виключно на профілюванні особи або оцінюванні її особистісних характеристик; виняток стосується підтримки оцінювання, яке вже спирається на об'єктивні та перевірювані факти, безпосередньо пов'язані з кримінальною діяльністю.

Тому у сфері протидії торгівлі людьми більш обґрунтованим є скоринг **ризику події або ситуації**. Наприклад, система може оцінювати сукупність ознак конкретного оголошення про працевлаштування, території, маршруту або цифрового облікового запису. При цьому результат повинен визначати необхідність додаткової перевірки, а не встановлювати факт злочину.

Важливо також визначити порогові значення. Наприклад, низький рівень ризику може означати відсутність достатніх підстав для додаткових заходів, середній – необхідність аналітичної перевірки, високий – пріоритетність перевірки компетентними суб'єктами. Однак конкретні пороги повинні визначатися емпірично та перевірятися на реальних даних.

Якість скорингової моделі повинна оцінюватися за сукупністю показників, зокрема загальною точністю класифікації (accuracy), точністю позитивних прогнозів (precision), повнотою виявлення позитивних випадків (recall), гармонійним середнім між точністю та повнотою (F1-score), чутливістю (sensitivity) і специфічністю (specificity) залежно від характеру завдання. Для задач, у яких пропуск потенційно небезпечної ситуації має особливо високу ціну, недостатньо орієнтуватися лише на загальну точність класифікації (accuracy), оскільки цей показник може приховувати значну кількість невиявлених небезпечних випадків. У таких ситуаціях особливого значення набуває чутливість (sensitivity), яка характеризує здатність моделі правильно виявляти випадки, що становлять інтерес.

6.4.5. Машинне навчання для прогнозування

Машинне навчання розширює можливості прогнозування за рахунок автоматизованого виявлення закономірностей у великих масивах даних. У сфері протидії торгівлі людьми потенційними об’єктами аналізу можуть бути часові ряди, географічні дані, цифрові оголошення, мережеві зв’язки, фінансові характеристики та інші структуровані або неструктуровані дані.

Для задач класифікації можуть використовуватися логістична регресія (logistic regression), дерева рішень (decision trees), випадковий ліс (random forest), метод опорних векторів (support vector machines) та градієнтний бустинг (gradient boosting). Для виявлення груп схожих об’єктів застосовуються методи кластеризації (clustering). Для виявлення нетипової поведінки можуть використовуватися алгоритми виявлення аномалій (anomaly detection). Для аналізу текстової інформації застосовуються методи оброблення природної мови (natural language processing) та сучасні мовні моделі (large language models).

Вибір алгоритму повинен визначатися не його технологічною складністю, а характером задачі, обсягом і якістю даних та вимогами до пояснюваності. У правоохоронному контексті модель, яку неможливо належним чином перевірити або пояснити, може бути менш придатною навіть за умови високої прогнозної точності.

Ключовим етапом є формування навчальної вибірки. Якщо історичні дані містять систематичні помилки, неповноту або нерівномірність виявлення випадків, модель може відтворити ці недоліки. Наприклад, якщо в певному регіоні випадки торгівлі людьми краще виявлялися лише тому, що там діяла активніша система контролю, модель може помилково інтерпретувати регіональну особливість виявлення як характеристику реального ризику.

Проблемою є також дисбаланс класів. Реальні випадки торгівлі людьми становлять відносно невелику частину загальної кількості всіх досліджуваних подій або цифрових повідомлень. У такій ситуації модель може демонструвати високу загальну accuracy, водночас погано виявляючи саме рідкісні події, які становлять найбільший інтерес для правоохоронної діяльності.

Необхідним є розділення даних на навчальну, валідаційну та тестову вибірки. Для часових даних випадкове перемішування спостережень може бути методологічно неправильним, оскільки інформація з майбутнього не повинна використовуватися для прогнозування минулого. Тому для часових моделей доцільніше використовувати часову валідацію.

Особливе значення має контроль перенавчання. Модель може дуже добре описувати навчальні дані, але погано працювати на нових спостереженнях. Тому реальна ефективність прогнозування повинна оцінюватися на даних, які модель не використовувала під час навчання.

Окремою проблемою є concept drift – зміна закономірностей у часі. У сфері торгівлі людьми вона особливо актуальна через зміну платформ, способів вербування, міграційних процесів, законодавства та поведінки злочинців. Модель, яка була ефективною кілька років тому, може втратити прогнозну здатність після зміни криміногенного середовища.

Отже, машинне навчання слід розглядати не як одноразово створений алгоритм, а як компонент життєвого циклу аналітичної системи. Такий цикл повинен включати формування даних, їх очищення, навчання, валідацію, тестування, моніторинг якості, виявлення деградації та періодичне оновлення моделі.

NIST AI Risk Management Framework підкреслює необхідність управління ризиками AI протягом життєвого циклу системи, а серед характеристик надійного AI називає валідність і надійність, безпечність, стійкість, підзвітність, прозорість, пояснюваність, інтерпретованість, захист приватності та управління шкідливими проявами упередженості [77, 78].

6.4.6. Пояснюваний штучний інтелект (Explainable AI) у прогнозуванні

Застосування машинного навчання у протидії торгівлі людьми породжує питання не лише прогнозної точності, а й пояснюваності отриманого результату. Якщо система визначає певну територію, оголошення або ситуацію як таку, що має підвищений ризик, користувач повинен мати можливість зрозуміти, які фактори вплинули на відповідний результат.

Explainable AI (XAI) являє собою сукупність підходів, спрямованих на забезпечення зрозумілого для людини представлення причин або факторів, пов’язаних із результатом роботи AI–системи. NIST розмежовує explainability та interpretability: перша стосується представлення механізмів функціонування системи, тоді як друга – можливості осмислити значення результату в контексті призначення системи.

Для прогнозування ризиків торгівлі людьми це має особливе значення. Користувачеві недостатньо повідомити, що певна ситуація отримала, наприклад, високий прогнозний бал. Необхідно показати, які характеристики зробили найбільший внесок у цей результат.

Для відносно простих моделей пояснення може бути безпосередньо пов’язане зі структурою моделі. Наприклад, у логістичній регресії можна проаналізувати коефіцієнти ознак. У дереві рішень можна простежити послідовність умов, яка привела до класифікації.

Для складніших моделей можуть використовуватися локальні та глобальні методи пояснення. Локальне пояснення характеризує причини конкретного прогнозу для одного об’єкта, тоді як глобальне пояснення допомагає зрозуміти загальну логіку поведінки моделі. До поширених методів належать LIME та SHAP, хоча їх результати також потребують обережної інтерпретації.

Особливо важливим є питання стабільності пояснення. Якщо незначна зміна вхідних даних призводить до суттєвої зміни пояснення без зміни самого прогнозу, користувач може отримати хибне уявлення про причини рішення. Тому XAI не слід сприймати як абсолютну гарантію правильності моделі.

Пояснюваність також не усуває проблему упередженості даних. Модель може цілком прозоро показувати, що певна ознака суттєво впливає на прогноз, але це не означає, що використання такої ознаки є справедливим або правомірним. Наприклад, якщо модель систематично пов’язує високий ризик із характеристиками певної соціальної або демографічної групи, необхідно встановити, чи має така залежність реальне кримінологічне обґрунтування, чи вона є наслідком упередженості навчальних даних.

Саме тому Explainable AI повинна розглядатися у ширшому контексті управління штучним інтелектом (AI governance). NIST підкреслює, що пояснюваність і інтерпретованість сприяють моніторингу, документуванню, аудиту та управлінню AI–системами, але самі по собі не гарантують їхньої надійності.

Для правоохоронного застосування доцільно передбачати щонайменше чотири рівні пояснення: пояснення для аналітика, який безпосередньо працює з моделлю; пояснення для керівника, який використовує результат для прийняття рішення; технічне пояснення для розробника або аудитора; та документування моделі для контролю її функціонування протягом життєвого циклу.

Важливо також забезпечити принцип human–in–the–loop. Прогнозна система повинна формувати аналітичний результат, який оцінюється уповноваженим фахівцем. Людина повинна мати можливість відхилити або скоригувати аналітичний висновок, якщо має додаткову інформацію, яка не була врахована моделлю.

Особливо небезпечним є використання прогнозної системи за принципом «алгоритм визначив – отже, це правда». У правоохоронній сфері прогнозний результат має статус аналітичної інформації та потребує перевірки. Він може

бути підставою для визначення пріоритету аналітичної роботи, але не повинен автоматично породжувати негативні юридичні наслідки для особи.

Це відповідає загальному підходу сучасного регулювання AI у правоохоронній сфері. В AI Act ЄС підкреслено необхідність особливої обережності щодо систем, які використовуються для прогнозування злочинності або оцінювання ризиків щодо фізичних осіб, з огляду на ризики для фундаментальних прав, презумпції невинуватості, недискримінації та права на ефективний правовий захист.

Таким чином, Explainable AI у системах прогнозування торгівлі людьми виконує не декоративну, а функціональну роль. Пояснюваність необхідна для перевірки логіки моделі, виявлення помилок, контролю упередженості, забезпечення аудиту та підтримки обґрунтованого рішення людини.

Узагальнюючи, прогнозування ризиків торгівлі людьми доцільно розглядати як багаторівневу аналітичну систему, що поєднує часовий, просторовий, технологічний, мережевий та статистичний компоненти. На першому рівні здійснюється збір і нормалізація даних; на другому – виявлення тенденцій і факторів ризику; на третьому – формування прогнозних моделей; на четвертому – оцінювання їхньої точності та стабільності; на п’ятому – інтерпретація результатів фахівцем та визначення подальших дій.

Принциповим є перехід від ідеї «передбачення злочинця» до **прогнозування ризикового середовища**. Система може прогнозувати, де і коли можуть виникати підвищені ризики, які способи вербування набувають поширення, які цифрові канали демонструють аномальну активність, які сегменти мережі стають більш активними та які ситуації потребують додаткової перевірки. Такий підхід є методологічно безпечнішим і водночас практично кориснішим.

Отже, прогнозування ризиків торгівлі людьми повинно ґрунтуватися на поєднанні статистичного аналізу, просторового та часово́го моделювання, мережевого аналізу та машинного навчання. Водночас технологічна складність моделі не повинна підміняти якість даних і кримінологічну обґрунтованість.

Основними критеріями придатності прогнозної системи мають бути валідність, відтворюваність, пояснюваність, стійкість до зміни середовища, контроль упередженості та можливість незалежної перевірки результатів.

Застосування таких систем має здійснюватися в межах законодавства про захист персональних даних, кримінального процесу та інформаційної безпеки. Прогнозний результат повинен використовуватися як інструмент підтримки аналітичного рішення, а не як автоматична підстава для втручання у права людини. Саме поєднання алгоритмічного прогнозування з професійною оцінкою фахівця, перевіркою первинних даних та належним документуванням створює передумови для відповідального використання AI у протидії торгівлі людьми.

6.5. Формування моделі раннього попередження

Формування моделі раннього попередження є логічним продовженням визначення факторів ризику, моделювання злочинних мереж та прогнозування ризиків торгівлі людьми. Її призначення полягає не у встановленні факту вчинення кримінального правопорушення, а у своєчасному виявленні змін у криміногенному середовищі, які можуть потребувати додаткового аналітичного дослідження, перевірки або превентивного реагування. Такий підхід відповідає загальній логіці протидії торгівлі людьми, закріпленій у законодавстві України, де протидія торгівлі людьми охоплює її попередження, боротьбу з нею, а також допомогу і захист осіб, які постраждали від торгівлі людьми [6].

Необхідність раннього виявлення ризиків зумовлена специфікою самого явища торгівлі людьми. Відповідно до статті 149 Кримінального кодексу України, кримінально караними є, зокрема, торгівля людиною, а також вербування, переміщення, переховування, передача або одержання людини з метою експлуатації за наявності передбачених законом способів впливу [2]. Отже, механізм злочинної діяльності може складатися з низки взаємопов'язаних дій, які розгортаються в часі та просторі. Це створює можливість для виявлення певних ознак ще до моменту, коли всі елементи злочинної діяльності стають очевидними.

Міжнародні документи також орієнтують на використання індикаторного підходу. UNODC зазначає, що набори індикаторів можуть застосовуватися для виявлення потенційних випадків торгівлі людьми, але наявність або відсутність окремого індикатора не доводить і не спростовує факту торгівлі людьми. Виявлені ознаки повинні спонукати до подальшого з'ясування обставин та, за необхідності, направлення інформації до відповідних механізмів реагування [79].

З огляду на це в межах запропонованої автором моделі раннього попередження доцільно розмежувати первинні дані, індикатори, агреговану оцінку ризику, порогові значення, попередження та професійну оцінку отриманого сигналу. Узагальнено таку послідовність можна представити:

$$D \rightarrow I \rightarrow A \rightarrow R \rightarrow T \rightarrow W \rightarrow H$$

де D – первинні дані (Data), I – індикатори (Indicators), A – їх агрегація (Aggregation), R – оцінювання ризику (Risk assessment), T – порогова класифікація (Thresholding), W – формування попередження (Warning), H – професійна оцінка людиною (Human assessment).

Запропонована послідовність є авторською концептуалізацією і не ототожнюється з окремою моделлю UNODC, NIST, OSCE чи іншої міжнародної організації. Її теоретичною основою є поєднання індикаторного підходу до виявлення торгівлі людьми [79], ризик–орієнтованого підходу до управління AI–системами [77; 80] та принципу людського нагляду за автоматизованими системами [81].

У такій системі первинні дані не повинні безпосередньо трансформуватися у висновок про наявність торгівлі людьми. Спочатку з них виділяються релевантні індикатори, після чого здійснюється їх контекстуалізація та агрегування. Такий підхід має особливе значення тому, що фактори вразливості є комплексними. Міжнародна організація з міграції (International Organization for Migration, IOM) розглядає вразливість як результат взаємодії особистих, ситуаційних та контекстуальних факторів, наголошуючи, що сама по собі окрема

характеристика людини не повинна автоматично трактуватися як фактор вразливості [82; 83].

Таким чином, система раннього попередження повинна орієнтуватися насамперед на **зміни та комбінації факторів**, а не на механічну класифікацію осіб. Її аналітичними об'єктами можуть бути території, маршрути, цифрові канали, оголошення, часові періоди, фінансові операції, мережеві зв'язки або інші об'єкти, для яких наявні законні підстави збору та аналізу інформації.

6.5.1. Слабкі сигнали та їх агрегація

Одним із ключових елементів раннього попередження є виявлення слабких сигналів – окремих змін або ознак, які самі по собі не дають достатніх підстав для висновку про існування значного ризику, але можуть набувати аналітичної значущості в поєднанні з іншими сигналами.

Індикаторний підхід UNODC підтверджує необхідність саме такого обережного трактування. У рекомендаціях щодо індикаторів торгівлі людьми зазначено, що окремі індикатори не є доказом факту торгівлі людьми, а їх сукупність може бути підставою для подальшого з'ясування обставин [79].

Слабким сигналом у межах запропонованої моделі може бути, наприклад, зміна інтенсивності публікацій оголошень про працевлаштування, поява нетипового маршруту, збільшення активності певного цифрового середовища, зміна характеру пропозицій щодо роботи за кордоном або одночасна поява декількох пов'язаних ознак. При цьому жодна з них не повинна автоматично інтерпретуватися як підтвердження торгівлі людьми.

Значення слабкого сигналу визначається передусім його контекстом. Один і той самий показник може мати різну кримінологічну значущість залежно від території, періоду, типу експлуатації, особливостей міграційного середовища та інших факторів. Саме тому просте використання абсолютних значень індикаторів є недостатнім.

У найпростішому варіанті агрегація може здійснюватися за допомогою зваженої суми:

$$S = \sum_{i=1}^{n} w_i x_i$$

де x_i – нормалізоване значення i–го індикатора, w_i – його вага, а S – інтегральна оцінка сигналу.

Вибір ваги індикаторів повинен бути обґрунтований. Вони можуть визначатися експертним шляхом, на основі статистичного аналізу або за допомогою моделей машинного навчання. При цьому експертна оцінка не повинна залишатися єдиним способом визначення ваги, якщо існують достатні масиви емпіричних даних для їх перевірки.

Окреме значення має нормалізація. Індикатори можуть вимірюватися у різних одиницях, мати різний масштаб і різну статистичну природу. Без приведення їх до порівнюваного масштабу один показник може непропорційно впливати на результат лише через особливості його одиниці вимірювання.

Доцільним є врахування не тільки поточного значення індикатора, а й його динаміки. У цьому випадку може використовуватися перша різниця:

$$\Delta x_t = x_t - x_{t-1}.$$

Якщо значення індикатора тривалий час залишається стабільним, воно може мати інше аналітичне значення, ніж швидке зростання цього показника. Водночас сама позитивна динаміка не повинна автоматично розцінюватися як негативна: необхідно враховувати сезонність, структурні зміни та інші фактори.

Агрегація слабких сигналів повинна передбачати контроль над дублюванням інформації. Якщо два індикатори фактично відображають один і той самий процес, їх механічне додавання може штучно збільшити оцінку ризику. Тому під час побудови моделі доцільно аналізувати взаємозалежність показників та інформаційну надлишковість ознак.

У системі раннього попередження доцільно також накопичувати історію сигналів. Слабкий сигнал, який не досяг порогу попередження в момент його виникнення, може набути значення при подальшому повторенні або поєднанні з іншими ознаками. Такий підхід дозволяє перейти від аналізу окремих подій до аналізу тенденцій.

6.5.2. Багатофакторна оцінка ризику

Багатофакторна оцінка ризику є етапом, на якому окремі індикатори об'єднуються у комплексну оцінку. Її необхідність випливає з багатокомпонентного характеру торгівлі людьми та різноманітності умов, у яких формується вразливість до експлуатації.

ІОМ у своїх дослідженнях наголошує на взаємодії особистих, ситуаційних та контекстуальних факторів вразливості. Зокрема, аналіз міграційних маршрутів показав можливість використання статистичних моделей для дослідження факторів, пов'язаних із вразливістю мігрантів до торгівлі людьми та експлуатації [82].

У загальному вигляді ризик може бути представлений як:

$$R=f(X_1, X_2,\ldots, X_n)$$

де $X_1, X_2,\ldots, X_n$ – сукупність факторів, а f – функція їх об'єднання.

До складу такої функції можуть входити соціально–економічні, міграційні, географічні, часові, цифрові, фінансові та мережеві характеристики. Конкретний набір факторів має визначатися метою моделі, наявністю якісних даних і результатами її валідації.

Принципово важливим є розмежування **оцінки ризику** та **встановлення факту злочину**. Навіть високий показник ризику не є доказом вчинення торгівлі людьми. Такий підхід узгоджується з індикаторами UNODC, де прямо зазначається, що сукупність індикаторів повинна слугувати підставою для подальшого з'ясування, а не автоматичного висновку про наявність торгівлі людьми [79].

У разі використання машинного навчання багатофакторна оцінка може набувати форми ймовірнісної моделі. Наприклад, для бінарної задачі можна використовувати:

$$P(Y=1|X),$$

де Y=1 означає наявність певної події або класу, визначеного в навчальній вибірці, а X – сукупність вхідних ознак. Однак навіть така ймовірність не повинна трактуватися як імовірність того, що конкретна особа є злочинцем або

жертвою, якщо модель не має відповідного правового та методологічного обґрунтування.

Особливо важливо уникати включення до моделі ознак, які є лише непрямими проксі для чутливих характеристик людини. Це може призводити до дискримінаційних результатів навіть за відсутності прямого використання відповідної характеристики.

Управління ризиками AI повинно охоплювати весь життєвий цикл системи. NIST AI RMF пропонує чотири взаємопов'язані функції – Govern, Map, Measure і Manage, причому управління ризиками має бути безперервним і здійснюватися протягом життєвого циклу AI–системи [77; 80].

Для системи раннього попередження це означає необхідність не лише побудувати модель, а й постійно оцінювати її якість, актуальність даних, стабільність результатів та характер помилок.

6.5.3. Порогові значення та рівні небезпеки

Порогове значення визначає момент, коли інтегральна оцінка ризику переходить у категорію, яка потребує додаткової аналітичної уваги. У найпростішому варіанті:

$$W = \begin{cases} 0, & R < T \\ 1, & R \geq T \end{cases}$$

де R – оцінка ризику, а T – порогове значення.

Однак для практичної системи раннього попередження доцільніше використовувати декілька рівнів. Наприклад, можна передбачити низький, підвищений, високий та критичний рівні. Їх конкретне значення має визначатися в процесі валідації моделі та з урахуванням організаційних процедур.

Низький рівень може відповідати типовому стану середовища та не потребувати спеціального реагування. Підвищений рівень може бути підставою для додаткового моніторингу. Високий – для пріоритетного аналітичного опрацювання. Критичний – для невідкладної перевірки відповідно до повноважень та встановлених процедур.

Такі категорії не повинні автоматично породжувати юридичні наслідки. Вони є засобом **пріоритизації аналітичної уваги**.

Вибір порогового значення повинен здійснюватися з урахуванням помилок першого та другого роду. Надмірно низький поріг збільшує кількість хибнопозитивних попереджень, тоді як надмірно високий може призвести до пропуску значущих сигналів.

Для систем, які використовуються у чутливій сфері протидії торгівлі людьми, особливого значення набуває оцінювання наслідків помилкових рішень. Порогове значення не може визначатися виключно за критерієм загальної математичної точності моделі. Необхідно також враховувати характер можливих наслідків помилок.

Доцільним є застосування динамічних порогів, що враховують базову поведінку відповідного середовища. Якщо певний показник традиційно збільшується у визначений період року, його сезонне зростання саме по собі не повинно розцінюватися як аномалія.

Використання базової лінії дозволяє порівнювати поточне значення показника не з абстрактним універсальним порогом, а з типовим станом конкретного середовища. Такий підхід особливо актуальний для просторового аналізу, де різні території можуть мати істотно відмінні базові характеристики.

Порогові значення також повинні періодично переглядатися. Зміна способів вербування, цифрових платформ, міграційних потоків або структури доступних даних може змінити статистичні характеристики середовища. NIST рекомендує передбачати постійний моніторинг і періодичний перегляд процесів управління ризиками та їх результатів [77].

6.5.4. Автоматизоване формування попереджень

Автоматизоване формування попереджень передбачає перетворення результатів аналітичної моделі на інформаційний сигнал для уповноваженого користувача. Важливо, щоб такий сигнал містив не тільки категорію ризику, а й інформацію, достатню для його подальшої професійної оцінки.

Мінімальний набір інформації може включати час формування сигналу, аналітичний об'єкт, основні індикатори, їх динаміку, рівень ризику, джерела даних та фактори, які найбільше вплинули на результат.

Такий підхід відповідає загальним принципам AI risk management, згідно з якими результати системи повинні бути придатними для інтерпретації та подальшого управління ризиком [77; 80]. NIST наголошує на необхідності визначення ролей і відповідальності, постійного моніторингу, вимірювання та управління ризиками AI–систем [77; 80].

Для протидії торгівлі людьми актуальність такого підходу посилюється цифровізацією злочинної діяльності. Europol зазначає, що Інтернет, соціальні мережі та мобільні застосунки використовуються злочинними мережами для вербування, реклами, контролю потерпілих та інших елементів злочинної діяльності [84].

Більш сучасні матеріали Europol фіксують використання цифрових інструментів для рекрутингу, реклами, експлуатації та контролю потерпілих, а також появу AI–generated advertisements і багатомовних кампаній у соціальних мережах [85]. У 2024 році спільна операція INTERPOL та OSCE також була спрямована на виявлення випадків торгівлі людьми, пов'язаних із соціальними мережами, застосунками та іншими цифровими платформами [86].

Тому автоматизоване попередження може бути особливо корисним для первинного опрацювання значних масивів відкритої цифрової інформації. Водночас результати такого аналізу повинні розглядатися як аналітичні сигнали, а не як самостійний доказ.

Доцільним є формування попередження у структурованому вигляді, наприклад:

$$W=\{O,T,R,C,E,S\},$$

де O – аналітичний об'єкт, T – час, R – оцінка ризику, C – основні фактори (causes), E – докази або інформаційні джерела (evidence), S – статус сигналу (status).

Така структура є авторською пропозицією щодо організації інформаційного сигналу. Її перевага полягає в тому, що користувач отримує не абстрактне повідомлення «ризик високий», а структурований набір інформації, який може бути перевірений.

Особливого значення набуває механізм агрегації повторних попереджень. Якщо одна й та сама тенденція породжує велику кількість повідомлень, система повинна мати можливість їх групувати. Інакше надмірна кількість повідомлень може зменшувати практичну цінність системи та створювати інформаційне перевантаження.

Доцільним є також встановлення життєвого циклу попередження: нове, опрацьовується, підтверджене, відхилене, очікує додаткових даних, неактуальне. Така класифікація дозволяє зберігати історію роботи із сигналом і використовувати її для подальшої оцінки якості моделі.

Важливою є можливість аудиту. Система повинна фіксувати, які дані та алгоритмічні правила стали підставою для формування попередження, коли воно було сформоване, хто його переглянув та який результат перевірки отримано. Це узгоджується з вимогами до реєстрації випадків та моніторингу, передбаченими сучасними підходами до управління високоризиковими AI–системами [81].

6.5.5. Human–in–the–Loop у системі раннього попередження

Human–in–the–Loop передбачає включення людини до циклу функціонування автоматизованої аналітичної системи таким чином, щоб алгоритмічний результат не замінював професійної оцінки, а забезпечував її інформаційною підтримкою.

Для запропонованої моделі це можна представити як:

$$D \rightarrow M \rightarrow W \rightarrow H \rightarrow F$$

де D – дані, M – алгоритмічна модель, W – попередження, H – людська оцінка, F – подальший результат.

Принцип людського нагляду має не лише методологічне, а й нормативне обґрунтування. Регламент ЄС 2024/1689 (AI Act) передбачає, що високоризикові AI–системи повинні розроблятися таким чином, щоб забезпечувати ефективний нагляд людини протягом їх використання. При цьому особи, яким доручено нагляд, повинні мати можливість розуміти можливості та обмеження системи, контролювати її функціонування, виявляти аномалії та уникати надмірної залежності від автоматизованого результату [81].

Особливо важливим є положення про **automation bias** – тенденцію надмірно покладатися на результат автоматизованої системи. AI Act прямо передбачає необхідність забезпечення умов, за яких особа, що здійснює нагляд, може правильно інтерпретувати результат, не покладатися на нього автоматично та, за необхідності, проігнорувати, скасувати або змінити алгоритмічний результат [81].

Для системи раннього попередження про торгівлю людьми це має принципове значення. Високий ризик, сформований алгоритмом, не повинен автоматично означати, що конкретна особа є потерпілою або причетною до злочину. Він має означати лише те, що певна сукупність даних відповідає встановленому моделлю патерну та потребує професійної перевірки.

NIST також наголошує на необхідності чіткого розмежування ролей людини та AI–системи. У спеціальному додатку до AI RMF зазначено, що математичне представлення складних соціальних явищ може призводити до втрати контексту, необхідного для розуміння індивідуальних та суспільних наслідків [80].

Це застереження безпосередньо стосується прогнозування ризиків торгівлі людьми. Соціальна поведінка, міграційні процеси та експлуатаційні відносини є складними явищами, які не можуть бути повністю представлені набором числових ознак. Тому алгоритмічний результат завжди повинен розглядатися у відповідному контексті.

Людський контроль доцільно забезпечувати на декількох етапах життєвого циклу системи. На етапі розроблення фахівці визначають мету моделі, набір індикаторів, обмеження та допустимі способи використання результатів. На етапі тестування оцінюється точність, стабільність та характер помилок. Під час експлуатації здійснюється перевірка попереджень, а після накопичення досвіду – аналіз результатів для вдосконалення моделі.

Доцільно передбачити щонайменше три основні результати людської оцінки сигналу: підтвердження релевантності, відхилення як хибного або

визначення необхідності отримання додаткової інформації. Така класифікація є авторською пропозицією щодо організації зворотного зв'язку в системі.

Результати людської перевірки можуть використовуватися для подальшого вдосконалення моделі. Якщо певний тип сигналів систематично відхиляється як хибнопозитивний, це може свідчити про необхідність зміни набору ознак, ваг або порогових значень. Водночас рішення людини також не можна автоматично вважати безпомилковим; тому дані зворотного зв'язку повинні проходити контроль якості.

Важливою є документованість людського рішення. Для кожного суттєвого попередження бажано фіксувати час його формування, використану версію моделі, основні індикатори, результат перевірки та подальший статус. Такий підхід забезпечує можливість ретроспективного аналізу ефективності системи.

В Україні необхідність розвитку відповідних аналітичних та цифрових спроможностей підтверджується практикою міжнародної підтримки Національної поліції України. OSCE реалізує проєкти, спрямовані на посилення спроможності українських правоохоронних органів протидіяти торгівлі людьми, у тому числі кіберзлочинам, та використовувати спеціалізоване програмне забезпечення й аналітичні інструменти [87]. Раніше OSCE також зазначала, що цифрові технології використовуються злочинцями на різних етапах торгівлі людьми – від вербування до контролю потерпілих та фінансових операцій [64].

Сучасні тенденції додатково підтверджують необхідність інтегрованого підходу. Europol у 2025 році відзначав використання злочинними мережами AI–generated оголошень, багатомовних рекрутингових кампаній, зашифрованих каналів комунікації та цифрових інструментів моніторингу потерпілих [85]. Водночас OSCE у 2026 році звернула увагу на використання віртуальних активів у пов'язаних із торгівлею людьми фінансових схемах та запропонувала red–flag indicators для виявлення відповідних фінансових слідів [68].

Отже, Human–in–the–Loop у системі раннього попередження повинен розглядатися не як формальний етап погодження автоматичного рішення, а як

механізм контролю якості, контекстуалізації та відповідального використання алгоритмічних результатів.

Узагальнено авторську модель раннього попередження можна представити як багаторівневий контур:

$$D \rightarrow I \rightarrow A \rightarrow R \rightarrow T \rightarrow W \rightarrow H \rightarrow F$$

де D – первинні дані; I – виділення індикаторів; A – їх агрегація; R – оцінка ризику; T – порівняння з пороговими значеннями; W – автоматизоване попередження; H – людська перевірка; F – подальший аналітичний або організаційний результат.

Перевагою запропонованого підходу є розмежування функцій автоматизованої системи та людини. Алгоритм здійснює масштабний пошук закономірностей, агрегує індикатори та визначає пріоритетні сигнали, тоді як людина здійснює їх контекстуальну інтерпретацію та приймає рішення щодо подальшого опрацювання.

При цьому раннє попередження не повинно ототожнюватися з «передбаченням злочинця» або автоматизованим встановленням винуватості. Застосування такої системи є найбільш обґрунтованим щодо процесів, територій, цифрових середовищ, маршрутів, мережевих взаємозв'язків та інших аналітичних об'єктів, для яких існує достатня доказова база та правові підстави для оброблення інформації.

Відповідно, головним результатом системи має бути не твердження про те, що злочин неодмінно відбудеться, а структурований сигнал про зміну рівня ризику, який дозволяє своєчасно спрямувати професійну увагу на відповідний об'єкт. Саме така інтерпретація відповідає індикаторному підходу UNODC, відповідно до якого виявлення індикаторів має вести до подальшого з'ясування обставин, а не автоматичного встановлення факту торгівлі людьми [79].

Таким чином, система раннього попередження може розглядатися як проактивний аналітичний контур, який поєднує виявлення слабких сигналів, багатофакторну оцінку ризику, порогову класифікацію, автоматизоване формування попереджень та людський контроль. Її ефективність визначається не

ступенем автоматизації як таким, а здатністю своєчасно виявляти релевантні зміни, мінімізувати хибні сигнали, забезпечувати інтерпретованість результатів та залишати остаточну професійну оцінку за уповноваженим фахівцем.

Саме такий підхід дозволяє технологічно розширити можливості кримінологічного прогнозування, не перетворюючи алгоритмічну оцінку ризику на автоматизоване рішення щодо конкретної людини. У цьому полягає принципова відмінність запропонованої моделі раннього попередження від спрощеного підходу до predictive policing, за якого прогнозний показник може помилково сприйматися як встановлений факт майбутньої кримінальної поведінки.

6.6. Концептуальна модель кримінологічної дата-аналітики

Сучасна протидія торгівлі людьми потребує переходу від переважно реактивного аналізу вже виявлених кримінальних правопорушень до системного опрацювання різнорідних даних, які характеризують криміногенне середовище, поведінку злочинних мереж, фактори вразливості, міграційні процеси, цифрову активність, фінансові потоки та просторово-часові закономірності. Такий підхід відповідає загальній тенденції цифровізації правоохоронної діяльності, у межах якої великі масиви даних використовуються для виявлення закономірностей, формування аналітичних гіпотез і підтримки прийняття рішень.

Під кримінологічною дата-аналітикою доцільно розуміти системну діяльність із отримання, інтеграції, очищення, структурування, аналізу та інтерпретації даних про злочинність, фактори її детермінації, суб'єктів злочинної діяльності та криміногенне середовище з метою виявлення закономірностей, оцінювання ризиків, прогнозування можливих змін і забезпечення інформаційної підтримки управлінських рішень.

У контексті торгівлі людьми дата-аналітика має специфічний характер, оскільки відповідне кримінальне явище формується під впливом соціальних, економічних, міграційних, геополітичних, цифрових та інших факторів. Крім того, значна частина сучасної злочинної діяльності переміщується в цифрове середовище. OSCE зазначає, що Інтернет, смартфони та цифрові платформи

використовуються для вербування, контролю потерпілих, переміщення коштів та розширення злочинних мереж, водночас ті самі технології можуть застосовуватися правоохоронними органами для виявлення та протидії торгівлі людьми [88].

UNODC у підготовці Global Report on Trafficking in Persons використовує як інформацію, що надходить від держав через спеціалізований опитувальник, так і офіційні дані, доступні у відкритих джерелах, включаючи звіти поліції, органів юстиції та національні звіти щодо торгівлі людьми [60]. Це демонструє принципову можливість побудови кримінологічної аналітики на основі інтеграції різних типів інформації.

Запропонована автором концептуальна модель кримінологічної дата–аналітики може бути представлена як послідовність:

$$D \rightarrow I \rightarrow A \rightarrow M \rightarrow P \rightarrow R \rightarrow U$$

де D – джерела даних (Data sources); I – інтеграція та підготовка даних (Integration); A – аналітична обробка (Analytics); M – моделювання (Modelling); P – прогнозування (Prediction); R – оцінювання ризику (Risk assessment); U – підтримка управлінського рішення (Decision support).

Ця схема є авторською концептуалізацією і не відтворює якогось одного існуючого стандарту або моделі. Її призначення полягає у поєднанні інформаційного, кримінологічного, статистичного та прогностичного компонентів в єдиний аналітичний контур.

Принциповим є те, що результатом такого контуру має бути не автоматичне встановлення факту злочину або винуватості конкретної особи, а формування аналітично обґрунтованої інформації про тенденції, ризики, взаємозв'язки та об'єкти, які потребують професійної уваги. Такий підхід відповідає сучасному ризик-орієнтованому підходу до використання штучного інтелекту та аналітичних систем. NIST визначає надійність, валідність, безпеку, прозорість, пояснюваність, захист приватності та управління шкідливими проявами упередженості як важливі характеристики надійних AI-систем [77].

6.6.1. Джерела даних

Першим рівнем кримінологічної дата-аналітики є формування сукупності джерел даних. Якість подальшого аналізу значною мірою визначається не лише алгоритмами, а й повнотою, достовірністю, актуальністю та правомірністю використання вихідної інформації.

Для аналізу торгівлі людьми доцільно розглядати декілька основних категорій даних: кримінально-правові та кримінологічні; оперативно-службові; міграційні; соціально-економічні; географічні; цифрові; фінансові; медійні та інші відкриті дані.

До кримінологічних даних належать відомості про зареєстровані кримінальні правопорушення, кримінальні провадження, способи вчинення злочинів, характеристики потерпілих і правопорушників, види експлуатації, маршрути переміщення, місця виявлення потерпілих та інші параметри, які можуть бути законно використані для кримінологічного аналізу.

Важливим джерелом є статистична інформація. Її використання дозволяє визначати динаміку виявлення кримінальних правопорушень, просторову концентрацію, часові закономірності та зміни структури злочинності. Водночас статистика зареєстрованих або виявлених випадків не може ототожнюватися з реальною поширеністю торгівлі людьми. На показники можуть впливати особливості виявлення, реєстрації, діяльності правоохоронних органів та доступності механізмів повідомлення.

UNODC під час формування глобальної бази даних використовує виявлені випадки торгівлі людьми як одиниці аналізу, поєднуючи кількісну та якісну інформацію [60]. Такий підхід демонструє важливість поєднання статистичних показників із характеристиками конкретних випадків.

Окрему групу становлять міграційні дані. Вони можуть характеризувати напрямки переміщення населення, інтенсивність міграційних потоків, перетин кордонів, зміни маршрутів та інші процеси, що мають кримінологічне значення. Що стосується України, то особливого значення набувають вимушене переміщення населення, переміщення за кордон та зміна соціально–економічних

умов. OSCE звертає увагу на те, що війна, переміщення населення, скорочення доходів і робочих місць підвищують вразливість до торгівлі людьми [87].

Соціально-економічні дані можуть включати показники зайнятості, доходів, безробіття, демографічної структури, доступності соціальних послуг та інших характеристик територій. Їх доцільно використовувати переважно на агрегованому рівні, оскільки метою кримінологічної аналітики є виявлення закономірностей середовища, а не автоматична оцінка окремих осіб за соціальними характеристиками.

Принципово важливу групу становлять геопросторові дані. Вони дають можливість аналізувати розподіл подій, маршрути, територіальні кластери, близькість до транспортної інфраструктури та інші просторові характеристики. Поєднання просторових і часових параметрів дозволяє переходити від статичної карти подій до аналізу динаміки криміногенних процесів.

Цифрові дані набувають дедалі більшого значення. До них можуть належати законно доступні відомості з вебсайтів, соціальних мереж, платформ оголошень, цифрових комунікацій та інших онлайн-середовищ. OSCE зазначає, що технології використовуються злочинцями на різних етапах торгівлі людьми, а правоохоронні органи, своєю чергою, можуть використовувати технологічні інструменти для виявлення та аналізу відповідних явищ [88].

Практичне значення цифрової аналітики підтверджується діяльністю правоохоронних органів. У лютому 2025 року Europol провів міжнародну операцію, орієнтовану на виявлення та припинення діяльності мереж торгівлі людьми, які використовували онлайн-платформи; у межах операції фахівці здійснювали моніторинг онлайн-платформ і перехресне зіставлення отриманої інформації з національними базами даних [89].

Фінансові дані можуть характеризувати рух коштів, підозрілі фінансові операції та інші економічні ознаки, пов'язані з діяльністю злочинних мереж. Вони особливо важливі для реконструкції економічної складової торгівлі людьми, оскільки фінансові операції можуть утворювати додатковий незалежний від цифрових комунікацій інформаційний слід.

Отже, джерела даних доцільно розглядати не ізольовано, а як взаємодоповнювальні компоненти. Найбільшу аналітичну цінність часто має не окремий набір даних, а можливість встановити взаємозв'язок між різними джерелами.

Водночас інтеграція даних повинна здійснюватися лише за наявності відповідної правової підстави, з дотриманням вимог щодо захисту персональних даних, інформаційної безпеки, доступу до інформації та визначеної мети її використання. NIST окремо відносить захист приватності до ключових характеристик надійних AI–систем [77].

6.6.2. Аналітичні рівні

Кримінологічна дата-аналітика повинна передбачати декілька рівнів опрацювання інформації. Однорівневий підхід, за якого всі дані безпосередньо подаються у прогнозну модель, ускладнює інтерпретацію результатів і підвищує ризик помилкових висновків.

На першому рівні доцільно здійснювати **описову аналітику**. Її завданням є встановлення того, що вже відбулося: кількості виявлених випадків, їх просторового розподілу, часової динаміки, типів експлуатації, характеристик злочинної діяльності та інших параметрів.

На другому рівні здійснюється **діагностична аналітика**, спрямована на встановлення можливих взаємозв'язків між явищами. Наприклад, аналіз може бути спрямований на визначення того, чи пов'язані зміни інтенсивності міграційного потоку з кількістю виявлених випадків, чи концентруються певні способи вербування на конкретних цифрових платформах, чи пов'язані між собою окремі учасники злочинних мереж.

Третій рівень становить **прогнозна аналітика**, яка використовує історичні дані для оцінювання ймовірності певних майбутніх подій або тенденцій. Саме на цьому рівні застосовуються статистичні моделі, часові ряди, просторові моделі та алгоритми машинного навчання.

Четвертий рівень – **прескриптивна або підтримувальна аналітика**, яка не обмежується прогнозом, а допомагає визначити можливі варіанти реагування.

Водночас для правоохоронної діяльності доцільніше говорити саме про підтримку прийняття рішення, а не про автоматичне формування рішення.

Узагальнено рівні можна представити як:

$$D \rightarrow Des \rightarrow Dia \rightarrow Pr \rightarrow Dec$$

де D – дані; Des – описова аналітика (descriptive analytics); Dia – діагностична аналітика (diagnostic analytics); Pr – прогнозна (предиктивна) аналітика (predictive analytics); Dec – підтримка прийняття рішень (decision support).

Значення такого розмежування полягає у забезпеченні логічної послідовності аналітичного процесу. Прогноз не повинен формуватися без розуміння вихідних даних та механізмів, які визначили історичну закономірність. Якщо статистичні дані відображають не лише реальні зміни злочинності, а й зміни інтенсивності її виявлення, це повинно враховуватися під час побудови прогнозної моделі.

Аналітичні рівні можуть також бути розподілені за масштабом. Макрорівень характеризує загальні тенденції торгівлі людьми та зміни криміногенного середовища. Мезорівень охоплює території, маршрути, організовані групи та цифрові середовища. Мікрорівень стосується окремих подій, взаємозв'язків, транзакцій або інших об'єктів аналізу.

Таке поєднання рівнів дозволяє уникнути помилки, за якої закономірності, встановлені для великої території або групи об'єктів, автоматично переносяться на конкретну людину. Результат аналізу на макрорівні не повинен автоматично трактуватися як характеристика конкретної особи.

6.6.3. Моделі прогнозування

Прогнозування є центральним елементом кримінологічної дата-аналітики, однак його ефективність безпосередньо залежить від якості даних, коректності постановки задачі та відповідності моделі характеру досліджуваного явища.

Для аналізу торгівлі людьми можуть застосовуватися декілька класів моделей. До найпростіших належать статистичні моделі часових рядів, які

дозволяють досліджувати тренди, сезонність та інші повторювані закономірності.

Для просторового прогнозування можуть застосовуватися моделі, які враховують координати або територіальні одиниці, просторову автокореляцію та взаємозв'язок між сусідніми територіями. Їх використання може бути доцільним для виявлення територій із підвищеною концентрацією відповідних подій.

Окрему групу становлять мережеві моделі. Вони дозволяють досліджувати зв'язки між суб'єктами, цифровими обліковими записами, телефонами, фінансовими операціями, подіями та іншими об'єктами. Такий підхід особливо важливий для торгівлі людьми, оскільки, за даними UNODC, значна частина виявлених злочинців діяла в межах організованих груп і мереж [62].

Машинне навчання може використовуватися для класифікації, регресії, кластеризації та виявлення аномалій. Для класифікаційної задачі модель може оцінювати ймовірність належності нового спостереження до певного класу:

$$P(Y=c|X),$$

де Y – цільова змінна, c) – відповідний клас, а X – набір ознак.

Для регресійної задачі прогнозується числове значення:

$$\hat{y} = f(x)$$

Виявлення аномалій дозволяє знаходити спостереження, які істотно відрізняються від типової поведінки. У контексті торгівлі людьми це потенційно може використовуватися для виявлення нетипової активності у цифровому середовищі, незвичайних мережевих зв'язків або змін у фінансовій поведінці.

Водночас складніші моделі не обов'язково є кращими. Для правоохоронної аналітики особливого значення набуває можливість пояснити, чому модель сформувала певний прогноз. NIST підкреслює важливість пояснюваності та інтерпретованості AI-систем, оскільки вони допомагають користувачам зрозуміти механізми роботи системи та значення її результатів [77].

Тому вибір моделі повинен здійснюватися не лише за показниками predictive performance. До критеріїв мають належати стабільність,

узагальнюваність, пояснюваність, стійкість до зміни даних, можливість аудиту та відповідність правовим обмеженням.

Окремою проблемою є зміна розподілу даних у часі. Модель, навчена на історичних даних, може втрачати точність у разі зміни способів вербування, цифрових платформ, міграційних маршрутів або інших умов. OSCE наголошує на швидкій трансформації технологічного середовища торгівлі людьми, включаючи використання нових цифрових інструментів та AI [88].

Отже, прогнозна модель повинна розглядатися як динамічний компонент системи, який потребує регулярної перевірки та, за необхідності, перенавчання.

NIST рекомендує документувати обмеження узагальнюваності моделі, регулярно оцінювати її валідність і надійність, відстежувати ризики у часі, а також перевіряти питання приватності, справедливості, прозорості та пояснюваності [90].

Таким чином, прогнозування у кримінологічній дата-аналітиці повинно розглядатися не як одноразове застосування алгоритму, а як безперервний цикл: підготовка даних – навчання – валідація – експлуатація – моніторинг – оцінювання помилок – оновлення моделі.

6.6.4. Механізм формування управлінського рішення

Кінцевим призначенням кримінологічної дата-аналітики є не саме прогнозування, а забезпечення обґрунтованої інформаційної підтримки управлінського рішення. Аналітична система повинна допомагати відповідальному працівнику визначити, на які процеси, території або об'єкти доцільно спрямувати подальшу увагу та які інформаційні дії можуть бути виправданими.

Механізм формування рішення можна представити як:

$$A \rightarrow R \rightarrow E \rightarrow H \rightarrow D$$

де A – аналітичний результат; R – оцінка ризику; E – професійна експертна оцінка; H – перевірка людиною (Human review); D – управлінське рішення.

Першим етапом є отримання аналітичного результату. Це може бути прогноз зміни рівня ризику, виявлений просторовий кластер, потенційний зв'язок між об'єктами, аномалія або інша закономірність.

Другим етапом є інтерпретація цього результату з позицій поставленої кримінологічної задачі. Наприклад, збільшення активності певного цифрового середовища не означає автоматично збільшення торгівлі людьми. Воно може бути наслідком сезонних процесів, зміни популярності платформи або інших не кримінальних причин.

Третій етап полягає у перевірці аналітичної гіпотези. На цьому етапі можуть використовуватися додаткові джерела даних, порівняння з попередніми періодами, мережевий аналіз, просторовий аналіз або інші методи.

Четвертим етапом є професійна оцінка. Особа, яка приймає рішення, повинна розуміти, на яких даних базується прогноз, які ознаки мали найбільший вплив, які існують обмеження моделі та наскільки результат є надійним.

П'ятим етапом є власне управлінське рішення. Воно може стосуватися зміни пріоритетів аналітичної роботи, проведення додаткового збору інформації, посилення профілактичних заходів, міжвідомчої координації або інших дій, які відповідають компетенції відповідного суб'єкта.

Принципово важливо, щоб прогнозна модель не підміняла управлінське рішення. NIST розглядає AI як соціотехнічну систему, ризики якої формуються не лише алгоритмом, а й організаційним та людським контекстом його використання [77; 90].

Важливим елементом є пояснення прогнозного результату. Для користувача системи недостатньо інформації «ризик – високий». Доцільно надати відповідь на питання, які фактори вплинули на оцінку, наскільки модель упевнена у прогнозі, які дані були використані та за яких умов результат може бути ненадійним.

Пояснюваність не повинна ототожнюватися з абсолютною прозорістю алгоритму. NIST розмежовує прозорість, пояснюваність та інтерпретованість: прозорість відповідає передусім на питання про те, що відбулося в системі,

пояснюваність – як було отримано результат, а інтерпретованість – яке значення цей результат має для користувача [90].

З огляду на це управлінський інтерфейс кримінологічної аналітичної системи доцільно будувати таким чином, щоб прогноз супроводжувався поясненням, контекстом, рівнем невизначеності та зазначенням обмежень.

Важливо також забезпечити зворотний зв'язок. Після прийняття рішення та отримання фактичного результату інформація про його наслідки повинна повертатися в аналітичний контур. Це дозволяє оцінювати, наскільки прогноз був правильним, які індикатори виявилися корисними, а які – створювали надмірну кількість хибних сигналів.

Таким чином формується замкнений цикл:

Дані→Аналіз→Прогнозування→Прийняття рішення→Результат→ Зворотний зв’язок

Саме наявність зворотного зв'язку відрізняє систему дата-аналітики від статичної інформаційної системи. Вона не лише накопичує дані, а й використовує результати практичного застосування для оцінювання та вдосконалення аналітичних моделей.

6.6.5. Обмеження та ризики прогнозної аналітики

Застосування прогнозної аналітики у сфері протидії торгівлі людьми має суттєві обмеження, які повинні враховуватися ще на етапі концептуального проєктування системи.

Першим обмеженням є **неповнота даних**. Торгівля людьми характеризується високим рівнем латентності, тому доступні правоохоронним органам дані відображають насамперед виявлені випадки. Це означає, що модель може навчатися не стільки на повній сукупності злочинів, скільки на закономірностях їх виявлення та документування.

Другим обмеженням є **selection bias** – упередженість вибірки. Якщо певні території, категорії потерпілих або типи злочинів виявляються частіше, модель може помилково інтерпретувати цю нерівномірність як реальну різницю рівня ризику.

Третім ризиком є **data drift**. Зміна кримінальних практик, цифрових платформ, способів вербування або соціально–економічного середовища може призвести до того, що закономірності, характерні для навчального періоду, перестануть відповідати сучасним умовам. OSCE фіксує швидку трансформацію технологічного компонента торгівлі людьми, включаючи використання нових технологій та AI [88].

Четвертим ризиком є **алгоритмічна упередженість**. Якщо історичні дані містять систематичні перекоси, модель може відтворювати їх або навіть посилювати. NIST прямо відносить fairness та управління шкідливими проявами bias до характеристик надійних AI–систем [77; 90].

П'ятим обмеженням є **помилкова причинність**. Кореляційний зв'язок між двома показниками не доводить, що один із них є причиною іншого. Для кримінологічного аналізу це особливо важливо, оскільки соціальні, економічні та кримінальні процеси можуть одночасно змінюватися під впливом третього фактора.

Шостим ризиком є **automation bias** – надмірна довіра користувача до алгоритмічного результату. Чим вищий авторитет системи у сприйнятті користувача, тим більшою може бути небезпека некритичного прийняття її прогнозу. Тому результат моделі повинен супроводжуватися інформацією про його невизначеність та обмеження.

Сьомим ризиком є **порушення приватності та неправомірне використання персональних даних**. Інтеграція великих масивів даних може створювати можливості для формування детальних цифрових профілів. Навіть якщо окремі набори даних не містять очевидно чутливої інформації, їх поєднання потенційно може дозволити отримати додаткові висновки про особу. NIST розглядає privacy як окрему характеристику надійності AI–систем і рекомендує оцінювати пов'язані з нею ризики [77; 90].

Восьмим обмеженням є **пояснюваність складних моделей**. Висока predictive performance не гарантує можливості зрозуміти причину конкретного прогнозу. Це створює проблеми для аудиту, контролю та практичного

використання результатів. NIST наголошує, що пояснюваність та інтерпретованість сприяють належному розумінню результатів AI–систем, їх моніторингу, документуванню та управлінню [90].

Дев'ятим ризиком є **feedback loop**. Якщо результати прогнозної системи використовуються для визначення пріоритетів правоохоронної діяльності, це може впливати на те, де саме в майбутньому здійснюватиметься виявлення правопорушень. Отримані таким чином нові дані можуть знову потрапити до моделі та посилити початкову тенденцію. Тому необхідний постійний контроль за тим, чи не створює сама система штучне підтвердження власних прогнозів.

Десятим ризиком є **кібербезпека аналітичної системи**. Компрометація джерел даних, підміна інформації, несанкціонований доступ або маніпулювання моделлю можуть безпосередньо впливати на результати прогнозування. NIST включає безпеку та стійкість до ключових характеристик надійних AI-систем [77].

Одинадцятим обмеженням є **залежність від якості розмітки даних**. Якщо для навчання моделі використовуються історичні випадки, їх класифікація повинна бути послідовною. Різні підходи до кваліфікації, реєстрації або документування можуть створювати шум у навчальній вибірці.

Дванадцятим обмеженням є **небезпека редукціонізму**, тобто зведення складного кримінологічного явища до набору числових показників. Торгівля людьми залежить від соціального контексту, взаємодії людей, економічних умов, міграційних процесів та інших факторів, які не завжди можуть бути адекватно представлені у формі структурованих даних. Саме тому AI-систему доцільно розглядати як компонент соціотехнічної системи, а не як автономний механізм встановлення істини [77].

Особливо важливо забезпечити принцип **пропорційності аналітичного втручання**. Чим більш чутливими є дані та чим більш значними можуть бути наслідки помилки, тим вищими повинні бути вимоги до обґрунтованості, точності, пояснюваності та людського контролю.

Таким чином, кримінологічна дата-аналітика не повинна розглядатися як заміна кримінологічному аналізу, оперативній роботі чи професійному рішенню. Її призначення полягає у розширенні аналітичних можливостей шляхом оброблення значних масивів різнорідних даних, виявлення прихованих закономірностей, формування прогнозів та своєчасного інформування уповноважених суб'єктів.

У контексті торгівлі людьми така модель є особливо перспективною через одночасне існування традиційних і цифрових форм злочинної діяльності. Europol демонструє практичну цінність поєднання OSINT, аналітичних можливостей та перехресного зіставлення інформації з різних баз даних під час протидії онлайн–мережам торгівлі людьми [90]. OSCE, своєю чергою, підкреслює двоїстий характер технологій: вони можуть використовуватися злочинцями для вербування, контролю та переміщення незаконних доходів, але водночас створюють нові можливості для правоохоронних органів [63; 88].

Отже, запропонована концептуальна модель кримінологічної дата–аналітики може бути визначена як **інтегрований соціотехнічний контур**, у якому різнорідні дані перетворюються на аналітичні знання, аналітичні знання – на прогнози та оцінки ризику, а результати прогнозування – на інформаційну основу для професійного управлінського рішення. Її принциповими характеристиками повинні бути багатоджерельність даних, багаторівневість аналізу, валідація прогнозних моделей, пояснюваність результатів, захист приватності, контроль алгоритмічних упереджень, кіберстійкість та обов'язкова участь людини у прийнятті значущих рішень.

У такій конструкції технологія виконує функцію **інструмента кримінологічного пізнання та підтримки рішення**, а не самостійного суб'єкта прийняття рішення. Саме це дозволяє поєднати можливості сучасної дата–аналітики з принципами законності, обґрунтованості та відповідального використання цифрових технологій у протидії торгівлі людьми.

Висновки до розділу 6

Проведений у розділі аналіз дає підстави розглядати сучасну торгівлю людьми як динамічне та багатофакторне кримінальне явище, механізми якого поєднують традиційні способи вербування, переміщення та експлуатації з мережевими, транскордонними й цифровими формами організації злочинної діяльності. Цифрове середовище не змінює сутності торгівлі людьми, однак істотно розширює можливості злочинців щодо пошуку потенційних потерпілих, формування довіри, здійснення психологічного контролю, організації окремих форм експлуатації та переміщення незаконних доходів. Водночас цифрові технології формують додаткові можливості для правоохоронної діяльності, оскільки електронні комунікації, цифрові оголошення, метадані, фінансові операції та інші цифрові сліди можуть використовуватися для виявлення зв'язків між учасниками злочинної діяльності та документування її окремих елементів.

Встановлено, що ризик торгівлі людьми має багатофакторний характер і не може визначатися за одним показником. Соціально-економічні, міграційні та геополітичні, цифрові, поведінкові, просторово-часові й фінансові фактори набувають кримінологічного значення передусім у їх взаємозв'язку та конкретному контексті. У зв'язку з цим доцільним є формування комплексної системи індикаторів ризику, яка використовується не для автоматичного встановлення факту торгівлі людьми або статусу потерпілої особи, а для первинного виявлення ситуацій, що потребують додаткової перевірки, захисту та, за наявності відповідних підстав, подальшого кримінального розслідування.

Обґрунтовано доцільність застосування мережевого підходу до кримінологічного аналізу торгівлі людьми. Представлення злочинної діяльності у вигляді мережі дає змогу досліджувати не лише окремих учасників, а й функціональні, комунікаційні, фінансові, транспортні та інші зв'язки між ними. При цьому особливого значення набуває розмежування встановлених і припущених зв'язків, оскільки аналітична кореляція не може ототожнюватися з доведеною кримінальною причетністю. Таким чином, мережеве моделювання доцільно розглядати як інструмент упорядкування та аналізу інформації, який

доповнює, але не замінює оперативну діяльність, доказування та процесуальне розслідування.

Дослідження можливостей прогнозування показало, що кримінологічна дата-аналітика має охоплювати описовий, діагностичний, прогнозний та рекомендаційний рівні. Їх послідовне поєднання забезпечує перехід від встановлення того, що вже відбулося, через виявлення взаємозв'язків і закономірностей до оцінювання можливих майбутніх змін та підтримки прийняття рішень. Для прогнозування ризиків торгівлі людьми можуть застосовуватися статистичні методи, аналіз часових рядів, просторове та мережеве моделювання, а також методи машинного навчання. Водночас вибір алгоритму повинен визначатися не його технологічною складністю, а характером завдання, якістю та обсягом даних, можливістю валідації та вимогами до пояснюваності результатів.

Показано, що застосування машинного навчання у сфері протидії торгівлі людьми потребує постійного контролю якості та актуальності моделей. Особливими ризиками є перенавчання, помилки першого та другого роду, зміна закономірностей у часі (concept drift), а також можливість некоректної інтерпретації прогнозного результату. Тому модель повинна розглядатися не як одноразово створений алгоритм, а як компонент життєвого циклу аналітичної системи, що передбачає формування та очищення даних, навчання, валідацію, тестування, моніторинг якості, виявлення деградації та періодичне оновлення.

Обґрунтовано концепцію системи раннього попередження як проактивного аналітичного контуру, що поєднує виявлення слабких сигналів, багатофакторне оцінювання ризику, порогову класифікацію, формування попереджень і професійний людський контроль. Принциповим є те, що рівень ризику має визначати пріоритет аналітичної уваги, а не автоматично породжувати юридичні наслідки. Застосування такого підходу дає змогу уникнути ототожнення прогнозної оцінки з установленим фактом майбутньої кримінальної поведінки та відмежувати запропоновану модель від спрощених форм predictive policing.

Установлено, що Human-in-the-Loop є необхідним компонентом відповідального використання аналітичних та AI-систем у протидії торгівлі людьми. Людина повинна брати участь не лише у фінальній перевірці сигналу, а й у визначенні цілей моделі, виборі індикаторів, встановленні обмежень її застосування, оцінюванні якості та аналізі помилок. Алгоритмічний результат при цьому має виконувати функцію інформаційної підтримки професійного рішення, а не замінювати його. Такий підхід знижує ризик автоматизованого прийняття рішень щодо конкретної особи.

Узагальнення результатів дослідження дає змогу сформувати концептуальну модель кримінологічної дата-аналітики торгівлі людьми як циклічного процесу, у якому різнорідні дані інтегруються, очищуються та структуруються для подальшого описового, діагностичного, прогнозного й підтримувального аналізу. Результати такого аналізу мають використовуватися для виявлення факторів ризику, встановлення мережевих зв’язків, прогнозування можливих змін криміногенного середовища та формування інформаційних сигналів для уповноважених суб’єктів. При цьому отримані результати повинні проходити професійну перевірку та формувати зворотний зв’язок для подальшого вдосконалення аналітичної моделі.

Водночас ефективність кримінологічної дата-аналітики безпосередньо залежить від якості, повноти, актуальності та законності отримання даних. Інтеграція інформації з різних джерел має здійснюватися лише за наявності відповідної правової підстави, з дотриманням вимог щодо захисту персональних даних, інформаційної безпеки та визначеної мети використання інформації. Не менш важливими є пояснюваність аналітичних результатів, можливість їх незалежної перевірки, контроль упередженості та документування процесу формування прогнозу або попередження.

Отже, кримінологічна дата-аналітика створює методологічні та технологічні передумови для переходу від переважно реактивного опрацювання вже виявлених випадків торгівлі людьми до проактивного виявлення факторів ризику, змін у злочинному середовищі та нових способів вербування й

експлуатації. Її практична цінність полягає не в автоматизації правоохоронного рішення, а у своєчасному формуванні обґрунтованих аналітичних сигналів, виявленні прихованих взаємозв'язків і підтримці професійної діяльності уповноважених суб'єктів. Саме поєднання багатофакторного аналізу, мережевого моделювання, прогнозних методів, систем раннього попередження та Human-in-the-Loop формує основу відповідального застосування сучасних інформаційних технологій у протидії торгівлі людьми.

РОЗДІЛ 7. ЦИФРОВІ ТЕХНОЛОГІЇ У ПРОФІЛАКТИЦІ ТОРГІВЛІ ЛЮДЬМИ ТА ЗАХИСТІ ПОСТРАЖДАЛИХ

Цифрове середовище істотно змінило не лише способи комунікації, працевлаштування, навчання чи переміщення, а й саму логіку профілактики торгівлі людьми. Значна частина рішень, які потенційно можуть впливати на безпеку людини, нині приймається після контакту з інформацією в соціальних мережах, месенджерах, на платформах оголошень, сайтах роботодавців або через приватне листування. Водночас цифрові технології мають подвійний потенціал: вони використовуються для вербування, контролю та експлуатації людей, але водночас створюють нові можливості для профілактичного інформування, звернення по допомогу, перенаправлення до відповідних служб і підтримки постраждалих [91].

Зміна підходів до профілактики відображена і в сучасному європейському законодавстві. Директива (ЄС) 2024/1712 вимагає приділяти спеціальну увагу онлайн-виміру торгівлі людьми, використовувати Інтернет для інформаційних та освітніх заходів і розвивати цифрову грамотність та навички, особливо серед дітей і осіб з інвалідністю [92]. Важливо, що цифрова профілактика тут розглядається не як окремий інформаційний канал, а як частина ширшої системи запобігання експлуатації.

Для України така логіка особливо актуальна в умовах тривалої війни, внутрішнього та зовнішнього переміщення населення, пошуку роботи за межами постійного місця проживання та активного використання цифрових платформ для вирішення побутових і професійних питань. У Плані реагування МОМ на кризу в Україні на 2025 рік передбачено національну безкоштовну консультативну лінію 527, загальнонаціональні інформаційні кампанії, цільові профілактичні заходи серед молоді та осіб, найбільш уразливих до експлуатації, а також розвиток безпечних механізмів перенаправлення до відповідних служб [93]. План також передбачає ведення випадку (case management), психологічну, правову, медичну, матеріальну, професійну та реінтеграційну підтримку постраждалих [93].

Профілактику й захист недоцільно розглядати як два ізольовані напрями. Між профілактичним інформуванням і захистом постраждалої особи формується послідовний маршрут: отримання інформації, перевірка сумнівної ситуації, звернення по консультацію, перенаправлення до відповідної служби та, за потреби, подальша підтримка. Саме цифрові засоби здатні скоротити відстань між цими етапами, але водночас створюють додаткові ризики для приватності, конфіденційності та автономії постраждалої особи.

У попередніх розділах монографії цифрові технології розглядалися переважно як засоби виявлення, аналітики, документування та інформаційної взаємодії суб'єктів протидії торгівлі людьми. У цьому розділі фокус зміщується на саму людину – її інформування, можливість безпечного звернення, доступ до допомоги, цифрову безпеку та відновлення автономії.

7.1. Трансформація профілактики торгівлі людьми в умовах цифрового середовища

Традиційна профілактика торгівлі людьми тривалий час була зорієнтована на інформаційні кампанії, просвітницькі заходи, друковані матеріали, гарячі лінії та безпосередню роботу з групами, які вважалися уразливими. Ці інструменти залишаються важливими, однак цифровізація змінила момент, у який людина стикається з потенційно небезпечною пропозицією.

Пошук роботи, житла, транспортних послуг, допомоги з документами або переїздом дедалі частіше починається з цифрового оголошення, рекомендації в соціальній мережі, повідомлення в месенджері чи сайту посередника. Відповідно, профілактична інформація має бути доступною саме в тих цифрових середовищах, де користувач фактично приймає рішення.

Це змінює саму форму профілактичного впливу. Загальне попередження про небезпеку поступово доповнюється ситуаційною підтримкою, коли людина отримує відповідь не лише на питання про існування ризику, а й про конкретний безпечний наступний крок.

Саме така логіка закладена у сучасних європейських підходах. Директива (ЄС) 2024/1712 прямо пов'язує профілактику з онлайн-виміром, інформаційними

та освітніми заходами через Інтернет, а також із розвитком цифрової грамотності [92]. Саме перенесення традиційної пам’ятки на вебсторінку ще не створює цифрової профілактики. Її зміст, формат і канал мають відповідати реальним сценаріям поведінки користувача.

Одним із ключових зрушень є перехід від інформаційної кампанії до багатоканальної моделі. Соціальна мережа може привернути увагу, офіційний сайт – дати перевірену інформацію, месенджер – забезпечити коротку консультацію, телефонна лінія – підтримати людину без доступу до стабільного Інтернету, а спеціалізований сервіс – перенаправити її до відповідної служби. МОМ у Плані реагування на кризу в Україні на 2025 рік саме так поєднує інформаційні кампанії, національну лінію 527, ранню профілактику, безпечні механізми перенаправлення та комплексну підтримку [93].

Цифровий формат водночас не є автоматично доступним. Користувач може мати лише мобільний пристрій, нестабільне інтернет-з’єднання або обмежені цифрові навички. Якщо профілактичний ресурс побудований як складний портал із багаторівневим меню, довгими текстами й обов’язковою реєстрацією, він може виявитися менш корисним, ніж коротка мобільна сторінка з чітким алгоритмом дій.

Не менш важливим є питання довіри. У цифровому середовищі офіційний ресурс конкурує з приватними сайтами, анонімними каналами, сторінками у соціальних мережах і ресурсами, що можуть імітувати легітимні організації. Саме тому профілактичний сервіс повинен дозволяти користувачеві перевірити, хто є його власником, де розміщені офіційні контакти і як незалежно підтвердити автентичність цього каналу.

ОБСЄ у звіті 2024 року про політику реагування на технологічно опосередковану торгівлю людьми наголошує на необхідності залучення не лише державних органів, а й громадянського суспільства та приватного сектору [91]. Це має принципове значення, оскільки значна частина цифрового середовища, де відбуваються перші контакти, належить приватним платформам.

Залучення цифрових платформ до профілактики водночас не повинно перетворюватися на необґрунтоване профілювання користувачів. Пошук роботи за кордоном, перегляд профілактичних матеріалів або звернення до консультаційного сервісу самі по собі не є підставою для посиленого цифрового спостереження.

Важливою стає і багатомовність. Людина може перебувати за кордоном, не знати місцевої мови або не розуміти правової термінології. Ефективний цифровий ресурс має пояснювати не лише назви установ, а й їхні функції та доступні види допомоги.

Регіональний план МОМ для України та сусідніх держав на 2025 рік прямо передбачає надання адаптованої інформації про захист, трудову експлуатацію, трудові права, правовий статус та доступ до підтримки різними мовами й через різні канали – від індивідуального консультування та гарячих ліній до соціальних медіа й масових інформаційних кампаній [94].

Узагальнення розглянутих підходів дає підстави запропонувати людиноцентричну модель цифрової профілактики та підтримки, у якій цифрові технології не утворюють самостійної паралельної системи, а забезпечують послідовний маршрут від профілактичного інформування до відновлення автономії постраждалої особи. Такий маршрут охоплює шість взаємопов’язаних етапів: інформування, незалежну перевірку ситуації, безпечне звернення, первинну підтримку, погоджене перенаправлення та подальше відновлення. На всіх етапах мають діяти наскрізні принципи мінімізації даних, доступності, безпечності комунікації, поінформованої згоди та збереження людського контролю.



Рис. 7.1. Людиноцентрична модель цифрової профілактики торгівлі людьми та підтримки постраждалої особи.

Рисунок розроблено на основі узагальнення [91; 92–94; 95; 96].

Таким чином, цифрова трансформація профілактики полягає не у механічному перенесенні традиційних інструментів в онлайн, а у формуванні безперервного маршруту між інформацією, перевіркою ситуації та доступом до допомоги.

Це водночас визначає межу між профілактикою і кримінологічним прогнозуванням. У межах цього розділу цифрові засоби не розглядаються як інструменти присвоєння людині «рівня ризику» або побудови прогнозної моделі її поведінки. Завдання профілактики інше – надати інформацію й інструменти, які дозволяють прийняти більш усвідомлене рішення, не перекладаючи на саму людину відповідальність за злочинні дії торговців людьми.

7.2. Цифрові канали профілактичного інформування та запобігання вербуванню

Цифрове профілактичне інформування має найбільшу практичну цінність тоді, коли воно з'являється не після того, як людина вже опинилася в небезпечній ситуації, а під час пошуку роботи, житла, транспортних послуг, навчання, документального супроводу або інших можливостей. Саме в цей момент користувач взаємодіє з оголошеннями, соціальними мережами, месенджерами, сайтами посередників і приватними цифровими контактами. Тому профілактика повинна бути інтегрована у звичне інформаційне середовище, а не існувати окремо від нього.

Сучасні дані підтверджують, що цифрове вербування може мати цілком переконливий зовнішній вигляд. У **Global Report on Trafficking in Persons 2024** UNODC описано використання автоматизованих засобів для створення оманливих вакансій, які поширювалися через соціальні мережі та месенджери. В окремих випадках використовувалися назви, логотипи й інші елементи брендингу реальних компаній, що підвищувало правдоподібність пропозиції [60].

Актуальність такої моделі профілактики посилюється появою нових форм експлуатації, безпосередньо пов'язаних із цифровою економікою. У 2026 році ОБСЄ окремо звернула увагу на торгівлю людьми з метою примусової участі у шахрайських онлайн-операціях (cyber scam operations), де цифрові канали можуть використовуватися одночасно для вербування, переміщення комунікації у контрольоване середовище та подальшої експлуатації. Для профілактики це означає необхідність враховувати не лише традиційні пропозиції фізичної праці, а й дистанційну «роботу» у сфері онлайн-продажів, інвестицій, криптовалют, підтримки клієнтів та інших цифрових сервісів, якщо характер роботи й умови її виконання неможливо незалежно перевірити.

Це означає, що зовнішня професійність оголошення, якісний дизайн або посилання на відомий бренд не можуть самі по собі підтверджувати достовірність пропозиції. Профілактичний цифровий канал має не лише

повідомляти про можливий ризик, а й спрямовувати користувача до перевірених джерел, консультації або іншого безпечного наступного кроку.

7.2.1. Соціальні мережі, месенджери та вебресурси як канали профілактики

Соціальні мережі мають значний потенціал для профілактичного інформування, оскільки дозволяють працювати саме в тому середовищі, де користувач отримує пропозиції, рекомендації та приватні повідомлення. Проте їх використання не повинно обмежуватися публікацією плакатів або загальних гасел.

Більш практичним є ситуаційний контент, пов’язаний із конкретним рішенням користувача: працевлаштуванням, поїздкою, передачею документів або зверненням до посередника. Такий формат безпосередньо пов’язує профілактичну інформацію з конкретною дією.

Разом із тим соціальна мережа не перебуває під повним контролем організації, яка проводить профілактичну кампанію. Алгоритми платформи визначають, кому і як довго буде показано матеріал; профілактичний допис може швидко зникнути зі стрічки, тоді як емоційно приваблива або маніпулятивна пропозиція продовжуватиме поширюватися.

Соціальні мережі доцільно використовувати як точку входу до перевіреного ресурсу, а не як єдине місце зберігання критично важливої інформації. Користувач повинен мати можливість перейти на офіційний сайт, перевірити контакти організації та за потреби скористатися іншим каналом зв’язку.

Месенджери мають подвійне значення: вони широко використовуються для повсякденної комунікації і водночас можуть бути середовищем вербування та контролю [91]. У профілактичній роботі їх доцільно використовувати як канал короткої консультації, навігації та переходу до фахівця, а не лише для масових розсилок.

Проте тут виникає питання автентичності. Користувач повинен мати незалежний спосіб перевірити, що акаунт справді належить заявленій установі.

Автентичність консультаційного акаунта має підтверджуватися незалежним офіційним джерелом.

Чат-боти можуть бути корисними як навігаційний інструмент. Вони можуть допомогти знайти офіційний контакт, надати базову навігацію та спрямувати користувача до відповідної служби.

Проте бот не повинен імітувати професійну оцінку складної ситуації. Якщо користувач повідомляє про примус, утримання документів, обмеження свободи пересування, погрози або іншу безпосередню небезпеку, автоматизований сценарій має забезпечувати перехід до людини-фахівця, а не продовжувати стандартний діалог.

Окремого врахування потребує генеративний штучний інтелект. За оцінкою ОБСЄ та Regional Support Office of the Bali Process, такі технології можуть масштабувати обман, імітацію особи та масову персоналізовану комунікацію [66]. Для профілактичних сервісів це означає, що критично важлива інформація про документи, правовий статус, екстрені контакти або порядок звернення має надходити з перевіреної бази знань, а не залежати від неконтрольованої генерації.

Вебресурси мають іншу перевагу – вони можуть бути стабільною точкою доступу до офіційної інформації. Їхня функція полягає не лише у публікації довідкових матеріалів, а й у забезпеченні можливості перевірити факти: офіційні контакти, реєстраційні дані та інші відомості, які можна зіставити з незалежними джерелами.

При цьому ресурс не повинен створювати хибне враження, що автоматична перевірка здатна однозначно визначити, чи є пропозиція безпечною. У складних випадках цифровий інструмент може лише допомогти зібрати й зіставити факти.

7.2.2. Від загального попередження до незалежної перевірки

Одним із найважливіших принципів цифрової профілактики є незалежність джерела перевірки. Якщо особа, яка пропонує роботу, сама надсилає сайт, документи, номер телефону, профіль компанії та контакт

менеджера, всі ці елементи фактично походять із одного інформаційного ланцюга.

Резолюція Комісії ООН із запобігання злочинності та кримінального правосуддя 33/1 від 2024 року рекомендує державам розвивати цільові інформаційні кампанії щодо онлайн-торгівлі людьми, підвищувати цифрову грамотність і забезпечувати особам у вразливому становищі безпечний доступ до якісних онлайн-ресурсів. Документ також закликає до співпраці з громадянським суспільством, академічним середовищем і приватним сектором у протидії технологічно опосередкованій торгівлі людьми [62].

Це свідчить про те, що профілактика не може бути відповідальністю лише одного державного порталу. Вона має бути розподілена між різними суб'єктами, однак користувачеві при цьому потрібна зрозуміла ієрархія довіри: де офіційна інформація, де консультація, де сервіс платформи, а де лише приватна порада.

QR-коди та короткі мобільні посилання можуть бути корисними в пунктах перетину кордону, транспортних вузлах, центрах допомоги, закладах освіти та місцях тимчасового проживання. Однак QR-код сам по собі не підтверджує автентичність ресурсу, тому поруч доцільно зазначати офіційну назву установи або адресу вебресурсу, яку користувач може перевірити незалежно.

Спеціалізований мобільний застосунок не завжди є оптимальним каналом профілактики. Його встановлення потребує довіри, технічних ресурсів і певного рівня цифрової компетентності, а сама наявність такого застосунку на пристрої може розкривати характер інтересу користувача. Якщо ту саму функцію можна забезпечити через мобільний вебресурс, месенджер або телефонну лінію, окремий застосунок може бути зайвим.

Профілактичне інформування не повинно будуватися лише на страху. Повідомлення про найтяжчі форми експлуатації можуть привертати увагу, але не обов'язково допомагають прийняти конкретне рішення. Значно практичнішими є рекомендації, пов'язані з дією: що перевірити перед оплатою послуг посередника, що з'ясувати до передачі паспорта, яку інформацію залишити довіреній особі перед поїздкою.

Профілактичний цифровий сервіс не повинен також підміняти реальні соціальні або економічні альтернативи. Людина може усвідомлювати небезпеку пропозиції, але погодитися через відсутність житла, доходу, документів або інших реальних можливостей.

Тому ефективне інформування має бути пов’язане з доступом до підтримки: перевіреного працевлаштування, правової консультації, соціальної допомоги, тимчасового житла або іншого ресурсу, який дає людині реальну альтернативу ризикованій пропозиції.

Цифрові канали мають утворювати взаємопов’язану систему, у якій користувач може перейти від профілактичного повідомлення до офіційного ресурсу, консультації та, за потреби, допомоги. Ключовою є не кількість каналів, а безперервність цього маршруту.

Цифровий канал профілактики має підтримувати інформоване рішення користувача, а не створювати ілюзію автоматичного визначення “безпечної” чи “небезпечної” ситуації. Його завдання – забезпечити доступ до перевіреної інформації, консультації та подальшої допомоги.

Наступним рівнем профілактики є вже не сама наявність інформації, а здатність користувача правильно її оцінювати і застосовувати. Тому подальший аналіз стосується цифрової грамотності та формування навичок безпечної поведінки.

7.3. Цифрова грамотність і формування навичок безпечної поведінки

Цифрова грамотність у сфері профілактики торгівлі людьми не зводиться до вміння користуватися смартфоном, соціальними мережами чи електронними сервісами. Вона охоплює здатність перевіряти джерела інформації, оцінювати достовірність пропозицій, контролювати доступ до персональних даних і розпізнавати маніпулятивну комунікацію в ситуаціях, пов’язаних із працевлаштуванням, переміщенням, передачею документів або коштів.

Такий підхід безпосередньо підтримується сучасними міжнародними документами. У Резолюції Комісії ООН із запобігання злочинності та

кримінального правосуддя 33/1 від 2024 року державам рекомендовано розвивати цифрову грамотність і навчання безпечному та захищеному використанню технологій як засіб профілактики торгівлі людьми, особливо серед жінок, дітей та осіб, які перебувають у вразливому становищі. У документі також наголошено на необхідності забезпечувати таким особам рівний і безпечний доступ до віковоvідповідної інформації, відомостей про власні права та якісних онлайн-ресурсів [62].

Профілактична цифрова освіта має виходити за межі загального заклику «бути обережними в Інтернеті» і формувати конкретні навички перевірки інформації, обмеження необґрунтованої передачі даних та звернення до незалежного джерела у разі сумніву.

Базовою навичкою є незалежна перевірка. Якщо пропозиція роботи надійшла через соціальну мережу або месенджер, недостатньо орієнтуватися лише на сайт, контакти чи документи, надіслані самим співрозмовником. Доцільно окремо знайти офіційний ресурс компанії, перевірити її юридичну назву, контактні дані, умови працевлаштування та іншу доступну офіційну інформацію. Мета такої перевірки полягає не у самостійному встановленні факту злочину, а у зменшенні залежності від інформації, сформованої лише однією заінтересованою стороною.

Окремі ознаки не повинні автоматично трактуватися як підтвердження торгівлі людьми. Висока заробітна плата, швидка відповідь, спілкування через месенджер або пропозиція термінового виїзду самі по собі не мають достатньої доказової сили. Значення має сукупність обставин і можливість незалежно перевірити ключові елементи пропозиції. Такий підхід є методично коректнішим за використання спрощених переліків «червоних прапорців», які можуть створювати хибне відчуття визначеності.

У таких випадках цифрова грамотність має формувати навичку зупинитися й перевірити інформацію, а не автоматично кваліфікувати ситуацію як злочинну.

Окремого значення набуває перевірка цифрової ідентичності співрозмовника. Генеративний ШІ ускладнює використання звичних ознак

довіри, оскільки дозволяє створювати переконливі тексти, зображення, голосові повідомлення та інші матеріали, що імітують реальну особу [66]. Тому важливі рішення про поїздку, працевлаштування, передачу документів або коштів доцільно підтверджувати через незалежний канал.

Це означає, що переконливий текст, професійна фотографія профілю, голосове повідомлення або навіть окремий відеофрагмент не повинні автоматично сприйматися як беззаперечне підтвердження особи. Наприклад, контакт компанії доцільно знаходити самостійно через офіційний ресурс, а не використовувати номер, отриманий лише у приватному листуванні.

7.3.1. Персональні дані, документи та фінансова інформація

Одним із найпоширеніших практичних питань є передача персональних документів. Під час працевлаштування, навчання, оформлення проживання або поїздки людину можуть просити надати копії документів, контактні, ідентифікаційні або фінансові дані.

Сам по собі такий запит не обов’язково є неправомірним. Значення має інше: хто просить інформацію, на якому етапі, для якої мети і яким каналом вона передається.

Тому профілактичне навчання має відходити від занадто загальної формули «ніколи не надсилайте документи в Інтернеті». Вона мало придатна для реального життя, оскільки значна частина легітимних адміністративних і трудових процедур сьогодні справді відбувається дистанційно.

Кориснішим є інший принцип: передавати лише ті дані, які обґрунтовано потрібні для конкретної дії, після перевірки отримувача та призначення інформації.

Подібна логіка стосується фінансових даних. Важливо розрізняти реквізити, необхідні для отримання коштів, і дані, що забезпечують доступ до рахунку або підтвердження операції: пароль, PIN-код, одноразовий код чи засоби відновлення доступу.

У контексті торгівлі людьми це важливо не лише для запобігання шахрайству. Втрата контролю над фінансовими засобами може істотно посилити

залежність людини, обмежити її мобільність і здатність залишити небезпечне середовище.

Тому фінансова цифрова грамотність тут є складовою ширшої автономії.

7.3.2. Соціальна інженерія та маніпулятивна комунікація

Багато небезпечних цифрових контактів не потребують складного технічного зламу. Достатньо створити довіру, відчуття терміновості, особистої прихильності або виняткової можливості, а потім поступово підштовхнути людину до передачі даних чи прийняття рішення.

Саме тому цифрова грамотність має включати розуміння соціальної інженерії.

Тривалість онлайн-спілкування, регулярні повідомлення, голосові дзвінки чи фотографії не підтверджують реальну ідентичність співрозмовника. Генеративний ШІ додатково посилює цю проблему, оскільки спрощує персоналізовану комунікацію та підтримання великої кількості паралельних контактів [66].

Практичний принцип полягає у відокремленні довіри до співрозмовника від перевірки конкретних фактів: роботодавця, умов проживання, підстав платежу, маршруту або документів.

Таке мислення є практичнішим за намагання визначити «типову поведінку торговця людьми», оскільки цифрові сценарії швидко змінюються.

7.3.3. Безпечне користування акаунтами та цифровими каналами

До базових профілактичних навичок належить захист ключових облікових записів, насамперед електронної пошти, через яку часто відновлюється доступ до інших сервісів. На цьому рівні достатньо сформувати розуміння, що безпека акаунта залежить не лише від пароля, а й від багатофакторної автентифікації, активних сесій та засобів відновлення доступу.

Важливо також контролювати активні сесії та довірені пристрої. Людина може змінити пароль, але не помітити, що акаунт залишається відкритим на іншому пристрої або пов’язаний із резервною електронною адресою, до якої має доступ стороння особа.

Профілактична цифрова грамотність також передбачає усвідомлене користування геолокацією. Йдеться не про її постійне вимкнення, а про розуміння того, які застосунки і люди мають доступ до місцеперебування та з якою метою. Перед поїздкою доцільно окремо погодити з довіреною особою резервний спосіб зв'язку і залишити їй основні відомості про маршрут та місце перебування.

Такі прості резервні заходи особливо важливі тому, що смартфон може бути втрачений, пошкоджений або стати недоступним. Контакти консульської установи, служби допомоги чи близької людини не повинні існувати лише в одному пристрої.

7.3.4. Навчання без перекладання відповідальності на потенційну постраждалу особу

Однією з принципових методичних вимог є недопущення віктимблеймінгу. Чим більше профілактика концентрується на правилах безпечної поведінки, тим вищий ризик хибного висновку, що постраждала особа сама відповідальна за недостатню обережність.

Цифрова грамотність здатна зменшити частину ризиків, але не може гарантувати абсолютного захисту. Організатори торгівлі людьми можуть використовувати справжні документи, легітимні компанії як прикриття, складні психологічні механізми, фінансову залежність, соціальну вразливість, технології імітації особи або поєднання кількох таких засобів.

Тому профілактичні знання мають посилювати можливості людини, а не переносити на неї відповідальність за злочинні дії іншої сторони.

Такий підхід узгоджується з планами реагування МОМ для України та сусідніх держав на 2025 рік, де профілактичні освітні заходи поєднуються з інформаційними кампаніями, роботою лінії 527, безпечним перенаправленням, правовою підтримкою, питаннями трудових прав та етичного рекрутингу [4; 5]. Цифрова грамотність у такій моделі не є самоціллю: вона має бути пов'язана з реальною можливістю звернутися по допомогу.

Це принципово: цифрова грамотність ефективна лише тоді, коли людина має куди звернутися після того, як виявила сумнів або проблему.

Особливої уваги потребують діти та молодь. Резолюція 33/1 прямо вимагає ставити права й безпеку дітей і осіб у вразливому становищі в центр профілактичної політики та забезпечувати їх доступом до віковоvідповідної інформації й ресурсів з цифрової грамотності [62].

При цьому дитина, яка вправно користується соціальними мережами, не обов'язково має сформовану здатність оцінити грумінг, маніпулятивне спілкування або наслідки передачі інтимного контенту, документа чи геолокації.

Саме тому профілактичне навчання для дітей повинно бути сценарним і практичним: що робити, якщо незнайома людина просить перейти у приватний канал; до кого звернутися, якщо виник тиск; як припинити небажаний контакт; чому не потрібно самостійно «доводити», що ситуація є небезпечною, перш ніж просити допомогу.

Для дорослих також доцільні короткі сценарні моделі, пов'язані з перевіркою роботодавця, передачею документів, оплатою посередницьких послуг або терміновим виїздом. Вони краще відтворюють реальну цифрову поведінку, ніж великі універсальні переліки заборон.

Водночас рекомендації мають враховувати різний рівень цифрових навичок. Те, що для одного користувача є очевидною дією, для іншого може бути технічно складним. Тому навчання варто будувати за принципом пріоритетності, а не максимальної кількості правил.

У конкретній ситуації людині достатньо спершу знати кілька дій, що мають безпосереднє значення для її безпеки. Поступове засвоєння таких практик є реалістичнішим, ніж очікування, що кожен користувач опанує великий набір універсальних правил цифрової безпеки.

Отже, цифрова грамотність у профілактиці торгівлі людьми полягає не у здатності самостійно встановити факт злочину, а у вмінні перевірити ключову інформацію, обмежити необґрунтоване поширення даних, контролювати основні

цифрові акаунти та своєчасно звернутися по консультацію. Саме можливість такого звернення визначає перехід від профілактики до системи допомоги.

7.4. Цифрові засоби звернення по допомогу

Можливість звернутися по допомогу є критичною ланкою між профілактичним інформуванням і реальною підтримкою постраждалої особи. У цифровому середовищі ця можливість уже не обмежується телефонною гарячою лінією. Вебчати, текстові повідомлення, месенджери, електронні форми та інші дистанційні канали можуть стати першою точкою контакту для людини, яка не має можливості особисто звернутися до установи, перебуває за кордоном, боїться бути почутою або ще не готова відразу розкривати свою особу.

Сучасні міжнародні підходи дедалі виразніше закріплюють необхідність доступних і спеціалізованих механізмів допомоги. Директива (ЄС) 2024/1712 передбачає створення одного або кількох механізмів раннього виявлення, ідентифікації, допомоги та підтримки як встановлених, так і ймовірних постраждалих, а також вимагає, щоб така допомога надавалася за поінформованої згоди особи. Документ також вимагає враховувати індивідуальні потреби постраждалої особи та забезпечувати перенаправлення до відповідної форми підтримки [92].

У практичному сенсі це означає, що цифровий сервіс має насамперед забезпечити можливість безпечно розпочати контакт. Людина, яка перебуває під контролем іншої особи або діє в умовах гострого стресу, може мати лише кілька хвилин для звернення. Довга форма з обов’язковим введенням паспортних даних, адреси, повної дати народження, детального опису обставин і кількох способів зв’язку може фактично унеможливити звернення.

Доцільнішим є поетапний підхід: на першому етапі достатньо короткого повідомлення, яке дає змогу зрозуміти, якої допомоги потребує користувач і чи може він безпечно продовжувати розмову. Подальші відомості доцільно збирати лише тоді, коли вони стають необхідними для конкретної дії або послуги.

7.4.1. Канали цифрового звернення

Вебчат є зручним форматом у ситуаціях, коли людина не може або не хоче говорити телефоном. Текстова комунікація дає змогу поступово формулювати повідомлення і краще контролювати темп розмови, але водночас може залишати цифрові сліди у браузері або на пристрої.

Разом із тим вебчат має власні ризики. Історія браузера, відкриті вкладки, автоматичне збереження введених даних, кеш або повідомлення про відновлення сесії можуть залишати цифровий слід. Тому сервіс не повинен обіцяти «повну невидимість», якщо технічно цього гарантувати неможливо.

Функція швидкого виходу зі сторінки може зменшити видимість поточного сеансу, але не повинна подаватися як гарантія повного видалення локальних цифрових слідів.

Таблиця 7.1. Цифрові канали звернення по допомогу: можливості, ризики та умови безпечного використання

Канал	Основна перевага	Основний ризик	Умова безпечного використання
Телефонна лінія	швидкий прямий контакт	розмову можуть почути	погодження безпечного часу дзвінка
Вебчат	текстовий формат і контроль темпу	історія браузера, локальні сліди	нейтральний інтерфейс, пояснення меж «швидкого виходу»
Месенджер	звичний і доступний канал	активні сесії, попередній перегляд повідомлень	перевірка безпечності акаунта і пристрою
Електронна форма	структуроване звернення	надмірний збір даних	мінімум обов’язкових полів
Відеозв’язок	ширший контекст	розкриття оточення і місцеперебування	використання лише за згодою та в

	комунікації		безпечному середовищі
Чат-бот	швидка навігація	помилкова автоматична інтерпретація	чіткий перехід до фахівця у складних випадках

Таблиця узагальнена на основі [92; 93; 96].

Месенджери мають низький поріг входу, але їхня безпечність залежить від налаштувань пристрою й акаунта. Попередній перегляд повідомлень, активні сесії на інших пристроях або спільний доступ можуть зробити звернення видимим сторонній особі. Тому сам факт використання певного акаунта не означає, що цей канал безпечний для подальшої комунікації.

Електронна форма корисна для структурованого першого звернення, але легко провокує надмірний збір даних. Обов'язковими мають залишатися лише ті поля, без яких неможливо відповісти користувачеві або визначити наступний крок.

Мобільний застосунок не повинен бути єдиним способом звернення. Його встановлення потребує технічних ресурсів і може розкривати характер інтересу користувача через назву чи іконку. Якщо функцію можна реалізувати через мобільний вебресурс, чат або телефонну лінію, окремий застосунок не завжди виправданий.

Телефонна гаряча лінія, попри цифровізацію, не втрачає значення. Вона залишається критично важливою для людей без смартфона, із нестабільним Інтернетом або низькою цифровою грамотністю. У Плані реагування МОМ на кризу в Україні на 2025 рік функціонування національної безкоштовної консультативної лінії 527 поєднується з інформаційними кампаніями, профілактикою і безпечними механізмами перенаправлення [93].

Це показує доцільність багатоканальної моделі, в якій жоден окремий засіб не розглядається як універсальний.

7.4.2. Анонімність, псевдонімність і мінімізація даних

На етапі першого звернення важливо не вимагати від людини більше інформації, ніж необхідно для початку комунікації. Повна ідентифікація до першої консультації може стати бар'єром для тих, хто сумнівається у своїй ситуації, боїться наслідків звернення або не довіряє інституціям.

Якщо сервіс вимагає повної ідентифікації ще до першої консультації, частина потенційних користувачів просто не скористається ним.

Це не означає, що всі види допомоги можуть надаватися анонімно. На певному етапі ідентифікація може бути необхідною для медичної, соціальної, правової або іншої формалізованої послуги. Принципова різниця полягає в тому, що ідентифікація не повинна бути автоматичною умовою самого факту звернення.

Тому доцільно розрізняти анонімний первинний контакт, частково ідентифіковане консультування та формалізоване отримання конкретної послуги.

Цифровий сервіс також не повинен приховано збирати надлишкові технічні дані. IP-адреса, ідентифікатор пристрою, поведінкова аналітика або точна геолокація можуть бути чутливими не менше, ніж дані, які користувач вводить у форму.

Такі технічні дані доцільно збирати лише за наявності чіткої функціональної потреби.

7.4.3. Безпечність комунікації та доступність

Перш ніж починати змістовну розмову, важливо з'ясувати, чи безпечно людині отримувати повідомлення саме зараз. Просте запитання «Чи можна вам тут писати?» іноді є важливішим за детальне збирання обставин.

Доцільно також узгодити час, спосіб і формат подальшого контакту та з'ясувати, чи можуть інші особи бачити сповіщення на пристрої.

Така практика відповідає логіці підходу, орієнтованого на постраждалу особу (survivor-centred), та травма-інформованого підходу (trauma-informed), де особливе значення мають безпека, прозорість, контроль і можливість вибору. У

рекомендаціях Державного департаменту США 2024 року щодо meaningful survivor engagement серед ключових принципів прямо названо safety, trustworthiness and transparency, collaboration, empowerment, voice and choice [96].

Для цифрового сервісу це означає, що людина має розуміти, хто відповідає, чи працює сервіс цілодобово, коли чекати на відповідь і що відбудеться після надсилання повідомлення.

Сервіс не повинен створювати враження цілодобового спілкування з фахівцем, якщо поза робочим часом доступна лише автоматична відповідь. Бот може підтвердити отримання звернення або надати екстрені контакти, але не повинен імітувати повноцінну професійну підтримку.

Ключові повідомлення мають бути доступні зрозумілою мовою та, за потреби, у кількох мовних версіях. Машинний переклад може бути допоміжним засобом, але критично важлива правова, медична чи кризова інформація не повинна залежати лише від автоматичної інтерпретації [92].

Доступність для осіб з інвалідністю також не може бути додатковою опцією. Текстовий чат може бути зручним для людини з порушенням слуху, але недоступним для незрячого користувача, якщо сайт некоректно працює зі скрінрідером. Відеозв’язок може бути корисним для жестової комунікації, але вимагати стабільного Інтернету й приватного простору.

Саме тому цифровий сервіс має забезпечувати кілька функціонально рівноцінних каналів, а не один «універсальний» формат.

7.4.4. Автоматизація і межі використання чат-ботів

Автоматизовані засоби можуть полегшувати перший контакт, якщо їхня функція обмежена навігацією, наданням базової інформації та передаванням звернення відповідному фахівцю. Вони не повинні самостійно визначати, чи є людина постраждалою, відмовляти у доступі до фахівця або завершувати взаємодію лише через невідповідність повідомлення типовому сценарію.

Це особливо важливо для непрямих або неповних звернень, коли людина не використовує терміни «експлуатація», «примус» чи «торгівля людьми», але

описує обставини, що потребують професійної уваги. У таких випадках автоматизація має забезпечувати передачу звернення людині-фахівцю.

7.4.5. Перехід від цифрового контакту до реальної допомоги

Цифровий канал має сенс лише тоді, коли після отримання повідомлення користувач отримує зрозумілий наступний крок: перехід до консультанта, погоджене перенаправлення, контакт конкретного фахівця або організацію подальшої комунікації. Надання довгого списку телефонів без пояснення, до кого саме звертатися, фактично переносить адміністративний бар'єр в електронний формат.

План МОМ для України на 2025 рік поєднує консультативні канали з безпечними маршрутами перенаправлення та веденням випадку [93]. Це відповідає більш зрілій моделі: звернення розглядається не як ізольована комунікація, а як потенційний початок маршруту допомоги.

Якість цифрового засобу звернення визначається не кількістю функцій, а тим, чи може людина безпечно розпочати контакт, не розкриваючи зайвих даних, зрозуміти подальший порядок дій і перейти до реальної підтримки.

Після встановлення контакту основним стає вже не сам канал, а професійна організація подальшої взаємодії з постраждалою особою.

7.5. Цифрова підтримка первинного контакту з постраждалою особою

Після встановлення первинного цифрового контакту завдання системи змінюється. На цьому етапі йдеться вже не просто про доступність каналу, а про професійну взаємодію з конкретною людиною, яка може перебувати у стані страху, дезорієнтації, залежності або безпосередньої небезпеки. Цифрові засоби тут мають підтримувати комунікацію, але не підміняти фахівця і не диктувати логіку допомоги.

Першочерговим є не детальне збирання обставин, а встановлення безпечного формату подальшого зв'язку. Те, що людина звернулася з певного

номера, акаунта чи електронної адреси, ще не означає, що цей канал можна безпечно використовувати надалі.

Тому до змістовної розмови доцільно з'ясувати, чи безпечно продовжувати комунікацію саме зараз, чи можна писати пізніше, чи допустимий дзвінок і який канал сама людина вважає прийнятним. Така логіка відповідає підходу, орієнтованому на постраждалу особу (survivor-centred), та травма-інформованому підходу (trauma-informed), у межах яких особливе значення мають безпека, прозорість, можливість вибору і збереження контролю над процесом [96].

7.5.1. Безпечний канал і умови подальшої комунікації

Під час первинного контакту важливо розрізняти контактні дані і безпечні контактні дані. Номер телефону може бути відомий іншій особі. Електронну пошту можуть переглядати з іншого пристрою. Месенджер може залишатися відкритим у вебверсії або на комп'ютері, до якого користувач більше не має доступу.

Через це система або фахівець не повинні автоматично використовувати перший отриманий контакт для подальшої комунікації. Безпечність каналу потрібно перевіряти окремо.

Доцільно узгодити, чи безпечно надсилати повідомлення, у який час можливий контакт, чи допустимий дзвінок і чи потрібен альтернативний канал.

Такі запитання можуть здаватися другорядними, але на практиці вони безпосередньо пов'язані з фізичною безпекою.

Особливо обережно слід використовувати автоматичні підтвердження. Повідомлення «ваше звернення щодо торгівлі людьми отримано» може бути небезпечним, якщо його побачить стороння особа. Нейтральне формулювання або можливість відмовитися від автоматичного повідомлення часто є безпечнішим. Те саме стосується push-сповіщень, SMS та електронних листів із темою, яка прямо вказує на характер звернення.

Цифровий сервіс має дозволяти змінити канал у процесі взаємодії. Людина може почати з вебчату, а потім перейти до телефонного дзвінка, електронної

пошти або особистої зустрічі. Інша ситуація можлива у зворотному напрямі: голосовий контакт стає небезпечним, і продовжувати спілкування можна лише текстом.

Така гнучкість є частиною безпечної професійної комунікації.

7.5.2. Поетапний збір інформації та робота з цифровими матеріалами

Після встановлення безпечного каналу не слід одразу переходити до повного інтерв'ю. На початку важливо з'ясувати лише обставини, від яких залежить негайна допомога: наявність безпосередньої загрози, можливість залишити місце перебування, потребу в медичній допомозі та доступ до засобів зв'язку, документів і власних коштів.

Директива (ЄС) 2024/1712 передбачає раннє виявлення, ідентифікацію, допомогу та перенаправлення постраждалих до найбільш відповідної форми підтримки. Це не означає, що первинний цифровий контакт має перетворюватися на формальну процедуру встановлення статусу. Навпаки, на ранньому етапі доцільно збирати лише ті відомості, які потрібні для безпеки й організації наступної дії.

Надмірно деталізоване опитування створює одразу кілька проблем. Людина може не мати достатньо часу, не бути готовою описувати травматичні події або не розуміти, навіщо потрібна частина запитуваних відомостей. Для цифрової системи кожне додаткове поле означає ще один елемент чутливої інформації, який потрібно захищати й обґрунтовано зберігати.

Тому доцільним є принцип поетапності: спочатку мінімум інформації для безпечної відповіді, далі – лише те, що необхідне для конкретної послуги.

Сучасні дослідження trauma-informed care підтримують таку логіку. У роботі Gezinski та співавторів 2025 року серед важливих характеристик належної взаємодії з особами, які постраждали від сексуальної експлуатації, виокремлено довіру, співчутливу комунікацію, автономію, можливість вибору та безпечне середовище. Такий підхід несумісний із стандартизованим детальним опитуванням, яке проводиться незалежно від стану людини та її безпосередньої потреби.

Якщо необхідні відомості вже отримані уповноваженим фахівцем, наступний спеціаліст не повинен автоматично вимагати повного повторення травматичної історії. Цифрова система має передавати достатній функціональний контекст, не копіюючи без потреби весь зміст попередніх розмов.

Під час первинної комунікації людина може надсилати документи, листування, фотографії, адреси або інші цифрові матеріали. Сервіс має пояснювати, які з них справді потрібні для конкретної дії, а які не варто передавати на цьому етапі.

Це відповідає принципу мінімізації даних і зменшує ризик надлишкового накопичення чутливої інформації.

Фотографія або інший цифровий файл може містити приховані технічні відомості, які користувач не бачить безпосередньо. Тому цифрові матеріали не слід накопичувати або зберігати без функціональної потреби.

Водночас не слід примушувати людину самостійно вирішувати, чи має матеріал доказове значення. Якщо документ потенційно важливий для подальшої правової процедури, доцільно залучити компетентного фахівця, а не просто радити видалити або очистити пристрій.

У межах цього розділу йдеться саме про безпечність контакту, а не про технічні процедури цифрової криміналістики, які розглядаються окремо.

7.5.3. Комунікація, конфіденційність і збереження контролю постраждалої особи

Стиль комунікації під час первинного контакту має не менше значення, ніж технічна надійність каналу. Формулювання на кшталт «чому ви погодилися?», «чому не пішли раніше?» або «чому віддали документи?» можуть сприйматися як звинувачення, навіть якщо працівник не має такого наміру.

У текстовому форматі цей ризик посилюється через відсутність інтонації та невербальної підтримки.

Комунікацію доцільно зосереджувати на поточній ситуації, безпеці та найближчих потребах людини, а не на оцінюванні її попередніх рішень.

Корисним є коротке пояснення, навіщо ставиться певне запитання. Наприклад, замість формального «вкажіть номер телефону» можна пояснити: «ми уточнюємо це, щоб не зв’язатися з вами у небезпечний момент».

Для людини, яка вже пережила втрату контролю, така прозорість має принципове значення.

Підхід, орієнтований на постраждалу особу, передбачає реальну можливість зробити паузу, змінити канал, перенести розмову або відмовитися від окремого кроку [96].

Відеозв’язок також не слід вважати автоматично кращим форматом. Для фахівця він може давати більше контексту, але для постраждалої особи водночас розкривати приміщення, місцеперебування або присутність інших людей.

Тому формат має обиратися виходячи не зі зручності працівника, а з безпеки і прийнятності для користувача.

Постраждала особа повинна знати, хто має доступ до повідомлень, чи може інформація бути передана іншій організації та за яких умов. Формула «все конфіденційно» може бути так само проблемною, як і повна відсутність пояснень, якщо насправді існують законодавчо визначені випадки обов’язкового реагування.

Тому межі конфіденційності мають бути пояснені просто й заздалегідь.

Якщо інформація буде передаватися іншому суб’єкту, варто повідомити, кому саме і з якою метою. Якщо користувач може відмовитися від певної передачі, це також має бути зрозуміло.

Передбачуваність процесу зменшує відчуття втрати контролю.

У випадках, що стосуються дітей, порядок передачі інформації має одночасно враховувати вимоги законодавства і конкретні обставини безпеки. Директива 2024/1712 вимагає безпечних, конфіденційних і дружніх до дитини процедур повідомлення [92].

7.5.4. Людський контроль і завершення первинного контакту

Цифрова анкета, автоматичний чат або алгоритм можуть допомогти структурувати перші відомості, однак не повинні самостійно вирішувати, чи «відповідає» людина певній категорії і чи заслуговує на контакт із фахівцем.

Реальні звернення часто є неповними, непрямими або суперечливими. Людина може не називати пережите примусом чи експлуатацією або приховувати частину інформації через страх. Тому автоматизований сценарій не може бути остаточним фільтром доступу до допомоги.

У цьому випадку доцільний принцип людського контролю: цифрова система може структурувати, передавати або попередньо сортувати звернення, але рішення щодо безпеки, терміновості або подальшого перенаправлення має залишатися за компетентним фахівцем.

Первинний контакт має завершуватися зрозумілою наступною дією. Недостатньо відповісти людині «зверніться до соціальної служби» або надати перелік із десятка телефонів.

Людині слід пояснити, хто здійснюватиме подальший контакт, яким каналом, яка інформація вже передана і що робити, якщо запланований зв’язок не відбудеться.

Для України така логіка узгоджується з моделлю ведення випадку та безпечних маршрутів перенаправлення, передбаченою МОМ у Плані реагування на кризу 2025 року [93]. У ньому допомога постраждалим не розглядається як одноразова консультація, а як комплексний процес, який може включати психологічну, правову, медичну, матеріальну та реінтеграційну підтримку.

Первинний цифровий контакт можна вважати належно організованим тоді, коли людина безпечно повідомила про ситуацію, зрозуміла подальший порядок дій і зберегла можливість впливати на спосіб взаємодії. Наступним завданням є координація допомоги між різними суб’єктами без невиправданого дублювання процедур і поширення чутливої інформації.

7.6. Цифрові системи перенаправлення та координації допомоги

Первинне звернення постраждалої особи має сенс лише тоді, коли воно приводить до фактичного отримання потрібної допомоги. У практиці протидії торгівлі людьми це майже завжди передбачає взаємодію кількох суб'єктів: соціальних служб, медичних закладів, психологів, юристів, правоохоронних органів, громадських і міжнародних організацій. Саме тому цифрові системи перенаправлення мають забезпечувати не просто передачу контактів, а керований перехід від одного етапу підтримки до іншого.

Директива (ЄС) 2024/1712 передбачає створення механізмів раннього виявлення, ідентифікації, допомоги та підтримки постраждалих із визначенням відповідальних суб'єктів, процедур і каналів комунікації; для транскордонних випадків передбачаються окремі контактні механізми між державами-членами [92].

Отже, цифровізацію такого процесу доцільно починати не зі створення великої централізованої бази, а з чіткого опису маршруту допомоги. Потрібно визначити, хто може ініціювати перенаправлення, хто його приймає, який обсяг інформації є мінімально необхідним, хто залишається відповідальним до моменту фактичного початку нової послуги і що відбувається, якщо інша організація не може прийняти людину.

7.6.1. Організація цифрового перенаправлення

Перенаправлення відрізняється від простого надання контактів. Якщо людині передають номер іншої установи зі словами «зателефонуйте сюди», координація фактично перекладається на неї саму. У складній життєвій ситуації це може стати додатковим бар'єром.

Організоване перенаправлення передбачає, що за згодою постраждалої особи одна служба передає іншій мінімально необхідну інформацію, отримує підтвердження прийняття і пояснює, що відбудеться далі.

У цифровій системі це може підтримуватися через чіткі статуси: створено, передано, прийнято, потребує уточнення, контакт встановлено, завершено.

Важливо, щоб ці статуси описували стан послуги, а не оцінювали поведінку людини.

Тому формулювання на кшталт «не співпрацює», «ненадійний контакт» або «відмовляється від допомоги» є небажаними. Відсутність відповіді може бути наслідком втрати телефону, зміни місця перебування, зовнішнього контролю, страху або технічної проблеми. Нейтральні статуси краще відображають стан процесу і не формують упередженого ставлення наступного фахівця.

Цифровий маршрут має також передбачати альтернативу у випадку відмови. Якщо одна організація не може надати послугу через відсутність місць, територіальні обмеження або нестачу фахівців, система не повинна просто закривати направлення. Воно має повертатися координатору або автоматично пропонувати інший допустимий маршрут.

У протилежному випадку автоматизація лише швидше відтворюватиме ті самі адміністративні розриви, які існували до цифровізації.

7.6.2. Обмін даними, виправлення та підзвітність

Ключовим принципом є передача не повної історії справи, а того обсягу інформації, який потрібен конкретному суб’єкту для виконання своєї функції.

Різні суб’єкти допомоги потребують різного набору відомостей, тому передавання всім учасникам повного тексту первинного інтерв’ю не має функціональної необхідності і лише збільшує ризик поширення чутливої інформації.

Тому доцільно застосовувати принцип необхідності знати. Кожен учасник отримує лише ті дані, без яких не може виконати своє завдання.

Розмежування доступу має відповідати функціям користувача: технічний персонал не повинен автоматично отримувати доступ до змісту психологічних, медичних або правових консультацій лише через адміністративну роль у системі.

Таке розмежування одночасно підвищує безпеку і зменшує кількість випадкового доступу до інформації.

Водночас занадто складна модель прав може провокувати обхідні практики. Якщо кожен документ потрібно довго погоджувати, працівники починають пересилати файли через особисту електронну пошту або месенджери. Тому цифровий захист має бути не тільки суворим, а й придатним для реальної роботи.

Особливого значення набуває згода на передачу даних. Одноразова формула «дозволяю передавати мою інформацію партнерам» є занадто широкою для чутливої сфери.

Доцільніше застосовувати поетапну згоду, пов’язану з конкретною дією: кому передаються дані, для якої послуги і в якому обсязі.

Такий підхід відповідає логіці Директиви 2024/1712, яка пов’язує допомогу з поінформованою згодою та індивідуальною оцінкою потреб.

У випадках, де закон встановлює окремі обов’язки щодо захисту дитини або реагування на безпосередню небезпеку, порядок дій визначається такими нормами. Це означає, що загальний принцип згоди не може механічно застосовуватися однаково до всіх ситуацій.

Цифрова система має фіксувати, хто і коли отримував доступ до певної інформації або передавав її іншому суб’єкту. Журналювання необхідне для підзвітності, внутрішнього контролю та розслідування інцидентів.

Журнал має фіксувати подію, користувача, час і тип операції, не дублюючи без потреби зміст консультацій або документів. Інакше чутлива інформація може опинитися у менш контрольованих технічних журналах.

Одна й та сама особа може звертатися через різні канали, змінювати номер телефону або використовувати інше ім’я під час першого контакту. Система може позначити потенційний дублікат, але остаточне рішення про об’єднання записів має приймати фахівець після перевірки.

Водночас повне розділення кожного звернення змушує людину повторно надавати ті самі відомості. Завдання системи – зменшити дублювання, не створюючи ризику помилкового злиття записів.

Користувач також має мати можливість повідомити про помилку. Неправильний номер телефону, застаріла адреса або неточно сформульована обставина можуть поширитися між кількома установами й надалі сприйматися як факт.

Не всі історичні записи можна просто переписувати, але система повинна дозволяти додати уточнення, виправлення або актуальну інформацію так, щоб наступний фахівець бачив контекст.

7.6.3. Взаємодія державних, громадських і міжнародних суб'єктів

Механізм допомоги постраждалим від торгівлі людьми рідко функціонує лише в межах однієї установи. Громадські організації можуть забезпечувати тимчасове житло, психологічну підтримку, правову консультацію або інші послуги, які не завжди надаються державними структурами.

Директива (ЄС) 2024/1712 прямо передбачає участь відповідних громадських організацій у механізмах перенаправлення [82]. Для України така багатосуб'єктність також є практичною реальністю: План реагування МОМ на кризу у 2025 році передбачає ведення випадку, психосоціальну, правову, медичну та реінтеграційну підтримку, а також координацію між державними органами, місцевою владою, міжнародними та громадськими організаціями [93].

Проте технічні можливості цих суб'єктів можуть суттєво відрізнятися. Велика державна система може мати окрему службу кібербезпеки, тоді як невелика громадська організація працює з обмеженим бюджетом і стандартними хмарними сервісами.

Тому інтеграція не повинна автоматично означати прямий доступ кожного партнера до єдиної центральної бази. У багатьох випадках безпечніше передати конкретний мінімальний набір даних через контрольований канал і зафіксувати сам факт перенаправлення.

7.6.4. Інтероперабельність і транскордонне перенаправлення

Цифрова координація не зводиться до технічної інтеграції систем. Навіть наявність API не визначає, хто має право отримувати інформацію, що означає конкретний статус і хто відповідає за подальшу дію.

Тому інтероперабельність має щонайменше три виміри: технічний, семантичний і організаційний.

Технічний забезпечує сумісність форматів. Семантичний – однакове розуміння полів і статусів. Організаційний – розподіл відповідальності між учасниками.

Наприклад, статус «прийнято» може означати лише те, що запис технічно доставлено до іншої системи. Інша організація може трактувати той самий статус як початок роботи з людиною. У результаті кожна сторона вважатиме, що наступний крок уже виконує хтось інший.

Тому критичні статуси повинні мати однозначне значення. Доцільно окремо фіксувати: доставлено, підтверджено організацією, контакт із постраждалою особою встановлено, послугу розпочато.

Повна централізація не повинна автоматично вважатися кращою моделлю. Концентрація великого обсягу різнорідних чутливих даних в одному середовищі збільшує потенційні наслідки несанкціонованого доступу. Архітектура має визначатися реальними інформаційними потребами системи допомоги.

Транскордонні випадки створюють додаткову складність, оскільки інформація може передаватися між різними правовими режимами, мовами та організаційними структурами.

Директива 2024/1712 передбачає національні контактні механізми для транскордонного перенаправлення між державами-членами ЄС [92]. Їхня функція полягає у взаємодії між компетентними суб’єктами, а не в тому, щоб створювати ще одну точку, яку постраждала особа повинна самостійно знаходити.

Це принципово важливо: складність міжвідомчої та міжнародної координації має залишатися переважно «за лаштунками» сервісу.

Людині потрібно знати не структуру міжнародного обміну, а практичне: хто з нею зв’яжеться, якою мовою, що буде передано і що робити, якщо контакт не відбудеться.

У регіональному Плані МОМ для України та сусідніх країн на 2025 рік окремий акцент зроблено на механізмах перенаправлення, правовій допомозі, транскордонній координації та підтримці людей у різних країнах перебування [94].

Для України це має безпосереднє значення через велику кількість громадян, які тимчасово перебувають в інших державах і можуть потребувати одночасної взаємодії українських та іноземних суб'єктів.

7.6.5. Координація допомоги без надмірного цифрового контролю

Безперервність супроводу не повинна перетворюватися на постійний моніторинг постраждалої особи. Для координації достатньо знати, чи прийнято направлення, чи встановлено контакт і чи почалося надання потрібної послуги.

Це не створює підстав безстроково відстежувати місцеперебування, комунікації або іншу цифрову активність людини.

У центрі системи має бути контроль за виконанням обов'язків самих суб'єктів допомоги, а не контроль за поведінкою постраждалої особи.

Персональний кабінет може бути зручним для перегляду статусу звернення, консультацій або документів, але не повинен бути обов'язковою умовою отримання допомоги. У користувача може не бути безпечного пристрою, стабільного Інтернету або бажання зберігати на телефоні інструмент, який розкриває характер отримуваної підтримки.

Цифрові інструменти мають зменшувати фрагментарність системи, а не перекладати на постраждалу особу функції координатора власної справи.

Отже, цифрова система перенаправлення має забезпечувати керований маршрут між відповідальними суб'єктами, передавати лише необхідний обсяг інформації, фіксувати відповідальність і зменшувати повторне проходження тих самих процедур. Технологія тут виконує допоміжну функцію: вона може скоротити адміністративні розриви, але не замінює професійного рішення, поінформованої згоди та відповідальності конкретного суб'єкта за фактичне надання допомоги.

Після завершення кризового етапу цифрові засоби можуть підтримувати вже довготривале відновлення та реінтеграцію постраждалої особи.

7.7. Цифрові технології у процесі відновлення та реінтеграції постраждалих

Допомога постраждалій особі не завершується припиненням експлуатації, первинною консультацією чи перенаправленням до відповідної служби. Після кризового етапу виникають інші завдання: відновлення фізичного і психоемоційного стану, вирішення правових питань, поновлення документів, здобуття або відновлення освіти, працевлаштування, стабілізація матеріального становища, відновлення соціальних зв'язків. У цьому процесі цифрові технології можуть істотно розширити доступ до послуг, особливо коли людина перебуває далеко від спеціалізованих установ, змінює місце проживання або не має можливості регулярно отримувати допомогу очно.

Водночас цифровізацію реінтеграції не слід розуміти як просту заміну очних послуг дистанційними. Її цінність визначається тим, наскільки вона зменшує бар'єри доступу і водночас зберігає за людиною можливість обирати спосіб взаємодії. Після досвіду експлуатації, який часто пов'язаний із втратою контролю над власними рішеннями, документами, переміщенням чи фінансами, нова система допомоги не повинна відтворювати подібну залежність уже в цифровій формі.

Саме тому відновлення доцільно пов'язувати не з тривалістю перебування особи у спеціалізованій системі, а з поступовим поверненням їй контролю над повсякденними рішеннями. Цифровий сервіс має допомагати доти, доки це потрібно, але не перетворювати підтримку на постійне спостереження або адміністративну прив'язаність.

Комплексний характер такої допомоги простежується у Плані реагування МОМ на кризу в Україні на 2025 рік, де підтримка постраждалих охоплює ведення випадку, психологічну, правову, медичну, матеріальну, професійну та реінтеграційну допомогу [93]. Цифрові засоби можуть доповнювати кожен із цих

напрямів, але їхнє використання має підпорядковуватися потребам людини, а не технічним можливостям конкретної платформи.

7.7.1. Безперервність психологічної, медичної та правової підтримки

Однією з основних переваг цифрових технологій є можливість підтримувати безперервність допомоги після зміни місця проживання або фізичного віддалення від спеціалізованої установи. Для людини, яка вже встановила довірливий контакт із психологом, юристом чи іншим фахівцем, можливість продовжити частину взаємодії дистанційно може бути важливішою, ніж необхідність починати весь процес заново.

У психологічній підтримці можуть використовуватися захищений відеозв'язок, голосові та текстові консультації. Для частини постраждалих текстовий формат є комфортнішим, оскільки дозволяє відповідати у власному темпі й не вимагає негайної вербалізації травматичного досвіду. В інших випадках, навпаки, особистий контакт або відеозв'язок може бути більш прийнятним. Єдиного універсального формату тут немає.

Дослідження технологічно опосередкованих сервісів підтримки, оприлюднене Office of Justice Programs у 2025 році, охоплює телефонні, чат- і текстові формати допомоги для постраждалих від насильства, сексуального насильства та торгівлі людьми. Такі канали розглядаються як частина моделі доступної, орієнтованої на постраждалу особу і травма-інформованої підтримки.

Разом із тим дистанційна психологічна допомога потребує врахування умов, у яких перебуває людина. Потрібно з'ясувати, чи має вона приватний простір, чи не може інша особа чути розмову, чи можна безпечно завершити сеанс у разі раптової небезпеки. Отже, питання безпеки каналу не зникає після первинного звернення, а супроводжує людину і під час подальшої роботи.

Подібний принцип застосовується до медичної підтримки. Дистанційна консультація може бути корисною для уточнення подальших дій, обговорення результатів лікування або координації між фахівцями. Водночас вона не замінює фізичного огляду, лабораторної діагностики чи невідкладної медичної допомоги, коли вони необхідні.

Особливо обережною має бути робота з медичними та психологічними даними. Для координації між службами далеко не завжди потрібен повний зміст консультації або історія лікування. Часто достатньо знати, що допомогу призначено, що вона триває або що потрібне подальше перенаправлення. Це зменшує ризик того, що травматичний досвід почне безпідставно супроводжувати людину в усіх наступних інформаційних системах.

Цифрові технології можуть спрощувати і правову підтримку. Відеоконсультація, захищений текстовий канал, електронний запис на прийом або попереднє передавання окремих документів дають змогу скоротити кількість фізичних візитів і полегшити взаємодію у транскордонних випадках. Проте і тут діє принцип мінімізації: якщо для консультації достатньо окремого документа або короткого опису ситуації, немає потреби передавати весь масив матеріалів.

Загалом цифровий формат у цій сфері доцільно розглядати як інструмент безперервності допомоги, а не як її самостійну альтернативу.

7.7.2. Освіта, професійна адаптація та економічна самостійність

Довготривала реінтеграція неможлива без відновлення економічної самостійності. Цифрові технології можуть підтримувати цей процес через дистанційне навчання, професійну перекваліфікацію, електронні сервіси зайнятості, доступ до освітніх матеріалів і консультацій щодо працевлаштування.

МОМ включає професійну підготовку та заходи, спрямовані на відновлення доходу, до інструментів відновлення і реінтеграції постраждалих [93]. У цифровому середовищі це відкриває можливість отримувати навчальні матеріали незалежно від місця проживання, проходити окремі етапи підготовки дистанційно або підтримувати зв’язок із наставником чи консультантом.

Однак саме надання доступу до онлайн-курсу ще не означає реальної доступності освіти. Людина може користуватися лише смартфоном, мати нестабільний Інтернет або обмежені цифрові навички. Тому освітні програми мають враховувати мобільний формат, можливість повторного перегляду матеріалів, текстові альтернативи до відео та зрозумілу технічну підтримку.

Особливого значення набуває повернення до цифрового ринку праці. Для окремих постраждалих саме онлайн-платформи вакансій, соціальні мережі або месенджери могли бути середовищем попереднього вербування. Тому реінтеграція не повинна будуватися на простій рекомендації «знову шукати роботу онлайн».

Доцільніше підтримувати людину в перевірці роботодавця, розумінні умов трудового договору, використанні офіційних каналів працевлаштування та поступовому відновленні довіри до цифрових сервісів.

Такий підхід відрізняється від профілактики, розглянутої у 7.3. Тут ідеться вже не про загальну навичку безпечної поведінки, а про повернення людини до професійної активності після пережитої експлуатації.

Економічна самостійність тісно пов’язана і з контролем над фінансовими інструментами. Банківські застосунки, електронні платежі та цифрові державні сервіси можуть полегшувати отримання доходу чи соціальної допомоги, але лише за умови, що доступ до них контролює сама людина.

Формальна наявність банківського застосунку не створює фінансової автономії, якщо стороння особа все ще має доступ до номера телефону, електронної пошти або способів підтвердження операцій. Через це відновлення економічної та цифрової автономії часто відбувається паралельно.

7.7.3. Доступ до державних, соціальних послуг і соціальна реінтеграція

Цифрові державні та муніципальні сервіси можуть зменшувати адміністративне навантаження під час відновлення документів, оформлення соціальної допомоги, запису на консультації або взаємодії з іншими публічними службами.

Для людини, яка одночасно вирішує питання житла, лікування, документів і працевлаштування, можливість виконати частину цих дій дистанційно має очевидне практичне значення.

Водночас цифровий канал не повинен ставати єдиною умовою доступу до послуги. Відсутність смартфона, електронної ідентифікації, стабільного

Інтернету або достатніх цифрових навичок не може фактично виключати людину із системи допомоги.

Персональний цифровий кабінет може бути корисним для перегляду статусу звернення, запланованих консультацій або документів. Проте він має залишатися добровільним інструментом, а не обов'язковим елементом усіх процедур.

Особливого значення набуває конфіденційність сповіщень. Навіть звичайне нагадування про консультацію може розкрити характер звернення, якщо його побачить інша особа. Тому нейтральність повідомлень і можливість керувати способом їх отримання мають враховуватися і на реінтеграційному етапі.

Цифрові технології можуть підтримувати не лише формальні послуги, а й соціальні зв'язки. Онлайн-групи взаємодопомоги, освітні спільноти або професійні мережі можуть допомагати подолати ізоляцію і поступово відновлювати соціальну активність.

Однак такі середовища не є абсолютно конфіденційними. Інші учасники можуть робити скриншоти, пересилати повідомлення або поширювати особисту інформацію за межами групи. Тому організатор не повинен обіцяти абсолютну секретність там, де її неможливо забезпечити технічно. Потрібні чіткі правила участі, модерація та зрозуміле пояснення меж конфіденційності.

Не менш важливо, щоб статус постраждалої особи не ставав її постійною цифровою ідентичністю. Рекомендації Державного департаменту США 2024 року щодо змістовного залучення осіб із досвідом експлуатації наголошують на необхідності сприймати їх не лише через пережиту травму, а як осіб із ширшою професійною і соціальною ідентичністю [96].

Для цифрових систем це означає, що факт торгівлі людьми не повинен безстроково залишатися центральним атрибутом профілю в несуміжних сервісах, якщо для цього немає правової або функціональної потреби.

7.7.4. Відновлення цифрової автономії та поступове завершення спеціалізованої підтримки

У довгостроковій перспективі одним із головних результатів реінтеграції є поступове зменшення залежності від спеціалізованої системи допомоги. Йдеться не про формальне «закриття випадку», а про повернення людині здатності самостійно користуватися цифровими сервісами, управляти власними акаунтами, отримувати послуги і приймати рішення без постійного посередництва фахівця.

Цифрові технології можуть сприяти цьому процесу, але можуть і створити нову форму залежності. Це відбувається, наприклад, коли всі взаємодії можливі лише через один спеціалізований застосунок, працівник служби зберігає паролі користувача або сама система передбачає постійний моніторинг активності.

Допомога має бути організована так, щоб контроль поступово переходив до самої людини.

Фахівець може допомогти відновити доступ до акаунта, налаштувати захист або пояснити роботу сервісу, але не повинен без необхідності керувати ним замість користувача. Особливо це важливо після досвіду експлуатації, коли залежність від рішень іншої особи вже була елементом контролю.

Тривалий контакт із сервісом після завершення основного супроводу також має залишатися добровільним. Можливість повторно звернутися по допомогу є корисною, але вона не створює підстав для безстрокових повідомлень, регулярних запитів про стан людини чи спостереження за її цифровою активністю.

Завершення активного супроводу має супроводжуватися і переглядом обсягу даних, які зберігаються. Інформація, необхідна під час кризового етапу, не обов’язково залишається потрібною через тривалий час. Безстрокове накопичення повного цифрового досьє суперечить самій логіці відновлення автономії і має бути обґрунтоване лише конкретними правовими чи функціональними потребами.

У цьому сенсі цифрова реінтеграція досягає своєї мети тоді, коли технологія поступово перестає бути посередником між людиною і звичайним соціальним життям. Постраждала особа отримує можливість самостійно користуватися освітою, працевлаштуванням, державними, фінансовими та комунікаційними сервісами без постійного нагадування про статус постраждалої.

Однак відновлення автономії неможливе, якщо колишній експлуататор або інша особа зберігає доступ до електронної пошти, номера телефону, геолокації, хмарного акаунта, соціальних мереж чи фінансових сервісів. Тому наступним етапом є не загальна цифрова грамотність, а вже цілеспрямоване відновлення цифрової безпеки постраждалої особи після припинення експлуатації.

7.8. Цифрова безпека постраждалої особи

Припинення фізичної експлуатації не завжди означає припинення контролю над людиною. Доступ до смартфона, електронної пошти, хмарних сервісів, месенджерів, геолокації, банківських застосунків або пов’язаних пристроїв може давати іншій особі можливість і надалі отримувати інформацію про пересування, контакти, фінансову активність чи повсякденні дії постраждалої особи. Через це цифрова безпека має розглядатися як складова загального процесу захисту, а не як окремий набір технічних рекомендацій.

Цей аспект принципово відрізняється від цифрової грамотності, розглянутої у підрозділі 7.3. Там ішлося переважно про профілактичні навички до виникнення або усвідомлення небезпечної ситуації. На етапі після припинення експлуатації вихідні умови інші: окремі акаунти, пристрої або канали зв’язку вже можуть бути скомпрометованими, а стороння особа – мати чинний доступ, про який користувач не знає.

Саме тому стандартна рекомендація негайно змінити всі паролі, видалити підозрілі застосунки або скинути телефон до заводських налаштувань не є універсально безпечною. Практичні рекомендації eSafety Commissioner 2025 року щодо технологічно опосередкованого насильства наголошують, що різкі зміни цифрового доступу можуть бути помічені особою, яка здійснює контроль, і

в окремих ситуаціях спричинити ескалацію. Технічні дії доцільно планувати як частину ширшого плану безпеки.

Хоча зазначене джерело стосується передусім технологічно опосередкованого домашнього та сімейного насильства, описані механізми цифрового контролю – доступ до акаунтів, відстеження місцеперебування, прихований контроль пристрою – мають практичне значення і для захисту осіб, які постраждали від торгівлі людьми. Таке використання суміжного досвіду є виправданим за умови чіткого розмежування сфер його первинного застосування.

7.8.1. Відновлення контролю над акаунтами, номером телефону та пристроями

Першим завданням є визначення того, які елементи цифрового середовища можуть залишатися під стороннім контролем. Йдеться не лише про сам смартфон. Доступ може зберігатися через основну електронну пошту, номер мобільного телефону, системний акаунт пристрою, хмарні резервні копії, активні сесії у месенджерах, спільні сімейні акаунти або способи відновлення паролів.

Особливе значення мають облікові записи, через які можна відновити доступ до інших сервісів. Насамперед це основна електронна пошта, номер телефону та системний акаунт мобільного пристрою. Якщо стороння особа контролює один із цих елементів, зміна пароля лише в окремій соціальній мережі може не вирішити проблему.

Відновлення цифрового контролю тому має починатися не з хаотичної зміни всіх паролів, а з розуміння взаємозв’язків між ключовими акаунтами: які адреси й номери використовуються для відновлення, які пристрої залишаються авторизованими, чи є активні сесії на інших комп’ютерах або телефонах.

За можливості критичні зміни доцільно здійснювати з пристрою, щодо якого немає обґрунтованої підозри у сторонньому контролі. Якщо чинний смартфон може відстежуватися або містити небажане програмне забезпечення, використання його для зміни важливих облікових даних не завжди забезпечить очікуваний результат.

Окремого аналізу потребує номер мобільного телефону. Він часто використовується для багатофакторної автентифікації, підтвердження банківських операцій або відновлення акаунтів. Якщо SIM-карта оформлена на іншу особу або номер входить до спільного тарифного плану, сторонній користувач може мати додаткові можливості впливати на його обслуговування.

Зміна номера іноді є необхідною, але вона має бути підготовленою. Старий номер може залишатися пов'язаним із банківськими, державними, медичними та іншими важливими сервісами. Перед його заміною потрібно визначити, які системи до нього прив'язані і як буде безпечно перенесено доступ.

Не завжди вирішує проблему і придбання нового телефона. Якщо на новий пристрій відновити скомпрометований хмарний акаунт, стару резервну копію або попередні способи відновлення доступу, частина небезпечних налаштувань може зберегтися. У таких ситуаціях доцільність повного чи вибіркового перенесення даних має оцінюватися з урахуванням потреб конкретної людини.

7.8.2. Геолокація, stalkerware, трекери та інші форми цифрового стеження

Цифрове відстеження не обов'язково потребує складного шпигунського програмного забезпечення. У багатьох випадках достатньо звичайних функцій, які раніше були налаштовані добровільно: спільного доступу до місцеперебування, сімейної групи, сервісу пошуку пристрою, синхронізації фотографій, карт, фітнес-застосунків або хмарного облікового запису.

Через це просте вимкнення GPS не гарантує припинення стеження. Значення має те, які застосунки і сервіси мають доступ до геолокації, кому вона передається, чи активні спільні сімейні функції та чи не розкривається місцеперебування непрямо.

Таким непрямим джерелом можуть бути фотографії з упізнаваним оточенням, геотеги, позначки інших користувачів, публікації у соціальних мережах або автоматичні записи фітнес-сервісів. Отже, цифровий захист може потребувати не лише зміни налаштувань самої постраждалої особи, а й обережності з боку її близького оточення.

Окремим випадком є stalkerware – програмне забезпечення, яке використовується для прихованого контролю активності пристрою. Воно може давати доступ до даних про місцеперебування, повідомлення, дзвінки або іншу активність.

При цьому важливо не робити висновок про наявність stalkerware лише за непрямими технічними ознаками. Швидке розряджання батареї, перегрів або збільшення мобільного трафіку можуть мати багато причин. Більш значущим є контекст: інша особа систематично знає інформацію про переміщення, розмови чи дії, яку їй не повідомляли.

Якщо виникає обґрунтована підозра, автоматичне видалення підозрілого програмного забезпечення не завжди є безпечним. Зникнення доступу може бути помічене особою, яка здійснює контроль, і вплинути на її поведінку.

Так само необдумане очищення пристрою може призвести до втрати матеріалів, які згодом можуть мати значення для правового захисту. У цьому розділі не розглядаються процедури цифрової криміналістики, однак принцип є важливим: перед видаленням потенційно значущої інформації доцільно врахувати не лише технічну, а й правову сторону ситуації.

Схожий підхід застосовується до Bluetooth-трекерів, смартгодинників, автомобільних систем, фітнес-браслетів та інших підключених пристроїв. Якщо невідомий трекер виявлено, його негайне вимкнення не завжди є оптимальною першою дією. Рішення має бути узгоджене із загальним планом безпеки.

Таким чином, цифрове стеження слід розглядати не як проблему одного конкретного застосунку, а як сукупність можливих каналів доступу до інформації про людину.

7.8.3. Соціальні мережі, цифрове переслідування та імітація особи

Після припинення експлуатації соціальні мережі можуть залишатися каналом психологічного тиску, спостереження або повторного контакту. Для цього можуть використовуватися нові акаунти, фальшиві профілі, небажані згадки, публікація приватної інформації, погрози або звернення через знайомих.

У таких випадках блокування одного профілю часто не вирішує проблему повністю. Доцільно переглянути налаштування видимості, можливість пошуку профілю за номером телефону чи електронною адресою, активні сесії, підключені сторонні застосунки та правила позначення у публікаціях.

Водночас повна відмова від соціальних мереж не повинна розглядатися як стандартна модель захисту. Для людини вони можуть бути важливими для навчання, працевлаштування, підтримки соціальних зв'язків або професійної діяльності. Метою є не цифрова ізоляція, а повернення контролю над тим, хто може контактувати з користувачем і яку інформацію про нього бачити.

Окремою проблемою є імітація особи: створення фальшивих профілів, використання чужих фотографій, імені або інших персональних даних. Генеративний штучний інтелект полегшує створення переконливих матеріалів і масштабування таких дій [66].

У разі появи фальшивого профілю важливими можуть бути механізми скарг платформи, фіксація посилань та інших необхідних матеріалів, якщо це не створює додаткової небезпеки, а також правова консультація.

Особливо тяжкою формою цифрового тиску є поширення інтимних матеріалів без згоди. У таких випадках технічні дії щодо платформи мають поєднуватися з правовою та психологічною допомогою, оскільки сама процедура видалення контенту не усуває всіх наслідків для постраждалої особи.

Суміжні європейські підходи до technology-facilitated violence також дедалі більше виходять із того, що відповідальність за цифрову безпеку не може покладатися винятково на користувача. Рекомендація Ради Європи CM/Rec(2026)2 щодо відповідальності за технологічно опосередковане насильство проти жінок і дівчат акцентує на реагуванні, орієнтованому на постраждалу особу, та травма-інформованому реагуванні, доступі до захисту та відповідальності цифрових посередників. Хоча документ має ширший предмет, ніж торгівля людьми, його положення є релевантними для ситуацій цифрового переслідування та контролю після експлуатації.

7.8.4. Індивідуальний цифровий план безпеки та відновлення автономії

У межах цього дослідження пропонується використовувати поняття **індивідуального цифрового плану безпеки постраждалої особи**. Йдеться не про усталений міжнародний стандарт, а про авторську практичну модель, що систематизує дії з відновлення цифрового контролю з урахуванням ширшої безпеки людини.

Необхідність такого плану випливає з того, що одна й та сама технічна дія може мати різні наслідки залежно від ситуації. Для однієї людини першочерговим буде захист електронної пошти, для іншої – припинення спільного доступу до геолокації, для третьої – створення незалежного каналу зв'язку без негайного втручання у скомпрометований пристрій.

Тому універсальний чекліст не може замінити індивідуального рішення.

План доцільно будувати навколо кількох взаємопов'язаних компонентів: безпечного пристрою, ключових акаунтів, способів відновлення доступу, номера телефону, активних сесій, геолокації, хмарних сервісів, підключених пристроїв та резервного каналу комунікації.

Важливо також передбачити сценарій втрати доступу. Людина має знати, яким способом можна відновити критичні акаунти і через який незалежний канал зв'язатися з довіреною особою або службою допомоги. За потреби може бути заздалегідь погоджена кодова фраза для ситуацій, коли відкрито повідомити про небезпеку неможливо.

Цей план має бути підпорядкований одному принципу: технічні зміни здійснюються настільки швидко, наскільки це сумісно з реальною безпекою людини.

Таблиця 7.2. Компоненти індивідуального цифрового плану безпеки постраждалої особи

Компонент	**Що потребує перевірки**	**Потенційний ризик**	**Орієнтир безпечної дії**
Безпечний пристрій	хто мав фізичний або віддалений доступ	прихований контроль	для критичної комунікації за можливості використовувати незалежний пристрій
Основна електронна пошта	активні сесії, резервні адреси, способи відновлення	повторне отримання стороннього доступу	відновлювати контроль з урахуванням усіх пов’язаних способів авторизації
Номер телефону	власник SIM, прив’язані сервіси, SMS-підтвердження	контроль відновлення акаунтів і банківських операцій	за потреби планувати зміну номера разом із перенесенням критичних сервісів
Геолокація	спільний доступ, сімейні функції, застосунки	визначення місцеперебування	змінювати доступ з урахуванням можливого ризику ескалації
Хмарні сервіси	довірені пристрої, резервні копії, спільні акаунти	повторна компрометація нового пристрою	переглянути способи доступу до перенесення даних
Соціальні мережі	видимість профілю, теги, пошук за контактами	переслідування, імітація особи	обмежити небажаний доступ без автоматичної цифрової ізоляції

Резервний канал зв’язку	незалежний контакт, можливість втрати основного пристрою	повне припинення безпечної комунікації	заздалегідь погодити альтернативний спосіб контакту

Таблиця розроблена на основі узагальнення положень цього дослідження.

Таблиця не повинна використовуватися як універсальна послідовність обов’язкових кроків. Її функція – показати компоненти, які можуть потребувати уваги залежно від конкретної ситуації.

Відновлення цифрової безпеки має завершуватися не створенням постійної залежності від фахівця, а поверненням людині здатності самостійно контролювати власне цифрове середовище. Працівник служби може допомогти відновити доступ, пояснити налаштування або підтримати виконання окремої дії, але не повинен без необхідності зберігати паролі, керувати акаунтами чи приймати рішення замість користувача.

Особливо це важливо для людей із низькою цифровою грамотністю. Допомога має поступово передавати контроль самій людині: пояснювати, що змінюється, навіщо це робиться і як надалі перевіряти відповідні налаштування без постійного посередництва.

Не всі загрози можна усунути технічно. Якщо адресу розкриває знайомий, конфіденційну інформацію неправомірно передає працівник організації або переслідування продовжується через фізичні контакти, новий пароль до телефона не вирішить проблему. Цифрова безпека тому має залишатися частиною ширшої фізичної, правової, інформаційної та соціальної безпеки.

Кінцевою метою є **цифрова автономія**: постраждала особа контролює власні акаунти, канали комунікації, доступ до місцеперебування та обсяг інформації, який вона готова розкривати.

Водночас можливість реалізувати такі дії залежить від віку, інвалідності, цифрових навичок, доступу до власного пристрою, мови та інших індивідуальних обставин. Саме тому вимоги цифрової безпеки не можуть бути

однаковими для всіх користувачів і мають поєднуватися з принципами доступності та недискримінації.

7.9. Захист дітей та забезпечення диференційованої доступності цифрових сервісів

Цифрові сервіси профілактики й допомоги не можуть проєктуватися для умовного «середнього користувача». Вік, інвалідність, мовні й когнітивні бар'єри, рівень цифрової грамотності, доступ до власного пристрою та потреба в сторонній підтримці безпосередньо впливають на можливість безпечно скористатися цифровим каналом. У сфері протидії торгівлі людьми це має особливе значення: недоступний або неправильно спроєктований сервіс може не просто створити незручність, а фактично перекрити людині шлях до допомоги.

Окремої уваги потребують діти. Активне користування соціальними мережами, месенджерами чи мобільними застосунками не означає здатності правильно оцінювати наслідки передачі персональних даних, розпізнавати грумінг (grooming), маніпулятивну комунікацію або безпечно реагувати на небажаний контакт. Технічна вправність користування смартфоном не є тотожною цифровій безпеці.

Європейська комісія у Guidelines on the protection of minors under the Digital Services Act 2025 року наголошує на необхідності високого рівня приватності, безпеки та захищеності неповнолітніх у цифрових сервісах, зокрема щодо небажаних контактів, грумінг, кібербулінгу та маніпулятивних механізмів. Важливо, що відповідальність за безпечне цифрове середовище у такій моделі покладається не лише на саму дитину, а й на архітектуру платформи та її операторів.

7.9.1. Дружні до дитини цифрові сервіси та безпечне звернення

Цифровий сервіс, орієнтований на дитину, має бути побудований навколо зрозумілої логіки взаємодії. Довгі форми, складна правова термінологія або вимога самостійно визначити вид правопорушення створюють зайвий бар'єр.

Дитині має бути достатньо описати ситуацію своїми словами: її змушують щось робити, погрожують, просять надсилати інтимні матеріали, утримують документи, забороняють піти або контактувати з іншими людьми. Завдання цифрового сервісу полягає не в тому, щоб вимагати від неповнолітнього правової кваліфікації подій, а в тому, щоб забезпечити можливість безпечно розпочати контакт.

Дружній до дитини дизайн не обов'язково означає яскравий або стилістично «дитячий» інтерфейс. Для підлітка це може знижувати довіру до ресурсу. Значно важливішими є проста мова, короткі пояснення, передбачувана навігація, зрозумілі кнопки та можливість швидко перейти до живого фахівця.

Особливо важливо враховувати, що дитина може користуватися не власним пристроєм. Телефон, планшет чи комп'ютер можуть належати батькам, опікуну або іншій дорослій особі, яка в окремих випадках сама може бути джерелом небезпеки.

Через це автоматичне надсилання SMS, електронного листа чи push-сповіщення після звернення не завжди є безпечним. Так само не можна автоматично виходити з припущення, що повідомлення законного представника є безпечним у кожній ситуації. Подальші дії мають визначатися вимогами законодавства, віком дитини та конкретними обставинами захисту.

Сервіс має бути готовим і до раптового переривання комунікації. Дитина може закрити чат через появу іншої особи, страх або втрату зв'язку. Це не слід автоматично трактувати як відмову від допомоги. Якщо контакт відновлюється, доцільно продовжити взаємодію без вимоги заново відтворювати всю попередню історію.

Окремим завданням є захист від небажаних контактів. Рекомендації Європейської комісії 2025 року передбачають приватні налаштування за замовчуванням, можливість легко блокувати й обмежувати небажані контакти, захист від додавання до груп без згоди та доступні механізми повідомлення.

Для профілактики торгівлі людьми це має ширше значення: не можна перекладати всю відповідальність за цифрову безпеку на дитину. Частина захисту повинна бути вбудована у саму платформу.

7.9.2. Особи з інвалідністю та цифрова доступність

Доступність цифрового сервісу має розглядатися як базова умова його функціонування, а не як додаткова опція.

У звіті ОБСЄ Invisible Victims: The Nexus between Disabilities and Trafficking in Human Beings 2024 року інвалідність розглядається одразу в кількох вимірах: як фактор, що може посилювати вразливість до експлуатації; як характеристика, яку можуть використовувати торговці людьми; як можливий наслідок експлуатації; а також як обставина, що ускладнює доступ до захисту, правосуддя, охорони здоров'я, працевлаштування та реабілітації.

Отже, цифрова недоступність може додатково посилювати вже існуючі бар'єри.

Для людей із порушеннями зору критичними є коректна семантична структура сторінки, підписані поля форм, зрозумілі заголовки, альтернативні описи значущих зображень і сумісність зі скрінрідерами. Кнопка, яка візуально зрозуміла, але озвучується програмою читання з екрана лише як «button 3», фактично є недоступною.

Для осіб із порушеннями слуху телефонний дзвінок не може залишатися єдиним каналом звернення. Потрібні текстові альтернативи, субтитри до відео, а за потреби – можливість використання жестової мови.

Для людей із порушеннями опорно-рухових функцій важливими є можливість керування клавіатурою, достатній розмір активних елементів, відсутність надто коротких тайм-аутів і вимог до точних жестів.

Для користувачів із когнітивними чи інтелектуальними порушеннями особливе значення мають проста мова, логічна послідовність дій, відсутність непояснених абревіатур і чітке пояснення наслідків кожного кроку.

Міністерство цифрової трансформації України у 2025 році наголошувало на необхідності підвищення цифрової доступності державних сайтів і мобільних

застосунків. Для сервісів у сфері протидії торгівлі людьми це означає, що доступність має закладатися на етапі проєктування, а не додаватися після запуску.

Водночас важливо не ототожнювати інвалідність із автоматичною нездатністю приймати рішення. Якщо система за замовчуванням передає контроль родичу, опікунові або працівнику установи, навіть коли людина могла б діяти самостійно, цифровий сервіс може відтворювати залежність замість її зменшення.

Допоміжні технології мають розширювати можливості користувача, а не створювати нового обов'язкового посередника.

7.9.3. Мовні, цифрові та функціональні бар'єри

Мовна доступність має не менше значення, ніж технічна. Людина може володіти мовою на побутовому рівні, але не розуміти правових, медичних чи адміністративних формулювань. Для мігрантів, переміщених осіб або тих, хто перебуває за кордоном, проблема ускладнюється незнанням самої системи установ.

Тому цифровий ресурс має пояснювати не лише назву організації, а й її функцію: де можна отримати тимчасове житло, правову консультацію, медичну допомогу або підтримку у разі безпосередньої небезпеки.

Автоматичний переклад може бути корисним на первинному етапі, але не повинен залишатися єдиним інструментом у складній правовій, медичній або кризовій комунікації.

Окрему групу становлять люди з низькою цифровою грамотністю. Щоденне користування смартфоном не означає здатності перевірити адресу сайту, змінити налаштування приватності, відновити акаунт або визначити, які дозволи має застосунок.

У таких випадках великі технічні інструкції малоефективні. Практичніше допомогти людині виконати кілька дій, безпосередньо пов'язаних із поточною проблемою. Якщо небезпека стосується геолокації – перевірити саме її. Якщо

стороння особа має доступ до месенджера – відновити контроль над цим акаунтом. Якщо електронна форма надто складна – запропонувати інший канал.

Не всі користувачі мають власний смартфон, постійний доступ до Інтернету або електронну пошту. Людина може користуватися спільним пристроєм, телефоном родича, роботодавця чи партнера або мати лише базовий мобільний телефон.

Якщо система допомоги вимагає встановити застосунок, пройти електронну ідентифікацію, завантажити документи і провести відеодзвінок, вона автоматично виключає частину користувачів.

Цифровий канал тому має доповнювати, а не замінювати телефонний контакт, особисте звернення та інші доступні способи комунікації.

Важливим тимчасовим бар'єром може бути і психологічний стан. Навіть людина з високим рівнем цифрових навичок у стані гострого стресу або виснаження може мати труднощі з концентрацією, запам'ятовуванням інструкцій чи проходженням багатокрокових форм.

Саме тому до цифрової взаємодії доцільно застосовувати травма-інформовані принципи: мінімізувати необов'язкові кроки, пояснювати, що відбудеться далі, уникати перевантаження сторінки та не змушувати користувача повторно вводити великий обсяг чутливої інформації після технічної помилки.

Коректніше говорити саме про застосування травма-інформованих принципів до цифрового сервісу, а не про окрему стандартизовану методологію «trauma-informed digital design» у сфері протидії торгівлі людьми.

7.9.4. Автономія користувача та універсальність без уніфікації

Універсальний цифровий сервіс не означає, що всі користувачі мають проходити однаковий шлях.

Одна людина може обрати текстовий чат, інша – телефонний дзвінок; одна потребує скрінрідера, інша – перекладача; комусь потрібна проста мова, а хтось може користуватися звичайним інтерфейсом без додаткових адаптацій.

Спільним має залишатися результат: реальна можливість отримати допомогу без зайвих бар'єрів.

Саме тому адаптація цифрового сервісу повинна реагувати на конкретну функціональну потребу, а не вимагати від користувача надлишкового розкриття чутливої інформації. Якщо людині потрібен текстовий канал, більший шрифт, перекладач, жестова мова або додатковий час, система повинна забезпечити відповідну можливість без необхідності доводити належність до певної категорії там, де це не є юридично необхідним.

Такий підхід одночасно підтримує доступність і мінімізацію даних.

Окремо слід уникати надмірної опіки. Вік, інвалідність, низький рівень цифрової грамотності чи потреба в допоміжному засобі самі по собі не означають, що людина повинна втрачати контроль над власними рішеннями.

У роботі з дітьми ця автономія, безумовно, реалізується з урахуванням віку, розвитку, найкращих інтересів дитини та законодавчих вимог. Однак і тут метою є не пасивне усунення дитини від процесу, а забезпечення зрозумілої та безпечної участі настільки, наскільки це відповідає конкретній ситуації.

Отже, цифрова інклюзивність у сфері протидії торгівлі людьми полягає не у створенні окремої системи для кожної категорії користувачів, а у здатності одного сервісу забезпечити кілька безпечних шляхів до тієї самої мети.

Доступність, можливість вибору та збереження контролю мають розглядатися не як додаткові характеристики цифрової системи, а як умови її правомірного і етичного використання.

Саме ці вимоги безпосередньо пов’язані з завершальним питанням розділу – правовими, етичними та безпековими принципами проєктування й функціонування цифрових сервісів профілактики та допомоги.

7.10. Правові, етичні та безпекові вимоги до цифрових сервісів профілактики й допомоги

Цифровий сервіс у сфері протидії торгівлі людьми працює з особливо чутливим контекстом. Навіть якщо система не містить формалізованого статусу постраждалої особи, сукупність відомостей про звернення, місцеперебування, контакти, потребу в житлі, медичній чи правовій допомозі може прямо або

опосередковано розкривати обставини, які становлять значний ризик для приватності та безпеки людини.

Через це правові й етичні вимоги не можуть бути додатковим етапом після створення сервісу. Вони мають визначати саму логіку його проєктування: які дані збираються, для чого вони потрібні, кому передаються, як довго зберігаються, які рішення може приймати автоматизована система і де обов'язковою залишається участь фахівця.

Особливість таких сервісів полягає і в тому, що формально коректна технологічна дія може бути небезпечною в конкретній життєвій ситуації. Надсилання повідомлення, збереження геолокації, вимога підтвердити особу або автоматичне синхронізування даних можуть виглядати нейтральними функціями, але створювати додатковий ризик, якщо пристрій контролюється іншою особою.

Тому для цифрових сервісів профілактики й допомоги недостатньо лише відповідати загальним вимогам інформаційної безпеки. Потрібна людиноцентрична модель, у якій правомірність обробки даних, безпечність взаємодії, прозорість, доступність і збереження контролю постраждалої особи розглядаються як взаємопов'язані умови.

7.10.1. Мінімізація даних, прозорість і поінформована згода

Принцип мінімізації даних має особливе значення у сфері протидії торгівлі людьми. Цифровий сервіс не повинен збирати інформацію лише тому, що технічно здатний це зробити. Кожне поле форми, технічний ідентифікатор, геолокаційний параметр або додаткова характеристика користувача мають бути пов'язані з конкретною функціональною потребою.

На етапі першого звернення часто достатньо мінімального набору відомостей, необхідних для відповіді або визначення наступного безпечного кроку. Повна ідентифікація, детальний опис пережитого чи завантаження документів можуть бути потрібними пізніше, коли людина погоджується на конкретну послугу.

Такий поетапний підхід зменшує бар’єр звернення і водночас обмежує наслідки можливого витоку даних.

Мінімізація стосується не лише інформації, яку користувач вводить самостійно. Вебсервіс може автоматично отримувати IP-адресу, інформацію про пристрій, журнали активності, технічні ідентифікатори або дані аналітики. Якщо вони не є необхідними для надання послуги, їх збирання потребує окремого обґрунтування.

Прозорість передбачає, що людина розуміє, що відбувається з її інформацією. Повідомлення про обробку даних не повинно обмежуватися довгим юридичним текстом, який користувач фактично не читає. Критично важливі речі мають пояснюватися безпосередньо у момент, коли вони стають актуальними: навіщо запитується конкретна інформація, кому вона може бути передана і що відбудеться після натискання кнопки «надіслати».

Поінформована згода у таких системах також не повинна перетворюватися на одноразове формальне натискання позначки під час першого входу. Для різних етапів взаємодії можуть бути потрібні різні рішення: почати анонімну консультацію, повідомити контактні дані, передати інформацію іншій службі, долучити документ або погодитися на відеозв’язок.

Доцільнішою є поетапна згода, пов’язана з конкретною дією.

Водночас згода не повинна використовуватися як універсальне виправдання будь-якого збору інформації. Якщо певні дані не потрібні для функціонування сервісу, сам факт того, що користувач формально погодився на їх обробку, не робить такий збір необхідним або етично виправданим.

7.10.2. Privacy by design, safety by design і підхід, орієнтований на постраждалу особу

Для цифрових сервісів профілактики й допомоги принцип **privacy by design** – захист приватності на етапі проєктування – означає, що мінімізація даних, контроль доступу, обмеження строків зберігання та інші захисні механізми повинні бути закладені в систему до її запуску, а не додаватися після виникнення проблем.

Однак для сервісів, пов’язаних із торгівлею людьми, цього недостатньо. Необхідно враховувати і **safety by design** – безпеку користувача як вихідну умову проєктування.

Різниця має практичне значення. Система може технічно добре захищати дані на сервері, але водночас надсилати небезпечні push-сповіщення, вимагати обов’язкового відеодзвінка або залишати на екрані назву сервісу, яка розкриває характер звернення.

Безпека тому має оцінюватися не лише на рівні інформаційної системи, а й на рівні реальної взаємодії людини з нею.

Рекомендація Ради Європи CM/Rec(2026)2 щодо відповідальності за технологічно опосередковане насильство проти жінок і дівчат акцентує на підходах, орієнтованих на постраждалих, травма-інформованому реагуванні та необхідності враховувати безпеку вже на рівні цифрових сервісів. Хоча предмет документа ширший за торгівлю людьми, ці принципи є релевантними для цифрової підтримки осіб, які перебували під технологічно опосередкованим контролем.

Підхід, орієнтований на постраждалу особу, передбачає, що система не лише «надає послугу», а зберігає можливість людини впливати на спосіб її отримання. Це стосується вибору каналу, часу контакту, участі у відеозв’язку, передавання даних іншому суб’єкту, можливості зробити паузу або припинити цифрову взаємодію.

Травма-інформовані принципи доповнюють цю модель. Йдеться про передбачуваність, зрозуміле пояснення подальших дій, уникнення необов’язкового повторного опису травматичних обставин, зменшення когнітивного навантаження та відмову від формулювань, які можуть сприйматися як звинувачення.

При цьому коректніше говорити саме про **застосування травма-інформованих принципів до цифрового сервісу**, а не про окрему усталену методологію «trauma-informed digital design» у сфері протидії торгівлі людьми.

Те саме стосується підходу, що враховує досвід постраждалих осіб (survivor-informed). Доцільно враховувати досвід людей, які пережили експлуатацію, під час проєктування сервісів, тестування сценаріїв взаємодії та визначення бар'єрів доступу. Водночас участь постраждалих осіб не повинна бути символічною або використовувати їхній досвід без достатніх гарантій добровільності, безпеки і конфіденційності [96].

7.10.3. Межі автоматизації та використання штучного інтелекту

Автоматизація може бути корисною для навігації, маршрутизації звернень, надання стандартної довідкової інформації, запису на консультацію або нагадування про подальший крок. Проблема виникає тоді, коли автоматизований інструмент починає замінювати професійне рішення у ситуаціях, що мають пряме значення для безпеки або доступу до допомоги.

Система не повинна самостійно визначати, чи «достатньо серйозна» ситуація користувача, чи відповідає він певній категорії постраждалих або чи заслуговує на передачу звернення фахівцю.

Особливо це важливо через те, що реальні звернення часто не відповідають стандартизованому сценарію. Людина може не використовувати юридичні терміни, не усвідомлювати пережите як експлуатацію, повідомляти лише частину обставин або суперечити сама собі через страх, стрес чи залежність від іншої особи.

Генеративний штучний інтелект додатково ускладнює питання автоматизації. Він може використовуватися для мовної підтримки, попередньої навігації або формування нейтральної відповіді, але не повинен бути єдиним джерелом критично важливої правової, медичної чи кризової інформації.

ОБСЄ та Regional Support Office of the Bali Process у 2024 році звернули увагу на те, що генеративний ШІ може використовуватися і для масштабування обману, імітації особи та інших форм зловживання [66]. Через це система допомоги має чітко розмежовувати автоматизовану інформаційну функцію та професійне рішення.

Межі використання ШІ доцільно визначати ще на етапі проєктування. Користувач повинен розуміти, коли взаємодіє з автоматизованим інструментом, а коли – з людиною. Перехід до фахівця має бути простим і не залежати від того, чи «розпізнав» алгоритм достатню кількість формальних ознак.

Особливо небажаним є створення прихованих оцінок «ризиковості», «надійності» або «ймовірності правдивості» постраждалої особи на основі її мови, поведінки чи цифрової активності. Такі підходи не лише створюють ризик дискримінації, а й виходять за межі функції сервісу допомоги.

Рамкова конвенція Ради Європи про штучний інтелект і права людини, демократію та верховенство права 2024 року закріплює орієнтацію на права людини, людську гідність, недискримінацію, прозорість, підзвітність і можливість належного оскарження рішень, пов’язаних із використанням ШІ. Для цифрових сервісів допомоги це означає, що автоматизація має залишатися допоміжною і не повинна усувати людський контроль у рішеннях із суттєвими наслідками для людини.

7.10.4. Недискримінація, доступність і життєвий цикл даних

Правомірний цифровий сервіс має бути доступним не лише формально, а й фактично.

Як показано у підрозділі 7.9, єдиний цифровий канал може виключати людей із порушеннями зору або слуху, низькою цифровою грамотністю, відсутністю власного смартфона, мовними бар’єрами чи потребою у допоміжних технологіях.

Недискримінація тому стосується не лише змісту рішення, а й самої можливості скористатися сервісом.

Водночас адаптація не повинна вимагати надмірного збору даних. Для надання текстового каналу, більшого шрифту, перекладача чи іншої функціональної адаптації не завжди потрібно створювати окремий детальний профіль інвалідності або стану здоров’я користувача.

Принцип мінімізації має діяти і тут: система має знати стільки, скільки необхідно для конкретної функції.

Окремим питанням є строк зберігання інформації. Дані, які були необхідні на кризовому етапі, не повинні автоматично зберігатися безстроково лише тому, що система технічно дозволяє це робити.

Необхідно розрізняти інформацію, яку потрібно зберігати за законом або для обґрунтованої операційної потреби, і дані, що втратили своє функціональне значення.

Це особливо важливо для повних текстів чатів, аудіо- чи відеозаписів, копій документів, відомостей про місцеперебування та інших чутливих матеріалів. Їх накопичення «про всяк випадок» збільшує потенційні наслідки інциденту і може суперечити логіці реінтеграції та відновлення автономії.

Архівування також не повинно використовуватися як спосіб уникнути рішення про видалення. Переміщення старої інформації до іншої бази не змінює факту її зберігання.

Життєвий цикл даних має бути визначений заздалегідь: збирання, використання, передавання, актуалізація, зберігання, архівування за наявності підстав і видалення після їх зникнення.

Користувачеві при цьому має бути зрозуміло, які дані можуть бути виправлені або актуалізовані. Помилковий запис не повинен безконтрольно переходити між службами і впливати на подальшу допомогу лише тому, що колись був внесений до системи.

7.10.5. Реагування на інциденти та підзвітність операторів цифрового сервісу

Навіть належно спроєктована система не може гарантувати абсолютної відсутності технічних або організаційних інцидентів. Помилково надіслане повідомлення, неправильне перенаправлення, несанкціонований доступ, розкриття інформації іншому користувачеві чи компрометація облікового запису потребують заздалегідь визначеного порядку реагування.

У сфері протидії торгівлі людьми звичайного технічного повідомлення про інцидент може бути недостатньо. Потрібно оцінити, чи створює подія

безпосередню загрозу для конкретної людини і чи необхідні додаткові заходи безпеки.

Наприклад, розкриття часу консультації або нового номера телефону може мати зовсім інші наслідки, ніж витік нейтральної технічної інформації.

Реагування тому має охоплювати не лише усунення технічної причини, а й перевірку того, чи потрібна постраждалій особі зміна каналу, номера телефону, місця зустрічі або іншого елемента плану безпеки.

Підзвітність не може зводитися до загального твердження, що оператор «дотримується конфіденційності». Має бути зрозуміло, хто відповідає за роботу сервісу, хто ухвалює рішення про зміну функцій, кому повідомляються помилки і яким чином користувач може оскаржити неправомірне рішення або повідомити про проблему.

Це стосується і сторонніх розробників, хмарних сервісів, платформ комунікації та інших технологічних постачальників. Передача частини функцій зовнішньому провайдеру не означає передачу йому відповідальності за права та безпеку користувача.

Розробник може відповідати за технічну реалізацію, але оператор сервісу повинен розуміти, які саме дані обробляються, де вони зберігаються, які сторонні компоненти використовуються і які наслідки матиме їхня відмова або компрометація.

Особливе значення має відповідальність за зміни після запуску. Функція, яка була безпечною в одній конфігурації, може стати проблемною після підключення нового аналітичного модуля, автоматичного перекладу, зовнішнього чат-бота або іншого сервісу.

Тому правові й етичні вимоги повинні враховуватися не лише під час первинної розробки, а протягом усього життєвого циклу цифрового продукту.

У підсумку безпечний цифровий сервіс профілактики й допомоги не визначається кількістю технологічних функцій. Його якість полягає у здатності забезпечити людині зрозумілий і доступний шлях до підтримки, не збираючи

зайвих даних, не створюючи нового цифрового контролю і не передаючи критичні рішення непрозорим автоматизованим механізмам.

Правомірність, приватність, доступність, поінформована згода, безпечність за задумом, людський контроль і підзвітність утворюють не окремі технічні вимоги, а єдину систему принципів. Саме вона визначає межі допустимого використання цифрових технологій у профілактиці торгівлі людьми, підтримці постраждалих та їх подальшому відновленні.

Висновки до розділу 7

Цифровізація істотно змінює підходи до профілактики торгівлі людьми та організації допомоги постраждалим. Її значення полягає не у механічному перенесенні традиційних інформаційних матеріалів і сервісів в онлайн-середовище, а у формуванні безперервного маршруту від профілактичного інформування до безпечного звернення, професійної підтримки, перенаправлення, відновлення та повернення цифрової автономії постраждалої особи.

У межах цього підходу профілактика має бути присутньою саме в тих цифрових середовищах, де користувач фактично приймає рішення щодо працевлаштування, переїзду, передачі документів, коштів або взаємодії з посередником. Її практична цінність визначається не лише здатністю повідомити про небезпеку, а й можливістю спрямувати людину до незалежної перевірки інформації, консультації або іншого безпечного наступного кроку. Цифрова грамотність при цьому не повинна зводитися до набору універсальних заборон. Вона має формувати навички перевірки джерел, контролю над персональними даними та акаунтами, розпізнавання маніпулятивної комунікації і своєчасного звернення по допомогу.

Особливого значення набуває організація цифрового звернення. Канал, з якого людина вперше повідомила про ситуацію, не обов’язково є безпечним для подальшої комунікації. Тому ще до змістовного обговорення необхідно визначити безпечний спосіб, час і формат наступного контакту. Збирання

інформації доцільно здійснювати поетапно, обмежуючись на початку тими відомостями, які потрібні для оцінки безпосередньої небезпеки та організації наступної дії. Такий підхід зменшує ризик повторної травматизації, надмірного накопичення чутливих даних і необґрунтованого втручання у приватність.

Цифрові системи перенаправлення здатні зменшити фрагментарність допомоги, однак сама інформаційна система не є механізмом перенаправлення. Вона лише підтримує організаційні процедури, у межах яких мають бути визначені відповідальні суб'єкти, обсяг необхідних даних, порядок отримання згоди та відповідальність за подальшу дію. Статуси в таких системах доцільно формулювати як характеристику стану послуги, а не поведінки постраждалої особи. Аналогічно цифрова координація має контролювати виконання обов'язків установами, а не перетворюватися на спостереження за самою людиною.

Використання цифрових технологій у процесі відновлення та реінтеграції доцільно оцінювати через їхню здатність підтримувати безперервність психологічної, медичної, правової, освітньої та професійної допомоги. Разом із тим цифровий формат не повинен ставати обов'язковою умовою отримання послуг або створювати нову залежність від спеціалізованої платформи чи працівника служби. Кінцевим орієнтиром має залишатися поступове відновлення здатності людини самостійно користуватися державними, фінансовими, освітніми, професійними та комунікаційними сервісами.

Окремим результатом проведеного аналізу є обґрунтування необхідності розглядати цифрову безпеку постраждалої особи як складову загальної системи захисту. Припинення фізичного контролю не означає автоматичного припинення доступу до електронної пошти, номера телефону, хмарних сервісів, геолокації, соціальних мереж чи інших цифрових ресурсів. Водночас стандартна порада негайно змінити всі паролі, видалити підозрілі застосунки або скинути пристрій не може вважатися універсально безпечною: різкі зміни можуть бути помічені особою, яка здійснює контроль, або призвести до втрати потенційно значущих матеріалів.

У зв’язку з цим у дослідженні запропоновано авторську модель **індивідуального цифрового плану безпеки постраждалої особи**. Вона передбачає не стандартну послідовність технічних дій, а визначення пріоритетів з урахуванням конкретної ситуації, взаємозв’язків між акаунтами, номером телефону, пристроями, хмарними сервісами, геолокацією та резервними каналами зв’язку. Основним критерієм такого плану є не максимальна швидкість технічних змін, а їхня сумісність із реальною безпекою людини.

Цифрові сервіси мають також враховувати неоднакові можливості користувачів. Діти, особи з інвалідністю, люди з мовними чи когнітивними бар’єрами, низьким рівнем цифрової грамотності або без власного пристрою не повинні опинятися за межами системи допомоги через її технічну організацію. Універсальність сервісу в цьому контексті означає не однаковий шлях для всіх, а наявність кількох функціонально рівноцінних способів досягнення тієї самої мети.

Правові, етичні та безпекові вимоги до цифрових сервісів мають формуватися вже на етапі їх проєктування. Мінімізація даних, прозорість, поінформована згода, доступність, privacy by design, safety by design, орієнтація на постраждалу особу, застосування травма-інформованих принципів і людський контроль повинні діяти не як окремі додаткові заходи, а як взаємопов’язана система.

Автоматизація та штучний інтелект можуть бути корисними для навігації, надання стандартної інформації і маршрутизації звернень, однак не повинні самостійно визначати статус постраждалої особи, достовірність її повідомлення, рівень «надійності» або право на доступ до допомоги. Рішення, здатні істотно вплинути на безпеку людини, мають залишатися під контролем компетентного фахівця.

Значення цифрових технологій у сфері профілактики торгівлі людьми та підтримки постраждалих визначається не кількістю впроваджених платформ, чат-ботів або автоматизованих функцій, а тим, наскільки вони зменшують бар’єри між людиною і реальною допомогою.

Ключовим принципом запропонованого підходу є перехід від цифровізації послуг до цифрової автономії людини. Саме цей орієнтир дає змогу поєднати профілактику, доступ до допомоги, захист і реінтеграцію в єдину людиноцентричну модель протидії торгівлі людьми в цифровому середовищі.

У цьому розділі свідомо не оцінювалися кількісна результативність окремих цифрових рішень, їхня порівняльна ефективність, економічна доцільність або система формальних показників. Ці питання потребують іншого методологічного інструментарію і становлять предмет наступного розділу монографії.

РОЗДІЛ 8. МЕТОДОЛОГІЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЦИФРОВИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

8.1. Поняття та критерії ефективності цифрової протидії

Цифрова трансформація правоохоронної діяльності істотно змінила підходи до виявлення, документування, аналізу та розслідування кримінальних правопорушень, пов’язаних із торгівлею людьми. Сучасна торгівля людьми дедалі частіше має транснаціональний, мережевий та цифровий характер: вербування може здійснюватися через соціальні мережі, месенджери, онлайн-платформи працевлаштування, сайти знайомств, рекламні майданчики та інші інформаційні ресурси. Відповідно, ефективна протидія цьому явищу потребує не лише традиційних оперативно-розшукових і криміналістичних методів, а й системного використання інформаційно-аналітичних систем, технологій штучного інтелекту, інтелектуального аналізу даних, геоінформаційних систем, засобів цифрової криміналістики та технологій автоматизованого виявлення взаємозв’язків між інформаційними об’єктами.

Нормативно-правовою основою оцінювання результативності цифрових інструментів у зазначеній сфері є Закон України «Про протидію торгівлі людьми», який визначає організаційні та правові засади протидії цьому явищу, а також механізми захисту прав осіб, які постраждали від торгівлі людьми [6]. Методологія оцінювання не може обмежуватися лише показниками кількості виявлених випадків або результатами кримінального переслідування. Вона має враховувати своєчасність виявлення відповідних ознак, якість інформації, повноту аналітичної картини, достовірність отриманих результатів, можливість їх використання у процесуальній діяльності, захищеність інформаційних ресурсів, а також дотримання прав і свобод людини.

Особливого значення в цьому контексті набуває Державна цільова соціальна програма протидії торгівлі людьми на період до 2030 року, затверджена розпорядженням Кабінету Міністрів України від 3 вересня 2026 р. № 875-р. Програма орієнтована на удосконалення механізму запобігання та

протидії торгівлі людьми, своєчасне виявлення постраждалих, захист їхніх прав, надання комплексної допомоги, недопущення вторинної віктимізації та забезпечення притягнення винних осіб до відповідальності. Важливо, що документ передбачає визначення очікуваних результатів виконання програми, тобто закладає результативні та вимірювані підходи до оцінювання державної політики у цій сфері [97].

Отже, ефективність цифрової протидії торгівлі людьми доцільно розглядати як комплексну характеристику спроможності інформаційно-аналітичної системи забезпечувати отримання релевантної, достовірної та своєчасної інформації, перетворювати її на аналітичні висновки, підтримувати прийняття обґрунтованих рішень та сприяти досягненню визначених правових і безпекових результатів при одночасному забезпеченні законності, захисту персональних даних і кіберстійкості системи.

8.1.1. Поняття ефективності інформаційно-аналітичної системи

Інформаційно-аналітична система у сфері протидії торгівлі людьми являє собою сукупність організаційних, програмно-технічних, інформаційних, алгоритмічних та аналітичних компонентів, призначених для накопичення, оброблення, зіставлення, візуалізації та інтерпретації даних, необхідних для виявлення, попередження та розслідування відповідних кримінальних правопорушень. На відміну від традиційної інформаційної системи, основним результатом функціонування інформаційно-аналітичної системи є отримання нової інформації та знань, придатних для прийняття рішень.

У цьому аспекті особливого значення набувають методи інтелектуального аналізу даних. У навчальному посібнику Д. В. Ланде, І. Ю. Субача та Ю. Є. Бояринової розглядаються алгоритми класифікації, кластерного аналізу, пошуку закономірностей, Data Mining та аналізу складних мереж, що безпосередньо створює методологічну основу для побудови аналітичних механізмів у сфері кібербезпеки [107].

У контексті протидії торгівлі людьми це означає можливість перейти від ізольованого аналізу окремих повідомлень до виявлення прихованих

закономірностей у сукупності різнорідних даних. Наприклад, окремо взята інформація про оголошення щодо працевлаштування, переміщення особи, телефонні контакти, банківські операції, використання певних транспортних маршрутів або активність у соціальних мережах може не містити достатніх підстав для формування обґрунтованого висновку. Проте їх просторове, часове та мережеве зіставлення дозволяє виявити стійку сукупність ознак, характерну для певної схеми експлуатації.

Таким чином, ефективність інформаційно-аналітичної системи не слід ототожнювати лише з її технічною продуктивністю. Швидкодія серверів, обсяг сховища або кількість одночасно оброблених записів є важливими, однак вони мають допоміжне значення. Виважливим є те, наскільки технологічний комплекс сприяє досягненню кінцевої мети діяльності уповноважених суб'єктів.

З методологічного погляду ефективність можна представити як функцію декількох взаємопов'язаних характеристик:

$$E = f(O, T, P, D, C), \tag{8.1}$$

де E – загальна ефективність інформаційно-аналітичної системи; O – оперативність; T – точність; P – повнота; D – доказовість; C – кіберстійкість.

При цьому жоден із компонентів не може розглядатися ізольовано. Висока швидкість роботи системи за низької точності може призводити до значної кількості хибних спрацювань. Висока точність за надмірної тривалості аналізу може знижувати практичну цінність результату. Повна інформаційна картина без належної доказової якості також не гарантує можливості використання отриманих відомостей.

Відповідно, ефективна система має забезпечувати оптимальне співвідношення між зазначеними характеристиками.

Використання цифрових технологій у протидії торгівлі людьми передбачає оброблення значного обсягу інформації про фізичних осіб, тому технологічна результативність не може досягатися шляхом необмеженого накопичення персональних даних. Закон України «Про захист персональних даних» встановлює правові відносини у сфері оброблення персональних даних та

спрямований на захист основоположних прав і свобод людини у зв'язку з такою обробкою [10]. Отже, ефективною слід вважати не ту систему, яка збирає максимально можливу кількість інформації, а ту, яка забезпечує достатність і релевантність даних відповідно до визначеної мети їх використання.

8.1.2. Критерії оперативності

Оперативність є важливим критерієм оцінювання цифрової протидії торгівлі людьми. Вона характеризує здатність системи своєчасно виявити потенційно небезпечну подію, обробити пов'язану з нею інформацію, сформувати аналітичний сигнал та передати його відповідальному суб'єкту для прийняття рішення.

Важливість цього критерію у тому, що торгівля людьми є динамічним кримінальним явищем. Зволікання з виявленням відповідних ознак може призвести до переміщення постраждалої особи, зміни каналів комунікації, видалення цифрових слідів, зміни місця знаходження правопорушників або втрати інших важливих відомостей. Тому інформація, отримана із запізненням, може мати значно нижчу практичну цінність, навіть якщо вона є достовірною.

Оперативність доцільно характеризувати декількома часовими показниками. Першим є час виявлення – проміжок від моменту появи відповідної інформаційної ознаки до її автоматичного або операторського виявлення. Другим є час аналітичної обробки – період, необхідний для перевірки та зіставлення отриманих даних. Третім є час реагування – проміжок від моменту формування аналітичного сигналу до початку відповідних організаційних чи процесуальних дій.

Узагальнений показник оперативності може визначатися як:

$$O = \frac{T_{max} - T_{\text{fact}}}{T_{max} - T_{min}}, \qquad (8.2)$$

де T_{fact} – фактичний час реагування, T_{min}– найкраще досягнуте значення, T_{max} – гранично допустиме значення.

Чим ближче значення O до одиниці, тим вищою є оперативність системи.

У цифровому середовищі оперативність залежить не лише від обчислювальної потужності. Вона визначається архітектурою інформаційного

обміну, можливістю автоматичного отримання даних, швидкістю інтеграції різних джерел, ефективністю алгоритмів фільтрації та пріоритезації подій, а також якістю інтерфейсу взаємодії аналітика із системою.

Практична значущість оперативності підтверджується й нормативними підходами у сфері кібербезпеки. Стратегія кібербезпеки України орієнтує на підвищення спроможності до ефективної протидії загрозам, їх швидкого виявлення та розслідування, а також передбачає оцінювання результативності за допомогою системи індикаторів [105]. Аналогічний підхід застосовується і щодо інформаційно-аналітичних систем протидії торгівлі людьми.

8.1.3. Критерії точності

Точність характеризує ступінь відповідності сформованих системою аналітичних висновків фактичному стану досліджуваної ситуації. Для систем протидії торгівлі людьми цей критерій має принципове значення, оскільки помилкове віднесення особи, події або організації до ризикової категорії може мати серйозні правові та соціальні наслідки.

З позицій машинного навчання та Data Mining точність безпосередньо пов’язана з якістю класифікації. Під час побудови моделей можуть використовуватися різні методи класифікації, кластеризації та пошуку закономірностей [107]. Алгоритмічний результат не повинен автоматично ототожнюватися з юридично значущим висновком. Алгоритм формує аналітичну оцінку або сигнал, який потребує перевірки уповноваженою особою.

Для кількісного оцінювання точності доцільно використовувати показники, засновані на матриці помилок: True Positive, True Negative, False Positive та False Negative. Одним із базових показників є precision:

$$Precision = \frac{TP}{TP + FP}, \tag{8.3}$$

де TP – кількість правильно виявлених позитивних випадків, FP – кількість помилково визначених позитивних випадків.

Іншим важливим показником є *recall*:

$$Recall = \frac{TP}{TP + FN}, \tag{8.4}$$

де *FN* – кількість випадків, які система не виявила, хоча вони фактично належали до досліджуваної категорії.

Для інтегрованого оцінювання може застосовуватися F1-score:

$$F1 = 2\frac{Precision * Recall}{Precision + Recall}, \quad (8.5)$$

Застосування таких показників дозволяє перейти від суб'єктивного твердження «система працює добре» до кількісної оцінки її аналітичної спроможності.

Разом із тим точність алгоритму не є тотожною достовірності юридичного висновку. Наприклад, алгоритм може з високою точністю виявляти схожість між текстами оголошень, але сама текстова схожість ще не доводить факту торгівлі людьми. Вона є лише аналітичною ознакою, яка може бути використана для формування версії або визначення пріоритету подальшої перевірки.

Тому у правоохоронній системі застосовують багаторівневу модель точності. На першому рівні оцінюється технічна точність алгоритму; на другому – достовірність аналітичного висновку; на третьому – підтвердження висновку незалежними джерелами; на четвертому – можливість його використання у процесуальній діяльності.

Модель, навчена на неповних або репрезентативно обмежених даних, може систематично переоцінювати ризики щодо певних груп або регіонів. Тому оцінювання точності повинно передбачати тестування на незалежних вибірках, регулярне оновлення навчальних даних та контроль стабільності моделі.

8.1.4. Критерії повноти

Повнота характеризує ступінь охоплення системою інформації, необхідної для формування об'єктивного уявлення про досліджуване явище. У контексті протидії торгівлі людьми цей критерій має щонайменше три виміри: повнота джерел, повнота інформаційних зв'язків та повнота аналітичного результату.

Повнота джерел означає здатність системи отримувати інформацію з різних типів каналів: відкритих джерел, інформаційних систем державних органів, реєстрів, цифрових комунікацій, геопросторових даних, матеріалів

криміналістичної діяльності та інших дозволених законом інформаційних ресурсів.

Повнота інформаційних зв'язків означає можливість встановлення взаємозалежності між окремими інформаційними об'єктами. Наприклад, система має бути здатною пов'язувати між собою особу, номер телефону, обліковий запис у соціальній мережі, транспортний маршрут, адресу, організацію або цифровий ідентифікатор, якщо існують достатні фактичні підстави для такого зв'язку.

Водночас повнота не повинна ототожнюватися з безконтрольним накопиченням інформації. Надмірна кількість нерелевантних даних може, навпаки, знизити ефективність аналітичної системи, оскільки збільшує інформаційний шум і ускладнює виявлення значущих закономірностей.

Методи інтелектуального аналізу даних дозволяють частково розв'язати цю проблему за рахунок класифікації, кластеризації, пошуку закономірностей і виявлення взаємозв'язків між даними [107]. Таким чином, повнота має оцінюватися не абсолютною кількістю накопиченої інформації, а ступенем достатності інформаційної бази для виконання конкретного аналітичного завдання.

Важливим є також забезпечення просторової та часової повноти. Якщо інформаційно-аналітична система аналізує діяльність злочинних мереж, необхідно враховувати динаміку подій, переміщення осіб, зміну каналів комунікації та територіальну структуру відповідних процесів.

Коефіцієнт повноти інформаційного забезпечення визначають як:

$$K_p = \frac{N_r}{N_t}, \qquad (8.6)$$

де N_r – кількість релевантних інформаційних елементів, фактично доступних для аналізу; N_t – загальна кількість релевантних елементів, необхідних для вирішення конкретного аналітичного завдання.

Однак у реальних умовах значення N_t не завжди може бути встановлено точно. Тому практичніше застосовувати еталонні набори даних, контрольні вибірки та експертно визначені переліки необхідних інформаційних атрибутів.

Повнота має безпосередній зв’язок із Data Mining. Алгоритм може бути математично досконалим, але результати його застосування будуть ненадійними, якщо вихідний набір даних містить систематичні пропуски. У такому випадку виникає класична проблема «garbage in – garbage out»: низькоякісні або неповні вхідні дані породжують низькоякісні аналітичні результати.

Особливу проблему становить дублювання інформації. Один факт може бути представлений у декількох джерелах, тому механічне підрахування записів може створювати ілюзію високої повноти. Необхідно розрізняти кількість записів та кількість унікальних інформаційних об’єктів.

Повнота також передбачає збереження історії змін. Для цифрових об’єктів важливо знати не лише їх поточний стан, а й те, як вони змінювалися в часі. Це особливо важливо для реконструкції діяльності мереж вербування, встановлення послідовності комунікацій та визначення часової структури подій.

Практичні посібники ОБСЄ з протидії торгівлі людьми акцентують увагу на необхідності належного виявлення та роботи з постраждалими, а також на взаємодії різних суб’єктів протидії [117]. Це дозволяє розглядати повноту не лише як технічну характеристику даних, а і як характеристику міжвідомчого інформаційного забезпечення.

8.1.5. Критерії доказовості

Особливе місце в оцінюванні цифрових технологій посідає доказовість. На відміну від оперативності, яка характеризує часовий аспект, або точності, яка характеризує правильність класифікації, доказовість визначає можливість використання отриманих результатів як обґрунтування відповідних висновків.

Цифрова інформація може мати різний статус залежно від способу її отримання, фіксації, збереження, перевірки та подальшого використання. Тому інформаційно-аналітична система повинна не тільки сформувати певний висновок, а й забезпечити можливість встановити походження відповідних даних.

До основних характеристик доказовості відносяться:

- встановлене джерело походження інформації;
- можливість перевірки достовірності даних;
- фіксацію часу отримання та обробки;
- збереження історії змін;
- можливість відтворення алгоритму обробки;
- документування дій користувачів;
- цілісність цифрових об’єктів;
- можливість незалежної перевірки результату.

Особливого значення набуває принцип chain of custody, тобто документованого ланцюга збереження цифрового доказу. На кожному етапі повинно бути зрозуміло, де перебував цифровий об’єкт, хто мав до нього доступ, які операції з ним здійснювалися та яким чином забезпечувалася незмінність його змісту.

Для перевірки цілісності цифрової інформації можуть використовуватися криптографічні хеш-функції. У такому випадку для цифрового об’єкта розраховується хеш-значення, яке фіксується в документації. Подальше повторне обчислення хешу дозволяє встановити, чи змінився відповідний цифровий об’єкт.

Важливим є розмежування аналітичної та доказової функцій штучного інтелекту. Результат роботи алгоритму – наприклад, оцінка ризику або виявлена аномалія – не повинен автоматично ототожнюватися з доказом факту злочину. Штучний інтелект може допомагати знаходити релевантні об’єкти, встановлювати зв’язки, ранжувати інформацію та формувати аналітичні гіпотези, але юридична оцінка повинна здійснюватися уповноваженим суб’єктом із дотриманням установлених процедур.

Сучасні українські дослідження цифрової криміналістики підкреслюють необхідність уніфікації процедур збирання, фіксації, збереження та дослідження цифрових доказів. Актуальними є питання криміналістичного копіювання, документування хеш-значень, забезпечення ланцюга збереження та належного документування всіх операцій із цифровою інформацією.

У цьому контексті доказовість цифрової системи можна визначити як ступінь, до якого результати її роботи можуть бути перевірені, відтворені, документально підтверджені та, за наявності відповідних процесуальних умов, використані для обґрунтування юридично значущих висновків.

Доцільно використовувати інтегральний показник доказової готовності:

$$D = w^1 A + w^2 I + w^3 C + w^4 R + w^5 P, \quad (8.7)$$

де A – автентичність; I – цілісність; C – повнота документування ланцюга збереження; R – відтворюваність; P – процесуальна придатність; $w_1 ... w_5$ – вагові коефіцієнти.

Такий підхід дозволяє оцінювати не лише наявність цифрових даних, а якість процедури їх перетворення на потенційно доказову інформацію.

Саме тому аналітичний висновок системи доцільно розглядати як результат інформаційно-аналітичної діяльності, який потребує відповідної верифікації.

8.1.6. Критерії кіберстійкості

Кіберстійкість є інтегральною характеристикою здатності інформаційно-аналітичної системи функціонувати, протистояти кібератакам, відновлюватися після порушень та зберігати необхідний рівень конфіденційності, цілісності й доступності інформації.

Для систем протидії торгівлі людьми цей критерій має особливе значення, оскільки такі системи можуть містити персональні дані, оперативну інформацію, відомості про постраждалих, результати аналітичної діяльності та інформацію про правоохоронні заходи. Компрометація таких даних може створити додаткові ризики для постраждалих осіб і перешкодити діяльності правоохоронних органів.

Закон України «Про основні засади забезпечення кібербезпеки України» формує нормативну основу функціонування національної системи кібербезпеки та визначає організаційні засади захисту відповідних інформаційних ресурсів [58]. Водночас Стратегія кібербезпеки України прямо пов’язує результативність кібербезпеки з розвитком кіберстійкості, швидким виявленням загроз,

реагуванням на них та постійним моніторингом індикаторів стану кібербезпеки [105].

У методологічному аспекті кіберстійкість інформаційно-аналітичної системи доцільно оцінювати за такими групами показників:

- стійкість до порушення доступності – здатність системи продовжувати функціонування в умовах відмов, перевантаження або атаки на доступність;
- стійкість до компрометації даних – здатність запобігати несанкціонованій модифікації інформації;
- стійкість до витоку інформації – спроможність захищати конфіденційні та персональні дані;
- стійкість до маніпулювання даними – здатність виявляти навмисне внесення неправдивих або спотворених відомостей;
- здатність до відновлення – час і повнота відновлення інформаційних ресурсів після інциденту;
- адаптивність – спроможність системи пристосовуватися до нових типів атак і зміни поведінки суб’єктів злочинної діяльності.

Законодавство України поширює вимоги щодо оброблення персональних даних, зокрема на діяльність, яка здійснюється із застосуванням автоматизованих засобів [10]. Тому кіберстійкість не може розглядатися виключно як технічна властивість. Вона має включати організаційні та правові механізми захисту інформації.

Для оцінювання кіберстійкості доцільно використовувати показники середнього часу виявлення інциденту, середнього часу реагування, середнього часу відновлення, частки успішно локалізованих інцидентів, кількості порушень цілісності даних та частки інформаційних ресурсів, які мають актуальні резервні копії.

Загальний показник кіберстійкості може бути представлений у вигляді нормованої функції:

$$C = w_1 C_1 + w_2 C_2 + w_3 C_3 + w_4 C_4 + w_5 C_5, \qquad (8.8)$$

де C_i– нормовані показники окремих складових кіберстійкості, w_i – вагові коефіцієнти, сума яких дорівнює одиниці.

Кіберстійкість повинна оцінюватися динамічно. Система, яка демонструє належний рівень захисту в момент первинного тестування, не може автоматично вважатися стійкою протягом тривалого часу. Зміна технологій, поява нових вразливостей, удосконалення методів соціальної інженерії та адаптація злочинців до правоохоронних практик потребують регулярного перегляду механізмів захисту.

Стратегія кібербезпеки України передбачає саме такий підхід: ефективність має визначатися за допомогою постійного моніторингу та системи індикаторів, а результати оцінювання можуть бути підставою для коригування планів реалізації відповідних заходів [105].

Тому, кіберстійкість інформаційно-аналітичної системи протидії торгівлі людьми слід розглядати як здатність не лише запобігати кібератакам, а й підтримувати достовірність аналітичного процесу в умовах навмисного впливу на інформаційне середовище.

8.2. Система показників оцінювання

Оцінювання ефективності цифрових технологій у протидії торгівлі людьми потребує переходу від загальних якісних характеристик інформаційно-аналітичної системи до системи формалізованих кількісних показників. Такий підхід дає можливість не лише встановити факт результативності певного технологічного рішення, а й порівняти між собою різні алгоритми, моделі машинного навчання, інформаційні платформи та організаційно-технологічні підходи.

Відповідно до Закону України «Про протидію торгівлі людьми», протидія цьому явищу охоплює попередження торгівлі людьми, боротьбу з нею, а також допомогу і захист постраждалих осіб [6]. При цьому процедура встановлення статусу особи, яка постраждала від торгівлі людьми, передбачає отримання та аналіз інформації, оцінювання ймовірності вчинення відповідного діяння та формування висновку уповноваженою особою [6]. Отже, цифрові технології

можуть бути використані як інструмент підвищення якості та швидкості аналітичного процесу, однак їхні результати мають оцінюватися з урахуванням фактичної правильності, повноти, своєчасності та практичної корисності.

Важливе значення для формування системи показників має Державна цільова соціальна програма протидії торгівлі людьми на період до 2030 року. У ній безпосередньо передбачено функціонування цифрової системи збору й обміну даними між суб'єктами протидії торгівлі людьми, а серед очікуваних результатів визначено підвищення результативності виявлення та розслідування злочинів, удосконалення міжвідомчої взаємодії та проведення незалежного моніторингу стану протидії торгівлі людьми [97]. Документ також встановлює конкретні цільові орієнтири, зокрема щодо частки осіб, яким встановлено відповідний статус, осіб, які отримали допомогу, та кримінальних проваджень, у яких повідомлено про підозру.

Отже, система показників повинна поєднувати алгоритмічні, часові, організаційні, ресурсні та соціально-правові характеристики. До базових показників такої системи доцільно віднести Precision, Recall, F1-score, False Positive Rate, False Negative Rate, середній час виявлення, середній час реагування, показники якості прогнозування, масштабованості та економічної ефективності.

Методологічною основою для застосування зазначених показників є інтелектуальний аналіз даних. Ланде Д. В., Субач І. Ю. та Бояринова Ю. Є. розглядають задачі класифікації, Data Mining, кластерного аналізу та моделювання складних систем як важливі компоненти сучасного аналітичного опрацювання даних [107]. Практичне застосування алгоритмів штучного інтелекту, кластеризації, дерев рішень та нейромережевих технологій також висвітлено у праці О. О. Шаповалової [110].

Таким чином, система показників оцінювання повинна розглядатися не як набір незалежних метрик, а як взаємопов'язана модель, що дозволяє визначити, наскільки цифрова технологія забезпечує досягнення практичної мети протидії торгівлі людьми.

8.2.1. Precision, Recall та F1-score

Одними з основних показників оцінювання результативності алгоритмів класифікації є Precision, Recall та F1-score. Їх використання особливо доцільне під час розроблення та тестування моделей машинного навчання, призначених для виявлення потенційно небезпечних інформаційних об'єктів, повідомлень, оголошень, профілів, комунікаційних зв'язків або інших ознак, які можуть бути пов'язані з торгівлею людьми.

Методологічно зазначені показники ґрунтуються на чотирьох базових результатах класифікації:

- True Positive (TP) – кількість випадків, які система правильно визначила як позитивні;
- True Negative (TN) – кількість випадків, які система правильно визначила як негативні;
- False Positive (FP) – кількість негативних випадків, помилково класифікованих як позитивні;
- False Negative (FN) – кількість позитивних випадків, які система помилково визначила як негативні.

Таке представлення дозволяє сформувати матрицю помилок, яка є основою для подальшого розрахунку основних метрик.

Показник *Precision* (8.3) характеризує частку правильних позитивних прогнозів серед усіх випадків, які система визначила як позитивні:

Чим вище значення *Precision*, тим менше система формує хибних позитивних сигналів. Для інформаційно-аналітичної системи протидії торгівлі людьми цей показник характеризує, наскільки обґрунтованими є сформовані системою сигнали про потенційну наявність відповідних ознак.

Наприклад, якщо система проаналізувала 100 інформаційних об'єктів і 40 із них класифікувала як потенційно пов'язані з торгівлею людьми, але лише 30 згодом підтвердили відповідність визначеним критеріям, *Precision* становитиме:

$$Precision = \frac{30}{30+10} = 0{,}75, \tag{8.9}$$

Отже, точність позитивних прогнозів становить 75 %.

Для протидії торгівлі людьми важливим є не лише уникнення хибних спрацювань, а й недопущення пропуску реальних випадків. Саме це характеризує показник *Recall* (8.4)*:*

Recall показує, яку частку всіх фактично позитивних випадків система змогла виявити.

Наприклад, якщо у тестовій вибірці було 50 реальних випадків, а алгоритм виявив 40 із них, то:

$$Recall = \frac{40}{40 + 10} = 0{,}80, \tag{8.10}$$

Система забезпечила виявлення 80 % позитивних випадків.

Пропуск реального ризику або потенційного постраждалого може мати значно серйозніші наслідки, ніж додаткова перевірка помилково визначеного сигналу. Надмірне збільшення *Recall* за рахунок зниження *Precision* може призвести до інформаційного перевантаження аналітичних підрозділів.

Для комплексного врахування *Precision* та *Recall* використовується *F1-score* (8.5):

Застосування F1-score є доцільним у ситуаціях, коли просте використання Accuracy може створювати викривлене уявлення про якість моделі. Наприклад, якщо в дуже великій вибірці лише невелика частина об’єктів реально пов’язана з досліджуваною категорією, алгоритм, який майже завжди прогнозує негативний клас, може демонструвати високу загальну точність, але фактично бути непридатним для виявлення цільових випадків.

Підходи до класифікації та інтелектуального аналізу даних, які становлять методологічну основу використання зазначених метрик, розглядаються у навчальному посібнику Ланде, Субача та Бояринової [107]. Автори розглядають класифікаційні задачі, алгоритмічний аналіз і моделювання складних інформаційних систем у контексті кібербезпеки. Практичний аспект побудови моделей машинного навчання, зокрема кластеризації та дерев рішень, представлено також у роботі Л. М. Олещенко [108].

Для оцінювання цифрових технологій у протидії торгівлі людьми доцільно використовувати всі три показники одночасно. Їх функціональне призначення можна представити таким чином:

Таблиця 8.1

Функціональне призначення показників

Показник	**Що характеризує**	**Практичне значення**
Precision	Якість позитивних прогнозів	Зменшення кількості хибних сигналів
Recall	Повноту виявлення	Мінімізація пропущених випадків
F1-score	Баланс Precision і Recall	Комплексне порівняння моделей

Конкретні порогові значення цих показників не можуть бути однаковими для всіх моделей. Вони повинні встановлюватися з урахуванням призначення алгоритму, типу даних, вартості помилок та наслідків прийняття рішень.

8.2.2. False Positive Rate та False Negative Rate

Для поглибленого оцінювання алгоритмічних систем недостатньо визначати лише Precision та Recall. Варто окремо враховувати характер помилок, оскільки різні типи помилкової класифікації можуть мати принципово різні наслідки.

False Positive Rate (FPR) визначає частку негативних випадків, які система помилково класифікувала як позитивні:

$$FPR = \frac{FP}{FP + T\,N}, \tag{8.11}$$

Значення *FPR* характеризує схильність системи до формування хибних позитивних сигналів.

У практичній діяльності інформаційно-аналітичного підрозділу високий *FPR* може призводити до перевантаження операторів, збільшення кількості ручних перевірок, нераціонального використання ресурсів та формування

необґрунтованої уваги до інформаційних об’єктів, які фактично не становлять відповідного ризику.

У системах, що використовують OSINT, автоматичний моніторинг веб-ресурсів або соціальних мереж, проблема *FPR* набуває особливої актуальності. Велика кількість рекламних повідомлень, вакансій, повідомлень користувачів або мережевих взаємозв’язків може мати формальні ознаки, подібні до ознак ризикової поведінки, але не бути пов’язаною з торгівлею людьми.

Водночас **False Negative Rate (FNR)** характеризує частку позитивних випадків, які система не виявила:

$$FNR = \frac{FN}{TP + FN} \tag{8.12}$$

Між *FNR* та *Recall* існує безпосередній взаємозв’язок:

$$F\,FNR = 1 - Recall\,. \tag{8.13}$$

Отже, підвищення *Recall* автоматично означає зменшення *FNR*.

Для систем протидії торгівлі людьми *FNR* може бути критично важливим показником, оскільки кожен пропущений системою випадок потенційно може означати невиявлений ризик для людини або пропущений елемент злочинної схеми.

Водночас це не означає, що *FNR* необхідно мінімізувати за будь-яку ціну. Зниження *FNR* може супроводжуватися збільшенням *FPR*. Тому вибір оптимального порога класифікації повинен ґрунтуватися на співвідношенні наслідків двох типів помилок.

У загальному вигляді це співвідношення можна описати функцією вартості помилок:

$$L = CFP \cdot FP + CFN \cdot FN\,, \tag{8.14}$$

де *CFP* – умовна вартість хибнопозитивного результату, а *CFN* – умовна вартість хибнонегативного результату.

Для систем раннього виявлення ризиків торгівлі людьми зазвичай доцільно передбачати вищу вагу *FNR*, оскільки пропуск потенційно небезпечної ситуації може мати значні наслідки. Проте остаточне співвідношення повинно визначатися конкретним завданням, типом системи та правовими обмеженнями.

Методи Data Mining, класифікації, кластеризації та аналізу складних мереж створюють технологічну основу для такого оцінювання [107]. Практичне застосування алгоритмів штучного інтелекту та різних методів обробки даних дозволяє проводити порівняльне тестування моделей та визначати, як зміна параметрів алгоритму впливає на характер помилок [108, 110].

Отже, *FPR* і *FNR* повинні розглядатися не лише як технічні показники якості алгоритму, а як інструменти управління ризиком автоматизованої аналітики.

8.2.3. Час виявлення загрози

Час виявлення загрози є одним із ключових показників практичної ефективності цифрової системи. Він характеризує часовий інтервал між виникненням або появою інформаційної ознаки потенційної загрози та моментом її виявлення системою.

У найпростішому випадку:

$$T_{detect} = t_{detect} - t_{event}, \tag{8.15}$$

де t_{event} – момент виникнення події або появи відповідної інформації, а t_{detect} – момент її виявлення.

Чим менше значення T_{detect}, тим вищою є оперативність системи.

Для протидії торгівлі людьми скорочення часу виявлення має особливе значення через динамічний характер відповідних процесів. Інформаційні сліди можуть швидко змінюватися або видалятися, комунікаційні канали – припиняти функціонування, а особи – переміщуватися між територіями.

Тому цифрова система повинна забезпечувати не лише періодичний аналіз інформації, а, за можливості, безперервний або наближений до реального часу моніторинг релевантних джерел.

Показник часу виявлення доцільно аналізувати не лише як середнє арифметичне значення, а й за допомогою медіани, 90-го або 95-го перцентиля. Це дозволяє врахувати випадки, коли незначна кількість надзвичайно повільних операцій істотно впливає на середнє значення.

Наприклад, система може мати середній час виявлення 12 хвилин, однак 10 % подій обробляти понад годину. Для оперативної діяльності така ситуація є принципово іншою, ніж випадок, коли 95 % подій виявляються протягом 15 хвилин.

Доцільно використовувати такі показники:

$$T_{avg} = \frac{1}{n} \sum_{i=1}^{i} T_{detec,i}, \tag{8.16}$$

Актуальність скорочення часу виявлення узгоджується з національними підходами до кібербезпеки. Стратегія кібербезпеки України орієнтується на підвищення спроможностей щодо протидії кіберзагрозам, досягнення кіберстійкості та забезпечення ефективної взаємодії суб'єктів кібербезпеки [105]. Подібний принцип доцільно застосовувати до цифрових систем протидії торгівлі людьми.

Особливо важливим є розмежування часу збору даних, часу їх обробки та часу формування сигналу. У складній інформаційно-аналітичній системі загальна затримка може виникати на будь-якому з цих етапів.

Тому:

$$T_{detect} = T_{collect} + T_{transfer} + T_{process} + T_{analysis}, \tag{8.17}$$

Такий підхід дозволяє визначити вузьке місце системи та встановити, на якому етапі виникають найбільші часові втрати.

8.2.4. Час реагування

Якщо час виявлення характеризує здатність системи сформувати сигнал, то час реагування характеризує період між отриманням такого сигналу та початком відповідних дій.

Його можна представити як:

$$T_{response} = t_{action} - t_{alert}, \tag{8.18}$$

де t_{alert}– момент формування або передачі сигналу, а t_{action} – момент початку реагування.

Загальний час від появи загрози до реагування можна представити:

$$T_{total} = T_{detect} + T_{response} \ , \tag{8.19}$$

Автоматизація аналітичного процесу не гарантує автоматичного скорочення часу реагування. Якщо сформований системою сигнал передається із затримкою, не має достатнього контексту або потребує тривалої ручної перевірки, перевага автоматичного виявлення може бути втрачена.

Тому ефективна інформаційно-аналітична система повинна забезпечувати:

- автоматичне формування пріоритетів;
- ранжування сигналів за рівнем ризику;
- передачу повідомлень відповідальним працівникам;
- формування контексту навколо виявленої події;
- відображення пов'язаних інформаційних об'єктів;
- фіксацію часу отримання та опрацювання сигналу;
- контроль виконання відповідних дій.

Державна цільова соціальна програма протидії торгівлі людьми до 2030 року передбачає посилення спроможності правоохоронних органів і судів, підвищення ефективності розслідувань, покращення координації та міжвідомчої взаємодії [97]. Отже, час реагування має оцінюватися не лише на рівні програмного забезпечення, а як характеристика всього організаційно-технологічного процесу.

Доцільно розрізняти:

$$T_{response} = T_{verification} + T_{decision} + T_{action} \ , \tag{8.20}$$

де $T_{verification}$ – час перевірки сигналу, $T_{decision}$ – час прийняття рішення, T_{action} – час фактичного початку реагування.

Таке розкладання дозволяє встановити, чи проблема полягає у роботі алгоритму, інформаційному забезпеченні аналітика або в організаційній процедурі.

8.2.5. Якість прогнозування

Наступним важливим напрямом оцінювання є якість прогнозування. Якщо класифікація відповідає на питання про те, до якої категорії належить певний об'єкт, прогнозування спрямоване на визначення ймовірності майбутньої події або розвитку певного сценарію.

У сфері протидії торгівлі людьми прогнозні моделі можуть використовуватися для визначення:

- територій підвищеного ризику;
- часових періодів зростання відповідних ризиків;
- інформаційних каналів, які можуть використовуватися для вербування;
- потенційних зв'язків між учасниками злочинних мереж;
- ризикових характеристик оголошень про працевлаштування;
- ймовірності повторення певного сценарію.

Прогнозована модель не повинна використовуватися як автоматичний інструмент прийняття юридично значущого рішення щодо конкретної особи. Її призначення полягає у визначенні пріоритетів для подальшого аналізу.

Якість прогнозування може оцінюватися за допомогою MAE, MSE, RMSE, коефіцієнта детермінації R^2 – залежно від характеру задачі. Для ймовірнісної класифікації додатково доцільно оцінювати калібрування прогнозованих ймовірностей.

Середня абсолютна похибка визначається:

$$MAE = \frac{1}{n}\sum_{i=1}^{n}\left|y_i - \hat{y}_i\right|, \tag{8.21}$$

де y_i – фактичне значення, а $\hat{y}_i$ – прогнозоване значення.

Середньоквадратична похибка:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(y_i - \hat{y}_i\right)^2, \tag{8.22}$$

Корінь із середньоквадратичної похибки:

$$RMSE = \sqrt{MSE}. \tag{8.23}$$

У контексті інтелектуального аналізу даних важливо правильно сформувати навчальну та тестову вибірки. Посібник Ланде, Субача та Бояринової наголошує на комплексному характері Data Mining, що поєднує класифікацію, моделювання, аналіз складних систем та інші методи обробки інформації [107]. Практичні підходи до машинного навчання, зокрема використання кластеризації та дерев рішень, представлені Олещенко [108].

Особливу проблему становить зміна структури даних у часі. Поведінка злочинців може змінюватися у відповідь на діяльність правоохоронних органів, технологічні зміни або суспільно-політичні умови. Тому модель, яка продемонструвала високі показники на історичних даних, може втрачати ефективність при роботі з новими даними.

Отже, якість прогнозування необхідно оцінювати не одноразово, а періодично, використовуючи актуальні контрольні вибірки.

8.2.6. Масштабованість системи

Масштабованість характеризує здатність інформаційно-аналітичної системи зберігати прийнятні показники продуктивності при збільшенні обсягу даних, кількості користувачів, кількості джерел або складності аналітичних операцій.

Для цифрових систем протидії торгівлі людьми масштабованість є актуальною, оскільки сучасні інформаційні середовища генерують значні обсяги структурованих і неструктурованих даних. До них можуть належати текстові повідомлення, веб-сторінки, соціальні мережі, зображення, геопросторові дані, журнали подій та інші інформаційні масиви.

Методи Data Mining та інтелектуального аналізу дозволяють працювати з великими масивами даних, однак зі збільшенням їх обсягу зростають вимоги до обчислювальних ресурсів, архітектури сховищ та алгоритмів [107, 110].

Масштабованість можна оцінювати за такими показниками:

- максимальний обсяг даних, що обробляється за одиницю часу;
- кількість одночасних користувачів;
- кількість підключених інформаційних джерел;
- середній час виконання запиту;
- пропускна здатність;
- використання CPU, RAM та дискового простору;
- час масштабування системи;
- вартість збільшення продуктивності.

Один із базових показників можна представити:

$$T_{hroughput} = \frac{N}{T}, \tag{8.24}$$

де N – кількість оброблених інформаційних об’єктів, T – час їх обробки.

При цьому важливо оцінювати не тільки вертикальне, а й горизонтальне масштабування. Вертикальне масштабування передбачає збільшення ресурсів окремого сервера, тоді як горизонтальне – додавання нових обчислювальних вузлів.

Для інформаційно-аналітичної системи державного або міжвідомчого рівня перевагою є архітектура, яка дозволяє збільшувати потужність без істотної перебудови всієї системи.

Окремим аспектом є масштабованість аналітичних алгоритмів. Алгоритм, який ефективно працює на десятках тисяч записів, може виявитися непридатним для мільйонів об’єктів. Тому під час експериментальної перевірки доцільно використовувати набори даних різного обсягу та аналізувати залежність часу виконання від розміру вибірки.

Для геоінформаційного компонента системи масштабованість означає можливість одночасного аналізу значних масивів просторових і часових даних. Зокрема, може виникати необхідність зіставлення інформації про переміщення, місця вербування, маршрути, транспортні вузли, прикордонні території та інші просторові об’єкти. У таких випадках ефективність GIS-модуля повинна оцінюватися не тільки за точністю просторового аналізу, а й за часом обробки геоданих та можливістю інтеграції різнорідних джерел.

Важливим є також забезпечення горизонтального масштабування, за якого збільшення обчислювальних ресурсів дає змогу пропорційно збільшувати обсяг оброблюваної інформації. Для державних інформаційних систем це повинно поєднуватися з вимогами кібербезпеки та захисту інформації.

Важливе значення має постанова Кабінету Міністрів України від 31 грудня 2025 р. № 1799, якою затверджено Порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем. Документ передбачає оцінювання поточного стану кіберзахисту,

оцінювання відповідності національним стандартам та оцінку стану захищеності державних інформаційних ресурсів.

Особливо актуально це у зв'язку з передбаченим Державною програмою до 2030 року функціонуванням цифрової системи збору та обміну даними між суб'єктами протидії торгівлі людьми [97].

8.2.7. Економічна ефективність

Технічна результативність цифрової технології не є достатньою умовою її практичного впровадження. Навіть алгоритм, який забезпечує високі показники Precision, Recall та F1-score, може бути економічно недоцільним, якщо витрати на його функціонування перевищують отримуваний ефект.

Тому завершальним компонентом системи показників є економічна ефективність.

Її доцільно розглядати як співвідношення між ресурсами, витраченими на розроблення, впровадження та експлуатацію технології, і результатами, отриманими внаслідок її застосування.

Загальний коефіцієнт економічної ефективності може визначатися:

$$E_{econ} = \frac{B - C}{C}, \tag{8.25}$$

де B – економічний ефект від використання технології, C – сукупні витрати.

До витрат відносять:

- придбання або розроблення програмного забезпечення;
- серверне та мережеве обладнання;
- хмарні ресурси;
- ліцензійні платежі;
- витрати на зберігання даних;
- технічну підтримку;
- інформаційну безпеку;
- підготовку персоналу;
- оновлення алгоритмів;
- аудит і тестування системи.

Економічний ефект не обмежується прямою фінансовою економією. У сфері протидії торгівлі людьми важливими результатами є скорочення часу аналітичної роботи, зменшення кількості ручних операцій, підвищення кількості своєчасно виявлених ризиків, зменшення кількості пропущених випадків, покращення міжвідомчої взаємодії та підвищення ефективності використання ресурсів.

Тому доцільно використовувати показник вартості одного результативного виявлення:

$$C_{detect} = \frac{C_{total}}{N_{TP}}, \tag{8.26}$$

де C_{total} – сукупні витрати на функціонування системи за визначений період, N_{TP} – кількість правильно виявлених позитивних випадків.

Такий показник дозволяє порівнювати різні технологічні рішення не лише за абсолютними витратами, а й за кількістю реально корисних результатів.

Для порівняння традиційного та цифрового підходів може застосовуватися:

$$E_{saving} = \frac{C_{traditional} - C_{digital}}{C_{traditional}} \times 100\%, \tag{8.27}$$

У сфері протидії торгівлі людьми не можна застосовувати суто комерційну модель «вартість–прибуток». Частина результатів цифрової системи має соціальну та правозахисну природу і не може бути повністю виражена у грошовому еквіваленті.

Саме тому економічний показник повинен розглядатися у взаємозв’язку з результативністю. Якщо система зменшує витрати, але водночас збільшує кількість пропущених випадків або створює надмірну кількість необґрунтованих сигналів, її не можна вважати ефективною.

Державна цільова соціальна програма протидії торгівлі людьми до 2030 року передбачає фінансування заходів із державного та місцевих бюджетів, міжнародної технічної допомоги та інших не заборонених законодавством джерел; при цьому прогнозний обсяг фінансування програми визначено на рівні

141 570,5 тис. грн [97]. Це додатково підтверджує необхідність оцінювання не лише технологічної, а й ресурсної ефективності відповідних цифрових рішень.

Узагальнено економічну ефективність цифрової системи можна представити як функцію:

$$E_{econ} = f\left(C_{implementation}, C_{operation}, T_{saved}, N_{TP}, Q_{decision}\right), \quad (8.28)$$

де $C_{implementation}$ – витрати на впровадження, $C_{operation}$ – експлуатаційні витрати, T_{saved} – заощаджений робочий час, N_{TP} – кількість правильно виявлених випадків, $Q_{decision}$ – якість підтримки управлінських рішень.

Таблиця 8.2

Узагальнена модель системи показників

Група	Основні показники	Основне призначення
Якість класифікації	Precision, Recall, F1-score	Оцінювання правильності та повноти виявлення
Помилки	FPR, FNR	Оцінювання ризиків хибної класифікації
Оперативність	T_{detect}, $T_{response}$	Оцінювання швидкості виявлення і реагування
Прогнозування	MAE, MSE, RMSE, R^2R	Оцінювання прогнозних моделей
Масштабованість	Throughput, latency, resource utilization	Оцінювання роботи при збільшенні навантаження
Економічність	ROI, C_{detect}, економія часу	Оцінювання ресурсної доцільності
Практична результативність	кількість підтверджених випадків, частка результативних сигналів	Оцінювання реального внеску системи

Наведені показники не повинні застосовуватися механічно. Для різних функціональних компонентів цифрової системи вагомість окремих критеріїв буде різною. Наприклад, для модуля автоматизованого аналізу OSINT-даних критичними можуть бути Recall, Precision і час виявлення; для прогнозної моделі – якість прогнозування та стабільність результатів на нових даних; для інтегрованої платформи – масштабованість, час реагування, надійність та економічна ефективність.

Відповідно, комплексний показник ефективності може бути сформований як зважена сума нормованих показників:

$$E_{integral} = \sum_{i=1}^{n} \omega_i X_i, \tag{8.29}$$

Де X_i– нормовані значення окремих показників, ω_i – їх вагові коефіцієнти, причому:

$$\sum_{i=1}^{n} \omega_i = 1. \tag{8.30}$$

Застосування такої моделі потребує попереднього визначення пріоритетів. Для систем раннього виявлення ризиків доцільно надати більшої ваги Recall і часу виявлення, тоді як для систем аналітичної підтримки розслідування вагомішими можуть бути Precision, доказовість та якість прогнозування.

При цьому інтегральний показник не повинен приховувати критичні недоліки окремих компонентів. Наприклад, висока економічна ефективність не може компенсувати неприпустимо високий FNR, якщо система використовується для раннього виявлення потенційних постраждалих. Аналогічно, висока точність моделі не може компенсувати неприйнятно тривалий час обробки даних у ситуаціях, що потребують оперативного реагування.

Отже, доцільно використовувати дворівневу систему оцінювання: на першому рівні визначати мінімально допустимі значення критичних показників, а на другому – розраховувати інтегральний показник для порівняння технологічних рішень.

Запропонована система показників створює методологічну основу для порівняльного експериментального оцінювання цифрових технологій, що передбачає формування контрольних і тестових вибірок, проведення серії експериментів, статистичну перевірку отриманих результатів та порівняння традиційних і цифрових підходів. Саме ці питання становлять предмет подальших підрозділів методології оцінювання.

8.3. Оцінювання ефективності окремих технологічних компонентів

Ефективність цифрових технологій у протидії торгівлі людьми визначається їхньою здатністю забезпечувати своєчасне виявлення релевантної інформації, встановлення взаємозв'язків між інформаційними об'єктами, формування перевірюваних аналітичних висновків і підтримку обґрунтованих рішень уповноважених фахівців. Відповідно, оцінювання має охоплювати як технічні характеристики окремих компонентів, так і їхній практичний внесок у загальний процес протидії торгівлі людьми.

Методологічним підґрунтям такого оцінювання є підходи інтелектуального аналізу даних, машинного навчання та геоінформаційних технологій, викладені у відповідних навчальних і науково-методичних працях [107 - 110, 115]. Застосування цих підходів передбачає послідовне збирання, підготовку, опрацювання та інтерпретацію інформації, причому кожен етап має власні критерії якості.

Для оцінювання варто розмежовувати два рівні. Технологічний рівень охоплює продуктивність, точність, повноту, надійність, масштабованість і ресурсну ефективність. Функціонально-результативний рівень характеризує здатність компонента прискорювати аналітичну роботу, покращувати виявлення значущої інформації та забезпечувати перевірюваність отриманих результатів.

При цьому необхідно враховувати, що технічна результативність не тотожна юридичній або суспільній ефективності. Наприклад, алгоритм може швидко виявляти схожі оголошення, але це не доводить, що вони пов'язані зі злочинною діяльністю. Аналогічно, висока точність географічного аналізу не гарантує правильності висновку про характер подій у певному регіоні.

8.3.1. Ефективність OSINT

OSINT (Open Source Intelligence) охоплює методи пошуку, збирання, перевірки та аналітичного опрацювання інформації з відкритих джерел. У протидії торгівлі людьми цей інструментарій може використовуватися для аналізу публічних оголошень про працевлаштування, дослідження відкритих веб-ресурсів, виявлення повторюваних інформаційних шаблонів і формування сигналів, які потребують подальшої перевірки.

Ефективність OSINT визначається повнотою пошуку, точністю результатів, оперативністю, перевірюваністю та відтворюваністю. Для оцінювання повноти й точності можуть застосовуватися такі показники як Precision (8.3) та Recall (8.4).

Висока повнота за низької точності створює додаткове навантаження на фахівців, тоді як висока точність за низької повноти може призвести до пропуску важливих відомостей. Тому оцінювання має спиратися на кілька взаємодоповнювальних показників.

Оперативність вимірюють часом від початку пошуку до отримання перевірюваного аналітичного результату, включно з очищенням даних, усуненням дублікатів і перевіркою джерел. Перевірюваність передбачає документування походження відомостей, часу отримання, параметрів пошуку та виконаних процедур верифікації.

Під час тестування OSINT використовують контрольні сценарії з наперед визначеною релевантністю об’єктів. Результати перевіряються незалежним способом, а всі помилки класифікуються за типами. Окремо необхідно враховувати мінливість відкритих джерел: видалення публікації або зміна веб-сторінки може ускладнювати повторення пошуку.

Водночас збіг контактних даних, подібність текстів або наявність спільних цифрових атрибутів не є самостійним доказом причетності особи до торгівлі людьми. Результати OSINT мають розглядатися як інформаційні сигнали, що потребують контекстної та професійної перевірки. Оброблення відомостей про фізичних осіб повинно відповідати вимогам законодавства про захист персональних даних [98].

8.3.2. Ефективність Big Data

Big Data забезпечує опрацювання значних обсягів різнорідної інформації, інтеграцію даних із багатьох джерел і виявлення закономірностей, які складно встановити за допомогою ізольованого аналізу. У протидії торгівлі людьми ці технології можуть застосовуватися для зіставлення інформаційних записів,

виявлення повторюваних шаблонів, аналізу часової динаміки та формування комплексного інформаційного контексту.

Основними критеріями ефективності Big Data є продуктивність, масштабованість, повнота, якість інтеграції та ресурсна ефективність. Продуктивність визначається кількістю записів, опрацьованих за одиницю часу:

$$Q = \frac{N_{processed}}{T_{processing}}, \tag{8.31}$$

де $N_{processed}$ – кількість опрацьованих записів; $T_{processing}$ – тривалість оброблення.

Але цей показник не відображає повністю якість роботи системи. Для комплексного оцінювання необхідно враховувати частку успішно інтегрованих записів, кількість дублікатів, частоту помилок нормалізації, частку пропущених значень і кількість випадків, що потребують ручного виправлення.

Масштабованість оцінюється шляхом збільшення обсягу даних, кількості джерел або кількості одночасних користувачів із подальшим аналізом часу виконання операцій та використання ресурсів. Для порівняння технологічних рішень слід застосовувати однакові або зіставні тестові набори й документувати апаратні умови.

Окреме значення має якість вихідних даних. Збільшення обсягу інформації не обов’язково підвищує достовірність аналітичних висновків, якщо дані містять систематичні помилки, суперечливі ідентифікатори або нерівномірно представляють різні типи подій. Тому оцінювання Big Data має включати перевірку походження, повноти, актуальності та узгодженості інформації [107, 110].

8.3.3. Ефективність GIS

Геоінформаційні системи (Geographic Information Systems, GIS) забезпечують просторове опрацювання та візуалізацію інформації. У протидії торгівлі людьми вони можуть використовуватися для аналізу територіального розподілу повідомлень, зіставлення географічних характеристик подій, дослідження просторових закономірностей і підтримки планування заходів реагування.

Застосування GIS у протидії торгівлі людьми може забезпечувати:

– картографування місць виявлення фактів торгівлі людьми;

– просторовий аналіз маршрутів переміщення;

– визначення територій підвищеного ризику;

– аналіз просторового розподілу звернень та повідомлень;

– виявлення просторових кластерів;

– аналіз близькості об’єктів;

– моделювання потенційних маршрутів;

– візуалізацію мережевих і часово-просторових взаємозв’язків.

Основними критеріями оцінювання GIS є точність геоприв’язки, повнота просторових даних, швидкість виконання операцій, якість візуалізації та відтворюваність аналізу. Середню похибку геоприв’язки можна оцінювати за формулою:

$$E_{geo} = \frac{1}{n} \sum_{i=1}^{n} d_i, \tag{8.32}$$

де d_i – відстань між контрольним і визначеним системою розташуванням об’єкта; n – кількість перевірених об’єктів.

Під час оцінювання необхідно враховувати точність вихідних адрес, систему координат, масштаб карти та спосіб геокодування. Для перевірки просторових алгоритмів можна застосовувати контрольні набори із заздалегідь відомим розташуванням об’єктів і порівнювати результати різних методів аналізу.

Особливу увагу слід приділяти інтерпретації просторових концентрацій. Підвищена кількість повідомлень у певному регіоні не обов’язково означає вищий рівень торгівлі людьми, оскільки на цей показник можуть впливати доступність каналів повідомлення, інтенсивність перевірок і повнота реєстрації даних. Отже, GIS має підтримувати перевірку гіпотез, а не автоматичне встановлення факту правопорушення. Методичну основу практичного оцінювання GIS-операцій можна формувати з використанням навчальних матеріалів із геоінформаційних систем [115].

8.3.4. Ефективність ML/AI

Машинне навчання (Machine Learning, ML) та штучний інтелект (Artificial Intelligence, AI) дають змогу класифікувати інформаційні об’єкти, виявляти закономірності, аналізувати текстові матеріали та формувати прогнози. Методологічною основою оцінювання відповідних моделей є праці з інтелектуального аналізу даних і машинного навчання [107 - 110].

Для моделей класифікації застосовують Precision (8.3), Recall (8.4), F1-score (8.5), частоту хибнопозитивних і хибнонегативних результатів.

Проте оцінювання ML/AI не повинно обмежуватися показниками класифікації. Необхідно перевіряти здатність моделі узагальнювати результати на нових даних, її стійкість до шуму, наявність систематичних викривлень, пояснюваність і стабільність після впровадження.

Для достовірного тестування дані розділяють на навчальну, валідаційну й тестову вибірки. Тестова вибірка має бути відокремленою від навчального процесу. Якщо дані мають часову структуру, доцільно перевіряти модель на пізніших даних, щоб з’ясувати, чи зберігає вона якість за зміни інформаційного середовища.

Управління ризиками AI узгоджують з підходами NIST AI Risk Management Framework, який передбачає функції управління, визначення контексту, вимірювання та контролю ризиків протягом життєвого циклу системи [77].

Це важливо для систем, результати яких можуть впливати на права та законні інтереси людини.

Окремим напрямом оцінювання має бути пояснюваність алгоритмів. У сфері протидії торгівлі людьми автоматичний прогноз не повинен сприйматися як безумовно правильний висновок. Аналітик має розуміти, які характеристики даних стали підставою для формування певного ризикового сигналу. Це важливо при прийнятті рішень, які можуть впливати на права людини.

Рекомендації щодо відповідального використання ШІ підкреслюють необхідність контролю людини, захисту конфіденційності, належного

управління даними, прозорості та недискримінації. Отже, модель, яка має високі статистичні показники, але систематично дискримінує певні групи або використовує непрозорі ознаки, не може вважатися ефективною в контексті правозахисної діяльності.

Ще одним критерієм є стійкість моделі до зміни середовища. Злочинні мережі можуть змінювати способи комунікації, використовувати нові платформи, змінювати лінгвістичні шаблони та поведінкові характеристики. Модель, яка показувала високі результати на історичних даних, може поступово втрачати ефективність. Тому необхідними є регулярна валідація, моніторинг даних і перенавчання моделей.

Оцінювання ML/AI повинно включати не лише лабораторні метрики, а й операційні результати: скорочення часу аналітичної роботи, збільшення кількості підтверджених ризикових сигналів, зменшення інформаційного навантаження на аналітика, підвищення точності пріоритизації матеріалів та збільшення кількості результативних розслідувань.

Алгоритмічний результат не повинен трактуватися як самостійний доказ причетності особи до злочину. Його належить використовувати як засіб підтримки професійного аналізу, передбачаючи перевірку підстав класифікації, оцінювання альтернативних пояснень і можливість виправлення помилкових результатів.

8.3.5. Ефективність цифрової криміналістики

Цифрова криміналістика охоплює процедури виявлення, отримання, збереження, дослідження та документування цифрових об’єктів, що можуть мати значення для встановлення обставин події. На відміну від пошукової аналітики, її результативність залежить не тільки від здатності виявити інформацію, а й від забезпечення цілісності цифрових даних і відтворюваності процедур дослідження.

Професійна підготовка українських правоохоронців у сфері цифрової криміналістики також орієнтована на роботу з електронними доказами,

проведення криміналістичних досліджень та підготовку обґрунтованих звітів для підтримки кримінальних розслідувань.

Для оцінювання цифрової криміналістики використовуються такі показники:

– частка цифрових носіїв, з яких успішно вилучено інформацію;

– частка відновлених релевантних даних;

– повнота реконструкції цифрових подій;

– кількість встановлених цифрових зв’язків;

– час проведення криміналістичного дослідження;

– кількість виявлених цифрових артефактів;

– частка результатів, що пройшли незалежну перевірку;

– кількість або частка матеріалів, які можуть бути використані у процесуальному порядку;

– відповідність процедури міжнародним і національним вимогам;

– відтворюваність отриманого результату іншим фахівцем.

Основними критеріями є повнота виявлення релевантних об’єктів, цілісність даних, точність інструментів, відтворюваність дослідження, якість документування та час виконання операцій. Для тестування можна використовувати контрольні цифрові образи з наперед визначеними файлами, метаданими й іншими інформаційними артефактами.

Збереження цілісності інформації перевіряють за допомогою порівняння хеш-значень, обчислених на початковому та завершальному етапах оброблення. Збіг значень свідчить про незмінність вмісту в межах відповідної перевірки, але не підтверджує самостійно походження даних, законність їх отримання або правильність інтерпретації.

Важливим критерієм є документування послідовності дій із цифровим об’єктом, включно з відомостями про його отримання, передавання, зберігання й дослідження. Методичні орієнтири щодо цифрових розслідувань і збереження цифрових доказів містяться у публікаціях NIST [119 - 121].

Експериментальна перевірка має охоплювати повноту виявлення контрольних об’єктів, точність їх інтерпретації, цілісність копій і можливість повторення дослідження. При цьому технічна можливість отримати певний результат не замінює правової оцінки його допустимості та доказового значення.

8.3.6. Ефективність інтегрованої аналітичної платформи

Інтегрована аналітична платформа об’єднує результати OSINT, Big Data, GIS, ML/AI та цифрової криміналістики в єдиному інформаційному середовищі. Її ефективність залежить від узгодженості компонентів, коректності обміну даними, збереження походження інформації, наскрізної оперативності та надійності роботи.

Для оцінювання платформи використовують такі критерії:

- якість інтеграції даних і відсутність некоректних зв’язків;
- загальний час від надходження інформації до формування результату;
- частка успішно завершених наскрізних операцій;
- доступність системи й час відновлення після збоїв;
- масштабованість і ресурсна ефективність;
- якість журналювання та можливість аудиту;
- дотримання вимог інформаційної безпеки;
- зручність використання та практична результативність.

Загальний час опрацювання інформації можна подати у спрощеній формі:

$$T_{total} = T_{ingest} + T_{prepare} + T_{analysis} + T_{integration} + T_{delivery}, \tag{8.33}$$

де складові відображають надходження, підготовку, аналіз, інтеграцію й передавання результату. Якщо окремі етапи виконуються паралельно, фактичний час необхідно визначати за реальним графом виконання операцій.

Для комплексного оцінювання використовують інтегральний індекс:

$$I_{platform} = \sum_{i=1}^{n} \omega_i K_i, \qquad \sum_{i=1}^{n} \omega_i = 1. \tag{8.34}$$

де K_i– нормоване значення критерію; ω_i – його вага; n – кількість критеріїв.

При цьому вагові коефіцієнти не повинні задаватися довільно. Вони можуть визначатися експертним методом, методом аналізу ієрархій, на основі

статистичних даних або шляхом порівняння фактичного внеску технологічного компонента в досягнення кінцевих результатів.

Для інтегрованої платформи виділяють п’ять рівнів оцінювання.

Перший рівень – технологічний. Оцінюються швидкодія, доступність, масштабованість, надійність, стійкість, безпечність та інтероперабельність.

Другий рівень – інформаційний. Визначаються повнота, точність, актуальність, узгодженість та якість даних.

Третій рівень – аналітичний. Оцінюється здатність платформи виявляти закономірності, аномалії, зв’язки, ризики та прогнозувати потенційні сценарії.

Четвертий рівень – оперативно-процесуальний. Визначається, наскільки використання системи скорочує час опрацювання інформації, сприяє формуванню версій, покращує документування та підвищує результативність розслідувань.

П’ятий рівень – правозахисний і суспільний. Оцінюється дотримання прав людини, конфіденційності, принципів недискримінації, мінімізації даних, законності доступу та недопущення неправомірної автоматизації рішень.

Останній рівень є принципово важливим. Підвищення технологічної ефективності не може вважатися позитивним результатом, якщо воно досягається шляхом необґрунтованого масового збору персональних даних, порушення приватності або автоматизованого профілювання осіб без належних правових підстав. Отже, ефективність цифрової технології у сфері протидії торгівлі людьми повинна оцінюватися одночасно за критеріями результативності та правомірності.

Інтегральний індекс використовується разом із переліком обов’язкових вимог. Високі показники швидкості чи зручності не можуть компенсувати порушення цілісності даних, незаконне оброблення персональної інформації або відсутність належного контролю доступу.

8.4. Методика порівняльного оцінювання

Порівняльне оцінювання ефективності цифрових технологій у протидії торгівлі людьми є необхідною складовою методології дослідження, оскільки

саме воно дає змогу встановити, чи забезпечує впровадження інформаційно-аналітичних систем, технологій Data Mining, штучного інтелекту, геоінформаційних систем, засобів OSINT та цифрової криміналістики реальне підвищення результативності відповідних заходів порівняно з традиційними методами роботи. Під ефективністю розуміють не лише здатність технологічного рішення виявляти потенційні випадки торгівлі людьми, а комплексну характеристику, яка охоплює точність виявлення ризиків, повноту охоплення інформації, швидкість аналітичної обробки, якість встановлення зв'язків між об'єктами, відтворюваність результатів, придатність сформованих матеріалів до подальшого використання у кримінальному провадженні, а також дотримання прав і свобод людини.

Такий підхід відповідає сучасному розумінню державної політики у сфері протидії торгівлі людьми. Закон України «Про протидію торгівлі людьми» визначає протидію торгівлі людьми як систему заходів, спрямованих на її попередження і боротьбу з нею, а також надання допомоги і захисту особам, які постраждали від торгівлі людьми. Отже, результативність цифрового інструментарію не може визначатися винятково технічними характеристиками алгоритму. Вона повинна оцінюватися крізь призму того, наскільки технологія сприяє досягненню правових, оперативних, кримінологічних та соціальних цілей протидії торгівлі людьми.

Цифровізація процесів протидії торгівлі людьми повинна здійснюватися з урахуванням установлених законодавством вимог до доказування. Кримінальний процесуальний кодекс України визначає докази як фактичні дані, отримані у встановленому законом порядку, а оцінювання доказів передбачає перевірку їх належності, допустимості, достовірності, достатності та взаємозв'язку. Тому алгоритм, який демонструє високі показники машинної класифікації, не може автоматично вважатися ефективним правоохоронним інструментом, якщо його результати неможливо належним чином перевірити, інтерпретувати або використати відповідно до процесуальних вимог.

8.4.1. Традиційний та цифровий підходи

Традиційний підхід до виявлення та аналізу ознак торгівлі людьми передбачає використання професійного досвіду працівників уповноважених органів, аналіз матеріалів проваджень, опрацювання документів, проведення опитувань і співбесід, перевірку повідомлень, зіставлення відомостей із різних джерел та міжвідомчий обмін інформацією. Його важливою перевагою є можливість урахування соціального, психологічного, культурного та правового контексту конкретної ситуації. Фахівець може оцінити суперечності у свідченнях, звернути увагу на обставини, які не відображені в цифрових даних, а також врахувати індивідуальні потреби людини та ризики, пов’язані з її безпекою.

Традиційні процедури можуть характеризуватися значними витратами часу, залежністю від людського чинника, обмеженою здатністю одночасно опрацьовувати великі масиви інформації та складністю встановлення зв’язків між відомостями, що зберігаються в різних системах. За умов, коли дані надходять із багатьох джерел і постійно оновлюються, ручне зіставлення відомостей може ускладнювати своєчасне виявлення повторюваних закономірностей, взаємопов’язаних подій або нетипових моделей поведінки.

Цифровий підхід ґрунтується на застосуванні програмних засобів для автоматизованого збирання, структурування, пошуку, класифікації та аналізу інформації. До відповідних інструментів належать технології інтелектуального аналізу даних, машинного навчання, оброблення природної мови, аналізу мережевих зв’язків, геоінформаційного моделювання, цифрової криміналістики й інтеграції різнорідних інформаційних ресурсів. Українські науково-методичні праці з інтелектуального аналізу даних і машинного навчання створюють теоретичну основу для визначення способів опрацювання даних, побудови моделей та перевірки результатів їх застосування [107 - 110]. Використання геоінформаційних засобів, своєю чергою, дає змогу досліджувати просторові закономірності, співвідносити події з географічними об’єктами та виявляти

просторові зв’язки, які складно встановити шляхом ізольованого аналізу текстових записів [115].

Цифрові технології не усувають необхідності професійної оцінки. Автоматизовані системи працюють із даними, що можуть бути неповними, застарілими, упередженими або навмисно спотвореними. Алгоритм здатний виявити статистичну закономірність, але сама наявність такої закономірності не доводить факту вчинення злочину. Наприклад, збіг контактних даних, географічна близькість об’єктів або повторення певних ключових слів можуть бути підставою для подальшої перевірки, проте не повинні автоматично трактуватися як доказ торгівлі людьми.

Доцільно порівнювати не лише два окремі способи роботи, а й три моделі організації процесу: традиційну, цифрову та комбіновану. Традиційна модель передбачає переважно ручне опрацювання інформації; цифрова – активне використання автоматизованих інструментів для виявлення й упорядкування відомостей; комбінована – поєднання алгоритмічного аналізу з перевіркою результатів уповноваженим фахівцем. Саме комбінована модель дає змогу оцінити, чи сприяють цифрові інструменти поліпшенню професійних рішень, не підміняючи їх автоматизованими висновками.

Для забезпечення коректності порівняння всі три моделі потрібно перевіряти на однаковому наборі випадків або на вибірках, зіставних за обсягом, складністю, часовими характеристиками та доступністю вихідних відомостей. Необхідно також розмежовувати час, витрачений на автоматизоване опрацювання даних, час професійної перевірки та загальний час від надходження інформації до формування аналітичного висновку. Якщо цифрова система швидко генерує попередження, але кожне з них потребує тривалої ручної перевірки, сама швидкість алгоритму не свідчитиме про пропорційне підвищення ефективності всього процесу.

Основними критеріями порівняння традиційного та цифрового підходів варто визначити:

- результативність виявлення – здатність ідентифікувати релевантні випадки та ознаки, які потребують додаткової перевірки;
- повноту опрацювання інформації – частку доступних і релевантних відомостей, які фактично враховано під час аналізу;
- оперативність – час від надходження даних до отримання результату, придатного для професійного розгляду;
- точність – співвідношення правильних висновків і загальної кількості відповідних результатів;
- відтворюваність – можливість повторити процедуру за тих самих умов і отримати порівнювані результати;
- ресурсомісткість – витрати робочого часу, обчислювальних ресурсів і коштів;
- пояснюваність – можливість встановити, які дані та правила вплинули на результат;
- правову й етичну прийнятність – відповідність процедур вимогам законодавства, принципам захисту персональних даних і прав людини [6, 98, 118, 77].

Порівняльне оцінювання повинно враховувати й відмінності між типами завдань. Для первинного сортування великого масиву відкритих даних пріоритетними можуть бути швидкість оброблення, повнота пошуку та прийнятний рівень хибнопозитивних спрацювань. Для аналізу цифрових доказів більшої ваги набувають цілісність даних, документованість процедури, можливість незалежної перевірки й обґрунтованість висновку. Для оцінювання ризиків щодо конкретної людини особливого значення набувають мінімізація шкоди, недопущення дискримінації та обов’язкова перевірка результатів уповноваженим фахівцем.

Таким чином, універсального показника, який однаково відображав би ефективність усіх підходів і технологій, недостатньо. Порівняння має базуватися на наборі показників, вагомість яких визначається призначенням конкретного

інструмента, умовами його використання та можливими наслідками помилкових результатів.

8.4.2. Формування контрольних і тестових вибірок

Формування контрольних і тестових вибірок є одним із ключових етапів порівняльного оцінювання, оскільки достовірність експериментальних висновків безпосередньо залежить від якості вихідних даних, способу їх відбору та відповідності реальним умовам застосування цифрових технологій. Навіть технічно досконалий алгоритм може демонструвати високі показники на штучно сформованому наборі даних, але втрачати ефективність під час опрацювання реальних інформаційних потоків. Така ситуація може виникати внаслідок нерепрезентативності вибірки, надмірної частки типових випадків, недостатнього представлення рідкісних сценаріїв або наявності прихованих залежностей між даними, використаними під час навчання та перевірки моделі.

У межах дослідження цифрових технологій у протидії торгівлі людьми під вибіркою варто розуміти впорядковану сукупність записів, документів, повідомлень, подій або інших інформаційних об’єктів, відібраних за визначеними критеріями для проведення експериментального оцінювання. Залежно від поставленого завдання такими об’єктами можуть бути повідомлення з відкритих джерел, матеріали оголошень про працевлаштування, структуровані записи інформаційних систем, узагальнені відомості про маршрути переміщення, документи, що містять ознаки можливого примусу чи експлуатації, а також синтетично згенеровані приклади, які відтворюють певні сценарії загроз.

Формування вибірок не повинно передбачати неконтрольованого використання персональних даних постраждалих осіб або осіб, щодо яких здійснюється перевірка. Перевагу слід надавати знеособленим, належним чином захищеним або синтетичним даним, а доступ до інформації, яка дає змогу ідентифікувати людину, необхідно обмежувати відповідно до законодавства та визначеної мети оброблення [98]. Використання реальних матеріалів можливе лише за наявності належних правових підстав, дотримання вимог

конфіденційності та застосування процедур, які запобігають повторній ідентифікації осіб.

За функціональним призначенням у процесі експериментального дослідження розрізняють навчальну, валідаційну, тестову та контрольну вибірки. Навчальна вибірка використовується для побудови моделі або визначення її параметрів. Валідаційна – для добору гіперпараметрів, порогів класифікації та порівняння альтернативних конфігурацій. Тестова вибірка призначена для остаточного оцінювання моделі на даних, які не використовувалися під час її навчання та налаштування. Контрольна вибірка в межах порівняльного експерименту може слугувати спільним набором випадків, на якому зіставляють результати традиційного, цифрового та комбінованого підходів.

Для запобігання витоку інформації між вибірками перевіряють не лише збіг окремих записів, а й наявність пов’язаних об’єктів. Наприклад, повідомлення з різних веб-сайтів можуть бути копіями одного оголошення, а кілька записів – описувати ту саму подію. Якщо такі матеріали одночасно потрапляють до навчальної та тестової вибірок, модель може фактично розпізнавати раніше побачений зміст, а не виявляти закономірності, придатні для узагальнення. Тому потрібно передбачати дедуплікацію, групування пов’язаних записів і розділення даних за суттєвими ознаками залежності.

Під час формування вибірок враховують специфіку предметної області. Реальні випадки торгівлі людьми не завжди мають однозначну структуру, а достовірно підтверджені випадки можуть становити лише невелику частку загального масиву інформації. Значна кількість повідомлень може містити неповні відомості, суперечливі твердження або ознаки, які потребують додаткової перевірки. Тому механічне формування вибірки зі збереженням природного співвідношення класів не завжди забезпечує достатню кількість прикладів для надійного оцінювання здатності алгоритму виявляти рідкісні випадки.

Для вирішення цієї проблеми можна застосовувати стратифікований відбір, за якого вибірка формується з урахуванням визначених категорій, наприклад типу джерела, періоду створення запису, виду потенційної експлуатації, повноти інформації та статусу перевірки. За потреби використовують цільове доповнення рідкісних категорій, але під час розрахунку підсумкових показників необхідно враховувати, що штучно змінене співвідношення класів може спотворювати оцінки точності, поширеності подій і прогностичної цінності результатів.

Важливо звернути увагу на визначення еталонних міток, які використовуються для перевірки правильності алгоритмічних висновків. Для завдань протидії торгівлі людьми недостатньо позначити кожний запис лише як «торгівля людьми» або «не торгівля людьми». Інформація може бути непідтвердженою, суперечливою, неповною або такою, що не дає змоги зробити остаточний висновок.

Передбачають такі категорії:

- підтверджений релевантний випадок або наявність визначених дослідженням ознак;
- випадок, щодо якого ознаки не підтверджені за результатами перевірки;
- невизначений випадок, для якого недостатньо інформації;
- запис, що не відповідає предмету дослідження або не може бути коректно оцінений.

Ця класифікація дозволяє не ототожнювати відсутність підтвердження з доведеним фактом відсутності правопорушення. Вона також дає змогу окремо оцінювати роботу алгоритмів у ситуаціях інформаційної невизначеності. Еталонні мітки мають формуватися за заздалегідь визначеним протоколом, а складні випадки передавати на незалежний перегляд кількома компетентними фахівцями. Розбіжності між оцінювачами необхідно документувати, оскільки вони можуть свідчити про неоднозначність критеріїв, а не лише про помилки конкретної особи.

Для оцінювання здатності моделі працювати з новими даними варто використовувати часовий поділ вибірок: ранні записи застосовувати для навчання, а пізніші – для тестування. Такий підхід дозволяє частково відтворити ситуацію, коли після впровадження системи вона отримує інформацію, що відрізняється від тієї, на якій її було налаштовано. Це важливо для цифрових технологій, оскільки зміни способів комунікації, формування оголошень, платформ і тактик злочинної діяльності можуть призводити до поступового погіршення якості алгоритмічних прогнозів.

У підсумку належно сформована вибірка повинна характеризуватися релевантністю, достатньою різноманітністю, контрольованим співвідношенням категорій, документованим походженням даних і відсутністю некоректного перетину між навчальними та тестовими наборами. Усі процедури відбору, очищення, знеособлення та маркування необхідно описувати так, щоб інші дослідники могли зрозуміти, які саме дані використовувалися і які обмеження має отриманий результат.

8.4.3. Експериментальна перевірка алгоритмів

Експериментальна перевірка алгоритмів передбачає систематичне дослідження їхньої поведінки на визначених наборах даних за контрольованих умов. Її мета полягає у встановленні того, наскільки отримані результати відповідають призначенню системи, чи зберігається якість роботи за зміни вихідних умов і які обмеження необхідно враховувати під час практичного застосування. Для цифрових технологій у протидії торгівлі людьми експериментальне оцінювання має охоплювати не лише математичні показники якості, а й операційні характеристики, інтерпретованість результатів, стійкість до неповних даних і можливі наслідки помилкових спрацювань.

Загальний алгоритм експериментальної перевірки організовують як послідовність взаємопов’язаних етапів.

Перший етап – формулювання гіпотез і визначення критеріїв успіху. Перед початком експерименту необхідно визначити, які властивості системи підлягають перевірці. Наприклад, дослідницька гіпотеза може полягати в тому,

що використання інтелектуального аналізу даних скорочує середній час первинного опрацювання повідомлень без неприйнятного зниження повноти виявлення релевантних випадків. Інша гіпотеза може передбачати, що комбінований підхід забезпечує меншу частку пропущених випадків порівняно з ручним аналізом за прийнятного обсягу додаткових перевірок.

Гіпотези необхідно формулювати до перегляду остаточних результатів тестування. Для кожної з них визначають основний показник, допоміжні показники, умови прийнятності та спосіб статистичної перевірки. Це зменшує ризик вибіркового використання лише тих метрик, які демонструють бажану перевагу певної технології.

Другий етап – визначення експериментальних умов. Необхідно зафіксувати версію програмного забезпечення, параметри алгоритму, обчислювальне середовище, склад вхідних даних, критерії попереднього оброблення та правила інтерпретації результатів. Для моделей машинного навчання слід документувати методи навчання, гіперпараметри, порогові значення класифікації та спосіб оброблення пропущених значень. Для систем аналізу текстів – описати процедури нормалізації, токенізації, мовної обробки та видалення повторів. Для геоінформаційних систем – зазначити джерела просторових даних, їхню точність, систему координат і критерії просторового зіставлення.

Третій етап – формування базового сценарію. Результати цифрового алгоритму необхідно порівнювати з визначеною базовою моделлю. Нею може бути ручне опрацювання матеріалів за затвердженою процедурою, простий алгоритм пошуку за ключовими словами або інша модель, що виконує аналогічне завдання. Вибір базового сценарію залежить від мети дослідження. Якщо необхідно встановити, чи покращує складна модель виявлення ознак порівняно з простим пошуком, обидва інструменти мають перевірятися на одному наборі даних. Якщо досліджується організаційна ефективність, необхідно порівнювати повний цикл опрацювання матеріалів, а не лише час виконання окремої програмної операції.

Четвертий етап – проведення експерименту. Алгоритми запускають на підготовлених тестових даних відповідно до заздалегідь визначеного протоколу. Для кожного випадку фіксують вихідний результат, час опрацювання, категорію помилки, потребу в ручному перегляді та інші показники, передбачені планом дослідження. Якщо система використовує випадкові процедури або параметри, залежні від ініціалізації, експеримент необхідно повторити з різними значеннями початкового стану або застосувати інший обґрунтований метод оцінювання варіативності результатів.

П’ятий етап – незалежна перевірка. Важливо розмежовувати перевірку технічної правильності роботи програмного забезпечення та оцінювання придатності отриманих результатів для практичного використання. Перша передбачає встановлення відповідності системи технічним вимогам, тоді як друга – з’ясування того, чи відповідає результат реальному змісту аналізованого випадку. У сфері цифрової криміналістики наукова обґрунтованість методів, їхні обмеження та необхідність належного тлумачення результатів є предметом окремої уваги [119 - 121].

Шостий етап – аналіз помилок і документування висновків. На цьому етапі необхідно визначити, які типи випадків спричиняють хибнопозитивні або хибнонегативні результати, чи пов’язані помилки з якістю даних, мовними особливостями, зміною структури повідомлень, нерівномірним представленням категорій або недоліками алгоритму. Документування має включати не лише підсумкові значення метрик, а й обмеження експерименту, випадки невизначеності та умови, за яких результати можуть бути непридатними для узагальнення.

Для оцінювання алгоритмів класифікації використовують матрицю помилок, яка зіставляє передбачений результат з еталонною міткою. Для бінарної класифікації вона охоплює чотири основні категорії:

- істиннопозитивні результати – випадки, у яких алгоритм правильно виявив ознаки, визначені як позитивний клас;

- хибнопозитивні результати – випадки, які алгоритм відніс до позитивного класу, хоча за еталонною оцінкою вони до нього не належать;
- істиннонегативні результати – випадки, правильно віднесені до негативного класу;
- хибнонегативні результати – випадки, у яких алгоритм не виявив ознаки, наявні відповідно до еталонної оцінки.

На основі цих значень розраховують основні показники якості Precision (8.3), Recall (8.4) та F1-score (8.5).

Показник Precision характеризує частку правильних позитивних результатів серед усіх позитивних спрацювань алгоритму. Recall відображає частку виявлених позитивних випадків серед усіх випадків, позначених як позитивні за еталонною оцінкою. F1-score є гармонійним середнім Precision і Recall та дає змогу узагальнено оцінити їхнє співвідношення. При цьому необхідно враховувати, що F1-score не враховує істиннонегативні результати й не може самостійно характеризувати всі аспекти якості системи.

У протидії торгівлі людьми співвідношення цих показників має визначатися призначенням алгоритму. Для інструмента первинного пошуку потенційно небезпечних ситуацій високий рівень Recall може бути важливим, оскільки пропуск релевантного випадку створює ризик несвоєчасного реагування. Надмірне зростання кількості хибнопозитивних результатів може перевантажити фахівців і збільшити час перевірки. Для інструментів, які використовуються під час підготовки аналітичних висновків, значення має також точність і пояснюваність результату. Жоден із цих показників не повинен тлумачитися як самостійний доказ факту торгівлі людьми.

Крім метрик класифікації оцінюють операційні характеристики алгоритму: середній і медіанний час оброблення одного запису, пропускну здатність системи, частоту технічних збоїв, обсяг необхідної ручної перевірки, потребу в обчислювальних ресурсах та стабільність результатів за зміни вхідних даних. Якщо цифрова технологія використовується для прогнозування або ранжування

ризиків, необхідно окремо перевіряти якість ранжування, калібрування оцінок і відповідність прогнозів фактичним результатам у межах доступних даних.

Методологічно важливо, щоб експериментальна перевірка не обмежувалася лише одним набором даних або одним пороговим значенням. Для систем, чутливих до параметрів, доцільно дослідити декілька конфігурацій і визначити, як зміна порога класифікації впливає на співвідношення Precision, Recall, FPR і FNR. Вибір найкращої конфігурації необхідно проводити на валідаційних даних, а остаточні показники обчислювати на незалежній тестовій вибірці.

Для систем зі штучним інтелектом враховують рекомендації NIST AI Risk Management Framework, у якому оцінювання ризиків передбачає використання кількісних, якісних або комбінованих методів, визначення показників невизначеності, порівняння з базовими значеннями та документування результатів тестування [77].

Такий підхід дає змогу розглядати ефективність алгоритму не як незмінну характеристику, а як властивість, що потребує перевірки впродовж усього життєвого циклу системи.

Отже, експериментальна перевірка має забезпечувати контрольованість умов, незалежність тестування, відтворюваність процедур, повноту документування та змістовний аналіз помилок. Лише за таких умов отримані показники можуть використовуватися для обґрунтованого порівняння цифрових технологій і визначення меж їхнього практичного застосування.

8.4.4. Порівняння результатів

Порівняння результатів передбачає систематичне зіставлення показників традиційного, цифрового та комбінованого підходів із метою визначення їхніх переваг, обмежень і умов доцільного використання. Для коректного порівняння необхідно забезпечити спільність дослідницького завдання, зіставність вхідних даних, однакові правила визначення правильності результатів і єдині принципи вимірювання витрат часу та ресурсів.

Розмежовують порівняння за результативністю та за ресурсною ефективністю. Результативність відображає, наскільки повно й правильно система виконує поставлене завдання. Ресурсна ефективність характеризує співвідношення отриманого результату та витрачених ресурсів. Цифровий інструмент може демонструвати вищу швидкість оброблення даних, але не забезпечувати кращої якості висновків. Так само алгоритм із високим рівнем Recall може генерувати значну кількість хибнопозитивних спрацювань, унаслідок чого зростатиме навантаження на фахівців.

Для зіставлення результатів можна сформувати інтегровану систему показників, що охоплює чотири основні групи:

1. Аналітичні показники: Precision, Recall, F1-score, FPR, FNR, якість ранжування та повнота виявлення релевантних зв’язків.
2. Операційні показники: середній час оброблення, загальний час виконання завдання, пропускна здатність і частка випадків, що потребують додаткової ручної перевірки.
3. Ресурсні показники: витрати робочого часу, обчислювальні ресурси, вартість упровадження й супроводу, потреба в навчанні персоналу.
4. Організаційно-правові показники: пояснюваність, документованість результатів, захищеність даних, можливість аудиту та відповідність правовим вимогам.

Для моделей машинного навчання важливо перевіряти не лише загальну якість, а й стабільність роботи на підгрупах даних. Значні відмінності між підгрупами можуть свідчити про нерівномірне представлення прикладів, особливості джерел інформації або систематичні помилки моделі. Такі відмінності потрібно досліджувати, а не приховувати шляхом агрегування всіх результатів в одне середнє значення. Рекомендації щодо управління ризиками штучного інтелекту наголошують на необхідності систематичного вимірювання, документування та перегляду показників надійності й можливих негативних впливів системи [77].

Важливим компонентом порівняння є визначення компромісів між якістю, швидкістю та ресурсними витратами. Наприклад, модель із високим рівнем Recall, але значною кількістю хибнопозитивних спрацювань, може бути доцільною для первинного скринінгу, якщо подальший перегляд результатів здійснює підготовлений фахівець. Натомість для підготовки аналітичних матеріалів, що впливають на подальші процесуальні рішення, пріоритетними стають пояснюваність, простежуваність джерел і незалежна перевірка. Отже, оцінювання має виходити з функціонального призначення технології, а не з абстрактного прагнення максимізувати один показник.

Отже, порівняння результатів має забезпечувати не лише визначення найкращого алгоритму за певною метрикою, а й обґрунтування того, у яких умовах, для яких завдань і за яких обмежень відповідна технологія може бути корисною. Такий підхід сприяє переходу від формального зіставлення технічних характеристик до оцінювання реального внеску цифрових технологій у підвищення якості аналітичної та організаційної діяльності.

8.4.5. Статистична достовірність результатів

Статистична достовірність є необхідною умовою обґрунтованої інтерпретації результатів порівняльного оцінювання. Вона дає змогу встановити, наскільки отримані відмінності можуть пояснюватися випадковими коливаннями вибірки, а наскільки свідчать про систематичну різницю між досліджуваними підходами. У цьому контексті важливо розмежовувати статистичну значущість, практичну значущість і загальну достовірність висновків. Статистично значуща різниця не обов’язково є важливою для практики, а велика різниця між двома показниками не завжди є достатньо надійною, якщо дослідження ґрунтується на малій або нерепрезентативній вибірці.

Першим етапом статистичного аналізу є визначення дослідницьких гіпотез. Нульова гіпотеза зазвичай передбачає відсутність різниці між порівнюваними підходами за обраним показником, тоді як альтернативна – наявність такої різниці. Якщо дослідницьке завдання передбачає перевірку того,

чи перевищує цифровий підхід традиційний за конкретним показником, може формулюватися спрямована гіпотеза. Проте вибір односторонньої або двосторонньої перевірки необхідно обґрунтувати до аналізу даних, а не визначати після отримання результатів.

Для оцінювання результатів використовують довірчі інтервали, які відображають невизначеність оціненого параметра. Наприклад, для частки правильних класифікацій можна розраховувати довірчий інтервал для відповідної пропорції, а для середньої різниці часу – інтервал для середнього значення парних різниць. Довірчий інтервал дає змогу оцінити діапазон значень, сумісних із даними за обраною статистичною процедурою, і забезпечує інформативніше представлення результату, ніж лише точкова оцінка.

Вибір статистичного критерію має залежати від типу даних, дизайну експерименту, розміру вибірки та характеру розподілу показників. Для порівняння середніх значень у незалежних групах можуть застосовуватися параметричні критерії за виконання відповідних припущень. Якщо аналізуються парні вимірювання, наприклад час виконання одного й того самого завдання традиційним і цифровим способом, доцільно використовувати критерії для пов’язаних вибірок. За відсутності необхідних параметричних припущень можуть застосовуватися непараметричні методи. Для порівняння пов’язаних бінарних результатів, отриманих двома класифікаторами на тих самих випадках, може бути доречним критерій Мак-Немара.

Для оцінювання якості алгоритмів важливо враховувати не лише загальну кількість правильних результатів, а й невизначеність таких показників, як Precision, Recall, F1-score, FPR і FNR. Їхні оцінки можуть істотно змінюватися залежно від розміру тестової вибірки, поширеності позитивного класу та структури помилок. Особливої обережності потребують випадки, коли позитивний клас є рідкісним. За невеликої кількості підтверджених позитивних прикладів навіть декілька додаткових помилок можуть суттєво змінити оцінку Recall або F1-score.

Під час планування дослідження необхідно заздалегідь визначати бажану точність оцінювання та, за можливості, проводити розрахунок необхідного розміру вибірки. Такий розрахунок залежить від очікуваного розміру ефекту, рівня значущості, статистичної потужності, мінливості показника та обраного критерію. Якщо вибірка є занадто малою, дослідження може не виявити реальної різниці між підходами. Якщо ж кількість спостережень дуже велика, навіть практично незначна різниця може виявитися статистично значущою. Тому статистичний аналіз має супроводжуватися оцінюванням практичної важливості результатів.

Для коректного порівняння необхідно враховувати залежність спостережень. Якщо кілька записів стосуються однієї події, однієї особи або одного джерела, їх не завжди можна вважати незалежними. Ігнорування такого зв’язку може призвести до заниження оцінки невизначеності та перебільшення статистичної значущості. У таких випадках використовують групове розділення вибірок, агрегування на рівні незалежних одиниць аналізу або статистичні моделі, які враховують кластерну структуру даних.

Ще одним джерелом помилкових висновків є множинне тестування. Якщо дослідник одночасно порівнює десятки алгоритмів, показників і підгруп, зростає ймовірність отримання випадково значущих результатів. Для зменшення цього ризику визначають основні показники заздалегідь, відокремлюють підтверджувальний аналіз від пошукового та, за потреби, застосовують процедури коригування множинних порівнянь. Виявлені під час пошукового аналізу закономірності перевіряють на незалежних даних.

Статистична достовірність також залежить від якості еталонних міток. Якщо правильність випадків визначена непослідовно, результати алгоритму порівнюватимуться з ненадійним орієнтиром. Тому необхідно описувати процедуру експертного маркування, критерії розв’язання розбіжностей і частку випадків, для яких остаточну оцінку встановити не вдалося. Якщо частина даних залишається невизначеною, потрібно зазначати, як саме такі випадки враховано в аналізі, та проводити аналіз чутливості, коли це методологічно обґрунтовано.

Окремо слід розглядати статистичну достовірність у контексті цифрової криміналістики. У цій сфері результати аналізу мають оцінюватися з урахуванням надійності застосованої методики, властивостей цифрових артефактів, можливих обмежень програмних засобів і ризику помилкового тлумачення даних. У звіті NIST щодо наукових засад цифрових розслідувань підкреслено, що, попри опору цифрової криміналістики на усталені комп'ютерні методи, враховують обмеження, зумовлені неповнотою виявлення даних, появою сторонніх матеріалів під час відновлення інформації та змінами програмного забезпечення [119].

Отже, статистична обробка не замінює перевірки походження, цілісності та змісту цифрових даних.

У процесі дослідження систем штучного інтелекту статистичне оцінювання має бути інтегроване в загальну процедуру тестування, верифікації та валідації. NIST AI RMF передбачає використання об'єктивних і відтворюваних процедур оцінювання, документування метрик, аналіз невизначеності та регулярний перегляд відповідності системи її призначенню [77].

Для практичного застосування це означає, що модель потрібно перевіряти не лише перед упровадженням, а й після суттєвих змін у даних, програмному забезпеченні, алгоритмах або умовах роботи.

Звіт про статистичне оцінювання має містити опис вибірки, кількість спостережень, визначення основних показників, обґрунтування обраних статистичних методів, точкові оцінки, довірчі інтервали, результати перевірки гіпотез і пояснення практичного значення виявлених відмінностей. Також необхідно зазначати обмеження дослідження, можливі джерела систематичних похибок і умови, за яких результати не слід переносити на інші групи даних або операційні сценарії.

Таким чином, статистична достовірність результатів порівняльного оцінювання визначається не одним формальним критерієм, а сукупністю чинників: якістю даних, обґрунтованістю дизайну експерименту, коректністю

статистичних процедур, величиною ефекту, невизначеністю оцінок і можливістю відтворити отримані результати. Її забезпечення є необхідною умовою формування об’єктивних висновків щодо ефективності цифрових технологій у протидії торгівлі людьми.

8.5. Оцінювання надійності та стійкості аналітичної системи

Надійність і стійкість є ключовими характеристиками цифрових систем, що використовуються для аналізу інформації у сфері протидії торгівлі людьми. Надійність відображає здатність системи виконувати визначені функції з прийнятною частотою помилок, тоді як стійкість характеризує збереження працездатності та якості результатів за несприятливих умов, змін вхідних даних або навмисних спроб викривлення інформації.

Оцінювання цих характеристик має охоплювати якість даних, алгоритмічну стабільність, коректність інтеграції, захист від маніпуляцій і здатність відновлюватися після технічних збоїв. Для організаційної побудови процесу управління кіберризиками можна використовувати підходи NIST Cybersecurity Framework 2.0, що охоплює функції управління, ідентифікації, захисту, виявлення, реагування та відновлення [106].

8.5.1. Стійкість до неповних даних

Неповнота даних є поширеним явищем у системах, які інтегрують інформацію з різних джерел. Вона може виникати через відсутність окремих полів, недоступність джерел, помилки реєстрації або обмеження на оброблення певних відомостей.

Стійкість до неповноти оцінюється за здатністю системи зберігати прийнятну якість результатів за наявності пропущених значень. Для цього формують кілька контрольних наборів із різними частками пропусків і порівнюють якість роботи системи з базовим сценарієм.

Важливо перевіряти не лише кількість пропущених значень, а й характер їх розподілу. Випадкова відсутність окремих атрибутів може мати інші наслідки,

ніж систематична відсутність інформації з певного джерела або щодо певного типу подій.

Система має розрізняти відсутнє значення, невідоме значення та значення, яке не може бути розкрито через правові обмеження. Автоматичне заповнення пропусків без належного маркування може створити хибне враження, що система оперує фактичними відомостями.

До основних показників належать зміна Precision і Recall за різних рівнів пропусків, частка записів, що залишаються придатними до аналізу, та частка випадків, переданих на ручну перевірку.

8.5.2. Стійкість до зашумлення інформації

Зашумленням вважають наявність помилкових, суперечливих, неточних або нерелевантних елементів у даних. У цифровому середовищі воно може виникати через друкарські помилки, різні формати запису, дублікати, неточне розпізнавання тексту або автоматично згенерований нерелевантний вміст.

Для оцінювання стійкості необхідно сформувати контрольні набори з поступовим збільшенням рівня шуму. Після цього вимірюють зміну якості класифікації, повноти пошуку, точності зіставлення й часу оброблення.

Важливим є розмежування випадкового шуму та систематичного викривлення. Якщо система однаково помиляється через повторюваний формат даних, це свідчить про структурну проблему нормалізації, а не лише про випадкове погіршення якості.

Стійкість може підвищуватися завдяки очищенню даних, нормалізації тексту, перевірці дублікатів, використанню кількох незалежних ознак і документуванню невизначеності. Але автоматичне очищення не повинно безслідно видаляти інформацію, яка може бути важливою для подальшої перевірки.

8.5.3. Стійкість до навмисної маніпуляції даними

Навмисна маніпуляція може включати поширення неправдивих відомостей, створення дублікатів, підміну метаданих, зміну форматів запису або спроби вплинути на результати автоматизованої класифікації. Для аналітичних

систем такі загрози становлять особливу проблему, оскільки зовні правдоподібні дані можуть спричинити помилкові висновки.

Оцінювання стійкості до маніпуляцій має проводитися в контрольованому середовищі з використанням безпечних тестових наборів. Метою є перевірка здатності системи виявляти суперечності, позначати аномальні записи, зберігати походження інформації та уникати автоматичного підтвердження неперевірених висновків.

До показників належать частка виявлених маніпульованих записів, частота хибних спрацювань, час виявлення аномалій і частка результатів, які потребують додаткової перевірки. Окремо оцінюється здатність системи зберігати журнал змін і встановлювати, які саме операції вплинули на аналітичний результат.

Важливим захисним механізмом є зіставлення інформації з незалежними джерелами. Проте кілька джерел не можна вважати незалежними лише тому, що вони мають різні адреси: вони можуть відтворювати одне й те саме первинне повідомлення. Тому оцінювання має враховувати походження та інформаційну залежність джерел.

8.5.4. Адаптація до зміни поведінки злочинців

Інформаційні шаблони, способи комунікації та механізми вербування можуть змінюватися з часом. Через це алгоритми, навчені на історичних даних, поступово втрачають актуальність. Зниження якості моделі може бути спричинене зміною розподілу вхідних даних, появою нових форматів інформації або зміною взаємозв’язків між ознаками й цільовими результатами.

Для оцінювання адаптивності доцільно проводити періодичне тестування на нових даних, порівнювати показники з базовими результатами й аналізувати відмінності між часовими періодами. Водночас сам факт зміни статистичного розподілу не обов’язково означає погіршення якості: його необхідно підтверджувати контрольними вимірюваннями.

Процес адаптації має включати виявлення зниження якості, перевірку причин, оновлення тестових наборів, повторне навчання за необхідності та незалежну перевірку нової версії. Варто зберігати попередні версії моделей і

забезпечувати можливість повернення до стабільної версії в разі погіршення результатів.

Адаптація не повинна означати неконтрольоване автоматичне перенавчання на всіх нових даних. Якщо до навчального набору потрапляють помилкові або маніпульовані записи, оновлена модель може відтворювати й посилювати ці помилки. Тому нові дані мають проходити перевірку якості та відповідності встановленим правилам.

8.5.5. Кіберстійкість платформи

Кіберстійкість характеризує здатність платформи запобігати кіберінцидентам, виявляти їх, обмежувати наслідки, відновлювати працездатність і зберігати цілісність інформації. Для інтегрованої аналітичної системи це передбачає не лише захист інфраструктури, а й забезпечення доступності критичних функцій та надійності аналітичних результатів.

Оцінювання доцільно проводити за такими напрямами:

- управління доступом і розмежування привілеїв;
- захист каналів передавання та збереження інформації;
- контроль цілісності даних і журналів;
- резервне копіювання та перевірка відновлення;
- виявлення аномальної активності;
- реагування на інциденти;
- перевірка залежностей від зовнішніх сервісів;
- забезпечення безперервності роботи.

Для кількісного оцінювання можуть використовуватися доступність системи, середній час виявлення інциденту, час відновлення, частка успішно відновлених даних і частка критичних операцій, що залишаються працездатними під час відмови окремого компонента.

Тестування має проводитися в контрольованому середовищі та не повинно створювати ризиків для реальних даних або робочих процесів. За результатами перевірки формується перелік виявлених слабких місць, визначаються пріоритети усунення та повторно оцінюється ефективність захисних заходів.

Такий підхід узгоджується з циклічною логікою управління кіберризиками, представленою в NIST Cybersecurity Framework 2.0 [77].

8.6. Комплексна модель оцінювання ефективності

Комплексне оцінювання ефективності цифрових технологій у протидії торгівлі людьми є важливим етапом формування науково обґрунтованого підходу до визначення результативності інформаційно-аналітичних систем, алгоритмів інтелектуального аналізу даних, технологій штучного інтелекту, геоінформаційних систем та засобів цифрової криміналістики. На відміну від оцінювання окремого технологічного компонента, комплексна модель передбачає одночасне врахування технічних, організаційних, оперативних, економічних, правових та соціальних характеристик цифрового середовища. Її призначення не лише у встановленні того, наскільки точно алгоритм виявляє потенційні ознаки злочинної діяльності, а й у визначенні того, чи сприяє його використання своєчасному виявленню ризиків, підвищенню якості аналітичної роботи, належному документуванню інформації та захисту прав осіб, які можуть постраждати від торгівлі людьми.

Торгівля людьми може супроводжуватися використанням цифрових комунікацій, онлайн-платформ, фіктивних пропозицій працевлаштування, електронних платіжних інструментів, посередницьких мереж і переміщенням потерпілих між різними територіями. Виявлення таких проявів вимагає оброблення різнорідних даних, встановлення взаємозв’язків між подіями, обліковими записами, цифровими ідентифікаторами, фінансовими операціями та географічними об’єктами. Методи інтелектуального аналізу даних дають змогу виявляти приховані закономірності у великих масивах інформації, але отримані результати залежать від повноти й репрезентативності даних, коректності обраних алгоритмів і професійної інтерпретації сформованих висновків [107 - 110].

Нормативною основою оцінювання виступають положення законодавства України у сфері протидії торгівлі людьми та захисту персональних даних. Закон України «Про протидію торгівлі людьми» визначає загальні правові засади

відповідної діяльності, тоді як законодавство про захист персональних даних встановлює вимоги до їх оброблення та захисту [6, 98]. Тому ефективність цифрової системи не може визначатися винятково кількістю автоматично сформованих повідомлень, швидкістю пошуку або точністю класифікації. Вона має оцінюватися з урахуванням правомірності використання інформації, обґрунтованості аналітичних висновків, можливості перевірки результатів і потенційних наслідків помилок для конкретних осіб.

Методологічно комплексну модель будують як багаторівневу систему. На першому рівні оцінюються властивості окремих технологічних компонентів: якість виявлення, точність класифікації, стійкість до помилок, швидкодія та відтворюваність результатів. На другому рівні визначається ефективність інформаційно-аналітичного процесу загалом, зокрема здатність системи об’єднувати дані з різних джерел, формувати обґрунтовані аналітичні повідомлення та забезпечувати їх перевірку. На третьому рівні аналізується організаційний результат застосування технології: скорочення часу опрацювання інформації, раціональність використання ресурсів, поліпшення міжвідомчої взаємодії та підвищення якості підтримки рішень. Четвертий рівень охоплює правові, етичні та соціальні наслідки, включно із захистом приватності, недопущенням дискримінаційних результатів і забезпеченням належного контролю з боку уповноважених фахівців.

Такий підхід узгоджується із загальними положеннями NIST Artificial Intelligence Risk Management Framework, у якому управління ризиками штучного інтелекту розглядається як безперервний процес, що охоплює управління, визначення контексту, вимірювання та реагування на ризики. Документ акцентує на необхідності оцінювати системи з урахуванням умов їх реального застосування, надійності, прозорості, безпеки, захисту приватності та справедливості [77].

У контексті протидії торгівлі людьми це означає, що технологічний результат має розглядатися у взаємозв’язку з організаційною процедурою його використання та правовими наслідками прийнятих на його основі рішень.

8.6.1. Інтегральний показник ефективності

Інтегральний показник ефективності призначений для узагальнення результатів оцінювання за сукупністю критеріїв і представлення їх у формі, придатній для порівняння різних технологій, версій алгоритмів або організаційних моделей роботи. Його використання дає змогу уникнути ситуації, коли висновок про ефективність системи ґрунтується лише на одному показнику, наприклад точності класифікації, тоді як інші характеристики залишаються поза увагою.

Для побудова інтегрального показника послідовно виконують кілька методологічних процедур: визначення мети оцінювання; формування набору критеріїв; вибір показників для кожного критерію; приведення показників до порівнюваної шкали; визначення вагових коефіцієнтів; обчислення узагальненого значення; перевірку стійкості отриманого результату до зміни вихідних припущень. Кожна процедура має бути задокументована, оскільки необґрунтований вибір критеріїв або ваг може істотно вплинути на кінцевий рейтинг технологій.

До системи показників включають такі групи характеристик:

- аналітична результативність – Precision, Recall, F1-score, частота хибнопозитивних і хибнонегативних результатів;
- оперативність – час виявлення потенційної загрози, час опрацювання повідомлення, тривалість формування аналітичного висновку;
- повнота та якість інформації – частка опрацьованих релевантних даних, рівень дублювання, частка непідтверджених або застарілих відомостей;
- технологічна надійність – доступність, стабільність функціонування, масштабованість, відтворюваність результатів;
- організаційна й економічна результативність – витрати часу працівників, вартість обслуговування системи, співвідношення витрат і досягнутих результатів;

- правова та етична прийнятність – дотримання вимог щодо оброблення даних, можливість аудиту, пояснюваність висновків, контроль помилкових спрацювань і наявність процедур оскарження.

Для обчислення інтегрального показника застосовують нормалізацію, оскільки різні критерії мають неоднакові одиниці вимірювання. Наприклад, Precision виражається часткою або відсотком, час оброблення – секундами чи хвилинами, а фінансові витрати – грошовими одиницями. Після приведення показників до єдиної шкали їх можна об'єднати за допомогою зваженої адитивної моделі:

$$E_{\int \square} = \sum_{i=1}^{n} \omega_i z_i, \tag{8.35}$$

де $E_{\int \square}$ – інтегральний показник ефективності; z_i – нормалізоване значення i-го критерію; ω_i – ваговий коефіцієнт відповідного критерію; n – кількість критеріїв.

Для показників, збільшення яких свідчить про поліпшення результату, може використовуватися нормалізація за принципом «більше – краще»:

$$z_i = \frac{x_i - x_i^{min}}{x_i^{max} - x_i^{min}}, \tag{8.36}$$

а для показників, зменшення яких є бажаним, наприклад часу оброблення або частоти помилок, – за принципом «менше – краще»:

$$z_i = \frac{x_i^{min} - x_i}{x_i^{max} - x_i^{min}}, \tag{8.37}$$

де x_i – фактичне значення показника, x_i^{min} та x_i^{max} – нижня і верхня межі шкали оцінювання. Якщо діапазон показника дорівнює нулю або його межі визначені недостатньо обґрунтовано, необхідно обрати інший спосіб нормалізації, щоб уникнути математично некоректних результатів.

Вагові коефіцієнти можуть визначатися експертним методом, методом попарних порівнянь або на основі статистичних характеристик даних. Водночас у сфері протидії торгівлі людьми ваги не варто встановлювати винятково за критерієм технічної зручності. Наприклад, висока швидкість роботи не повинна компенсувати неприйнятний рівень хибнопозитивних результатів, якщо вони

можуть спричинити необґрунтовану підозру щодо людини. Так само низька вартість експлуатації не може бути достатньою підставою для вибору системи, яка не забезпечує належного захисту конфіденційної інформації.

З огляду на це інтегральний показник використовують разом із системою обов'язкових порогових вимог. До таких вимог належать мінімально прийнятні значення якості виявлення, дотримання вимог законодавства, наявність журналювання операцій, захист від несанкціонованого доступу, можливість незалежної перевірки результатів і контроль з боку відповідального фахівця. Якщо система не відповідає критичній вимозі, її високий сумарний бал не повинен автоматично означати позитивний висновок щодо можливості практичного використання.

Для підвищення достовірності інтегрального оцінювання перевіряють чутливість результатів до зміни вагових коефіцієнтів і способу нормалізації. Якщо невелика зміна ваг призводить до істотної зміни рейтингу, це свідчить про нестійкість висновку та потребує додаткового аналізу. Відповідно, підсумковий звіт має містити не лише інтегральне значення, а й профіль окремих критеріїв, опис обмежень, рівень невизначеності та пояснення чинників, які найбільше вплинули на результат. Методологічні підходи до інтелектуального аналізу даних і машинного навчання створюють основу для такого кількісного оцінювання, але остаточна інтерпретація повинна враховувати конкретну практичну мету та умови використання системи [107 - 110].

8.6.2. Багатокритеріальна модель оцінювання

Багатокритеріальна модель є розширенням інтегрального оцінювання, оскільки передбачає не лише обчислення узагальненого показника, а й систематичне зіставлення альтернатив за різними, іноді суперечливими характеристиками. Її застосування особливо актуальне в ситуаціях, коли порівнюються інформаційно-аналітичні платформи, алгоритми виявлення ризиків або способи організації оброблення даних, що мають різні переваги та обмеження.

Наприклад, одна система може демонструвати високу повноту виявлення потенційно небезпечних повідомлень, але водночас генерувати значну кількість хибнопозитивних результатів. Інша може забезпечувати кращу точність, проте пропускати частину складних або нетипових випадків. Третя може бути менш ресурсомісткою, але мати обмежені можливості пояснення висновків. У такій ситуації вибір лише за одним показником не дає достатніх підстав для визначення найбільш придатного рішення.

Багатокритеріальна модель має включати щонайменше три рівні: ціль оцінювання, групи критеріїв і конкретні вимірювані показники. На верхньому рівні визначається загальна мета – підвищення спроможності виявляти ознаки торгівлі людьми та забезпечувати якісну підтримку відповідних рішень. На другому рівні формуються групи критеріїв: аналітична якість, оперативність, технологічна надійність, ресурсна ефективність, правова відповідність і вплив на права людини. На третьому рівні встановлюються конкретні показники, за якими можна провести вимірювання й порівняння.

У межах багатокритеріального оцінювання розрізняють компенсаторні та некомпенсаторні критерії. Компенсаторна модель допускає, що нижчий результат за одним показником може бути частково компенсований вищим результатом за іншим. Саме до такого підходу належить зважена адитивна модель. Некомпенсаторна модель, навпаки, передбачає, що окремі вимоги є обов’язковими та не можуть компенсуватися перевагами за іншими параметрами. До них у відповідному контексті належать законність оброблення даних, належний рівень інформаційної безпеки та відсутність неприйнятного ризику істотного порушення прав людини.

Застосування комбінованого підходу дає змогу спочатку відсіяти альтернативи, які не відповідають обов’язковим вимогам, а потім порівнювати прийнятні системи за їхньою ефективністю, ресурсомісткістю та технологічними властивостями. Така процедура зменшує ймовірність того, що система з високими технічними характеристиками буде обрана попри істотні правові або етичні недоліки.

Важливе значення має обґрунтування вагових коефіцієнтів. Експертна група, яка визначає ваги, повинна охоплювати фахівців із протидії торгівлі людьми, аналітиків даних, спеціалістів із кібербезпеки, юристів, експертів із захисту персональних даних та, за можливості, представників організацій, які працюють із постраждалими. Залучення різних професійних перспектив дає змогу зменшити ризик однобічного оцінювання, за якого технологічні показники домінують над правовими та соціальними наслідками.

Для оцінювання можуть застосовуватися метод аналізу ієрархій, метод зваженої суми, методи ранжування альтернатив та аналіз Парето. Останній особливо корисний, якщо жодна альтернатива не переважає інші за всіма критеріями одночасно. У такому випадку формують множину недомінованих альтернатив і визначають, які компроміси між точністю, оперативністю, витратами та іншими характеристиками є прийнятними для конкретного сценарію використання.

Багатокритеріальне оцінювання необхідно здійснювати за однакових або максимально зіставних умов. Порівнювані системи повинні отримувати еквівалентні за змістом тестові дані, використовувати однакові визначення цільових подій та оцінюватися за єдиними правилами обчислення метрик. Якщо одна технологія тестується на простішому наборі даних або в більш сприятливих умовах, результати порівняння не відображатимуть реальних відмінностей у якості. Положення щодо оцінювання моделей, документування ризиків і регулярного моніторингу узгоджуються з рекомендаціями NIST AI RMF, де наголошується на необхідності оцінювати характеристики системи у зв’язку з контекстом її використання та потенційним впливом на зацікавлені сторони [77].

Отже, багатокритеріальна модель дає змогу не лише визначити відносно кращу технологічну альтернативу, а й пояснити, за рахунок яких властивостей вона отримала перевагу, які ризики залишаються невирішеними та які обмеження необхідно врахувати під час практичного впровадження.

8.6.3. Баланс «ефективність – законність – права людини»

Однією з ключових вимог до комплексної моделі є забезпечення балансу між технічною ефективністю цифрових технологій, законністю їх застосування та дотриманням прав людини. У протидії торгівлі людьми цей баланс має принципове значення, оскільки оброблення даних може стосуватися осіб, які перебувають у вразливому становищі, потерпілих, свідків, заявників, членів їхніх сімей або осіб, щодо яких наявна лише неперевірена інформація.

Ефективність характеризує здатність технології досягати визначеної мети: виявляти потенційні ознаки експлуатації, встановлювати взаємозв'язки між подіями, скорочувати час аналізу та підтримувати фахівців у перевірці інформації. Законність означає відповідність способів збирання, зберігання, зіставлення, передавання й використання даних чинним нормативно-правовим вимогам. Дотримання прав людини передбачає недопущення необґрунтованого втручання у приватність, дискримінаційного профілювання, автоматичного приписування вини, стигматизації вразливих груп і поширення чутливих відомостей без належних підстав.

Закон України «Про протидію торгівлі людьми» визначає правові засади діяльності у відповідній сфері [6]. Водночас Закон України «Про захист персональних даних» встановлює вимоги, які необхідно враховувати під час оброблення персональної інформації [98].

Звідси випливає, що доступ до даних і можливість їх автоматизованого аналізу мають визначатися не лише технічною доступністю інформації, а й правовою підставою, метою оброблення, необхідністю такого оброблення та відповідними заходами захисту.

Особливу увагу потрібно приділяти ризику хибнопозитивних результатів. Автоматизована система може позначити як підозрілу діяльність, яка насправді пов'язана із законною міграцією, пошуком роботи, наданням соціальної допомоги або іншими правомірними діями. Якщо такий результат сприймається як встановлений факт, він може спричинити необґрунтовані перевірки, обмеження доступу до послуг, репутаційні втрати або повторну травматизацію

людини. Тому алгоритмічний сигнал має розглядатися як підстава для подальшої перевірки, а не як самодостатній доказ вчинення правопорушення чи підтвердження статусу потерпілої особи.

Не менш небезпечними є хибнонегативні результати, коли система не виявляє реальні ознаки експлуатації. Їхні наслідки можуть полягати у втраті часу, несвоєчасному реагуванні або пропуску зв'язків між окремими епізодами. Таким чином, оцінювання повинно враховувати обидва типи помилок, але їхню вагомість слід визначати з урахуванням конкретного сценарію застосування, можливих наслідків і наявності процедур людської перевірки.

Для практичного забезпечення балансу передбачають такі запобіжники:

- Мінімізація даних. Збирати й обробляти лише ті дані, які необхідні для визначеної законної мети.
- Розмежування доступу. Надавати працівникам доступ відповідно до їхніх повноважень і службових завдань.
- Документування походження інформації. Фіксувати джерело, час отримання, умови оброблення та зміни даних.
- Людський контроль. Передбачати перевірку суттєвих алгоритмічних висновків уповноваженим фахівцем.
- Можливість виправлення помилок. Забезпечувати процедури перегляду неточних даних і оскарження рішень у межах застосовних правових механізмів.
- Контроль упередженості. Перевіряти, чи не погіршуються результати для окремих груп через нерепрезентативність даних або недоліки алгоритму.
- Захист цифрових доказів. Забезпечувати цілісність, простежуваність і належне документування цифрових матеріалів.

Питання цілісності та належного опрацювання цифрових доказів є важливими, якщо результати аналітичної системи використовуються для підтримки кримінального провадження. Рекомендації NIST щодо цифрових розслідувань і збереження цифрових доказів наголошують на необхідності процедурного документування, контролю цілісності даних та належного поводження з доказовими матеріалами [119 - 121]. Ці підходи не замінюють

вимог національного законодавства, але можуть використовуватися як методична основа для формування внутрішніх процедур.

У межах комплексної моделі законність і дотримання прав людини розглядатють не лише як додаткові критерії, які впливають на підсумковий бал, а як обов'язкові умови використання системи. Такий підхід запобігає ситуації, коли висока технічна результативність фактично виправдовує неприйнятне втручання в права людини. У разі виявлення критичного порушення система має бути обмежена в застосуванні, доопрацьована або тимчасово виведена з експлуатації до усунення відповідних недоліків.

Отже, збалансована модель оцінювання має відповідати принципу: цифрові технології є інструментом підтримки професійної діяльності, а не заміною правових процедур, доказового оцінювання та відповідальності уповноважених осіб. Їхня практична цінність визначається не тільки здатністю обробляти інформацію, а й можливістю застосовувати результати законно, обґрунтовано та з повагою до гідності людини.

8.6.4. Формування рейтингу ризиків

Рейтинг ризиків є інструментом упорядкування виявлених загроз за їхньою ймовірністю, потенційним впливом і терміновістю реагування. У сфері протидії торгівлі людьми його можна використовувати для визначення пріоритетності аналітичної перевірки повідомлень, виявлення підозрілих закономірностей у цифровому середовищі, розподілу ресурсів між напрямами роботи та планування подальших заходів. При цьому рейтинг повинен відображати рівень аналітичного ризику, а не встановлювати юридичну винуватість конкретної особи.

Формування рейтингу передбачає кілька послідовних етапів. На першому етапі визначаються об'єкти оцінювання: повідомлення, цифрові оголошення, взаємозв'язки між подіями, потенційні схеми експлуатації або інші аналітичні об'єкти. На другому етапі встановлюються критерії ризику, які можуть охоплювати наявність ознак примусу чи обману, суперечливість відомостей, повторюваність контактів, географічні закономірності, пов'язані цифрові

ідентифікатори та інші релевантні індикатори. На третьому етапі визначаються джерела даних і правила їх перевірки. На четвертому етапі обчислюється рівень ризику, після чого формується черговість аналітичного опрацювання. На завершальному етапі результати перевіряються фахівцями, а висновки документуються.

Для початкового ранжування можна використовувати модель, що поєднує оцінку ймовірності події та тяжкості її потенційних наслідків:

$$R_i = P_i * I_i, \tag{8.38}$$

де R_i – узагальнений рівень ризику для *i*-го об’єкта; P_i – оцінка ймовірності реалізації відповідної загрози; I_i – оцінка потенційного впливу. Якщо показники визначаються за шкалою від 1 до 5, то добуток може набувати значень від 1 до 25. Для практичного використання межі категорій низького, середнього та високого ризику необхідно встановлювати за результатами експертного узгодження й перевірки на реальних або належним чином підготовлених тестових даних. Такі межі не слід вважати універсальними для всіх сценаріїв.

За наявності декількох індикаторів можна застосовувати зважену модель:

$$R_i = \sum_{j=1}^{m} \alpha_j q_{ij}, \tag{8.39}$$

де q_{ij} – нормалізоване значення j -го індикатора для об’єкта i; α_j – ваговий коефіцієнт індикатора; m – кількість індикаторів. Ваги мають відображати обґрунтовану значущість відповідних ознак, а не лише їхню частоту в історичних даних. Якщо певні ознаки є надмірно представленими в навчальній вибірці або пов’язані з соціальними характеристиками певної групи, алгоритм може помилково відтворювати наявні в даних упередження.

Рейтинг ризиків має враховувати якість і надійність вихідної інформації. Наприклад, повідомлення з кількох незалежних джерел, які узгоджуються між собою, може мати інший рівень достовірності, ніж твердження, що походить з одного неперевіреного джерела. Водночас кількість згадок не обов’язково свідчить про незалежність підтверджень: кілька веб-сторінок можуть копіювати одне й те саме первинне повідомлення. Тому системі потрібно розрізняти

кількість згадок, кількість незалежних джерел і ступінь підтвердженості інформації.

У рейтингу теж потрібно розділяти два поняття: ризик для потенційної жертви та рівень пріоритетності аналітичної перевірки. Перший стосується можливості заподіяння шкоди людині та потребує особливо уважного, орієнтованого на захист підходу. Другий характеризує черговість опрацювання інформації з урахуванням терміновості, потенційного впливу та доступних ресурсів. Їх змішування може призвести до того, що високий рейтинг помилково сприйматиметься як характеристика самої людини, а не ситуації чи інформаційного сигналу.

Для зменшення таких ризиків треба передбачити можливість ручного перегляду рейтингу, фіксацію підстав його формування, зазначення рівня невизначеності та повторне оцінювання після отримання нової інформації. Якщо алгоритм не має достатніх даних або виявляє суперечності, доцільно формувати статус «недостатньо інформації для надійної оцінки», а не штучно присвоювати точне числове значення.

У практичному застосуванні рейтинг ризиків повинен бути динамічним. Нові відомості, результати перевірок, зміни в поведінці цифрових об’єктів або спростування раніше отриманої інформації мають спричиняти перегляд відповідної оцінки. Зміну рейтингу потрібно простежувати: система має зберігати попередні значення, підстави оновлення та відомості про те, хто і коли перевірив результат. Такий підхід узгоджується з рекомендаціями щодо управління ризиками ШІ, які передбачають пріоритизацію ризиків, документування рішень і регулярний моніторинг системи [77].

Отже, рейтинг ризиків розглядають як механізм підтримки пріоритетності роботи, а не як автоматизовану процедуру ухвалення остаточних правових або оперативних рішень. Його якість визначається не лише точністю ранжування, а й прозорістю критеріїв, достовірністю вихідних даних, можливістю перевірки та належним урахуванням прав людини.

8.6.5. Використання результатів оцінювання для вдосконалення системи

Результати комплексного оцінювання мають практичну цінність лише за умови їх систематичного використання для вдосконалення технологічних компонентів, організаційних процедур і методів роботи з даними. Саме тому оцінювання не повинно завершуватися формуванням звіту або присвоєнням системі певного рейтингу. Воно має стати частиною циклу управління якістю, у межах якого виявлені недоліки перетворюються на конкретні завдання з визначеними строками, відповідальними особами та критеріями перевірки результату.

Першим напрямом використання результатів є вдосконалення даних. Якщо аналіз показує, що алгоритм систематично пропускає певні типи ситуацій, необхідно перевірити репрезентативність навчальної та тестової вибірок, коректність розмітки, наявність пропусків, дублювання й помилкових атрибутів. У разі виявлення дисбалансу класів або недостатнього представлення окремих сценаріїв слід скоригувати процес формування вибірок і повторно перевірити модель на даних, які не використовувалися під час її навчання. Методичні підходи до інтелектуального аналізу даних та машинного навчання можуть бути використані для організації таких процедур [107 - 110].

Другий напрям полягає у вдосконаленні алгоритмів. Аналіз хибнопозитивних і хибнонегативних результатів дає змогу визначити, за яких умов система припускається помилок, які ознаки виявляються недостатньо інформативними та чи є доцільним змінювати поріг класифікації, модель ознак або алгоритм оброблення. Однак зміна параметрів не повинна ґрунтуватися лише на бажанні підвищити один показник. Наприклад, зниження порога спрацювання може збільшити повноту виявлення, але одночасно спричинити зростання хибнопозитивних повідомлень. Тому кожне вдосконалення необхідно перевіряти за комплексом показників, а також аналізувати його вплив на різні групи даних і практичні сценарії.

Третій напрям пов’язаний з оптимізацією організаційних процесів. Якщо оцінювання встановлює, що найбільше часу витрачається не на автоматизований пошук, а на ручне зведення даних із різних джерел, першочерговим завданням може бути не заміна алгоритму, а вдосконалення інтеграції інформаційних ресурсів, уніфікація форматів, усунення дублювання та оптимізація робочих процедур. Аналогічно, якщо система генерує значну кількість аналітичних повідомлень, які фахівці не встигають опрацьовувати, необхідно переглянути правила пріоритизації, структуру повідомлень і механізми контролю якості.

Четвертий напрям охоплює підвищення правової та інформаційної безпеки. Виявлені недоліки можуть стосуватися надмірного збирання даних, недостатнього розмежування доступу, відсутності журналювання, невизначених термінів зберігання або недостатньої простежуваності операцій. У таких випадках заходи вдосконалення мають включати перегляд політик доступу, уточнення процедур оброблення персональних даних, підвищення захищеності інформаційної інфраструктури та вдосконалення процесів збереження цифрових матеріалів [98, 119 - 121].

П’ятий напрям полягає в організації безперервного управління ризиками. Використовують цикл, який включає планування оцінювання, вимірювання показників, аналіз відхилень, визначення коригувальних заходів, повторне тестування та документування результатів. Такий підхід дає змогу оцінювати не тільки поточний стан системи, а й ефективність заходів, спрямованих на усунення попередньо виявлених недоліків.

Для практичної реалізації цього циклу кожному виявленому недоліку слід присвоювати рівень критичності, визначати ймовірні причини, відповідальну особу, необхідні ресурси, строк усунення та спосіб перевірки. Після виконання коригувальних заходів проводиться повторне оцінювання за тими самими або методологічно зіставними показниками. Це дає змогу встановити, чи було досягнуто очікуваного поліпшення, чи не виникли побічні негативні наслідки та чи не перемістився ризик до іншого компонента системи.

Для кожної версії алгоритму зберігають опис призначення, використаних даних, параметрів, результатів тестування, відомих обмежень і рішень щодо допуску до використання. Така документація створює основу для відтворюваності експериментів, порівняння версій і незалежного аудиту. Рекомендації NIST щодо управління ризиками ШІ також наголошують на документуванні результатів вимірювання, пріоритизації ризиків і постійному перегляді системи впродовж життєвого циклу [77].

Таким чином, результати комплексного оцінювання повинні бути безпосередньо пов’язані з управлінськими рішеннями щодо вдосконалення цифрової системи. Вони дають змогу обґрунтовано визначати пріоритети технічного доопрацювання, коригувати робочі процедури, удосконалювати підготовку фахівців і зменшувати ризики порушення прав людини. Комплексна модель у такому разі перетворюється з інструмента одноразового вимірювання на постійний механізм контролю якості та відповідального використання цифрових технологій.

Висновки до розділу 8

У цьому розділі монографії розглянуто методологічні засади оцінювання ефективності цифрових технологій у протидії торгівлі людьми, визначено основні критерії результативності інформаційно-аналітичних систем і систематизовано показники, що дають змогу оцінювати практичну цінність відповідних технологічних рішень. Встановлено, що ефективність цифрової протидії торгівлі людьми необхідно розглядати як комплексну характеристику, яка охоплює оперативність опрацювання інформації, точність і повноту виявлення потенційних загроз, доказовість аналітичних результатів, кіберстійкість системи та можливість використання отриманих відомостей для підтримки обґрунтованих рішень уповноважених фахівців.

Обґрунтовано доцільність застосування системи кількісних показників, зокрема Precision, Recall, F1-score, False Positive Rate і False Negative Rate, а також

показників часу виявлення загрози, оперативності реагування, якості прогнозування, масштабованості та економічної ефективності. Їх комплексне використання забезпечує можливість порівнювати різні технологічні рішення, виявляти обмеження їх функціонування та визначати напрями подальшого вдосконалення. При цьому оцінювання не повинно обмежуватися окремими технічними характеристиками, оскільки швидкість оброблення даних або висока точність класифікації самі по собі не гарантують належного практичного результату.

Визначено особливості оцінювання основних технологічних компонентів протидії торгівлі людьми. Зокрема, OSINT забезпечує пошук і первинний аналіз інформації з відкритих джерел, Big Data сприяє опрацюванню значних масивів різнорідних даних, а геоінформаційні системи дають змогу виявляти просторові закономірності та взаємозв'язки. Технології машинного навчання й штучного інтелекту підтримують автоматизоване виявлення ознак ризику та прогнозування, тоді як цифрова криміналістика орієнтована на дослідження, збереження цілісності й перевірюваність цифрових доказів. Результативність інтегрованих аналітичних платформ залежить від узгодженої взаємодії зазначених компонентів, якості вхідних даних і належної організації інформаційних процесів.

Важливим методологічним положенням є необхідність порівняльного оцінювання цифрових технологій із традиційними підходами на основі контрольних і тестових вибірок, повторюваних експериментів та статистичної перевірки результатів. Такий підхід дає змогу об'єктивніше визначати реальний внесок технологічних засобів у підвищення результативності протидії торгівлі людьми. Доцільним є використання дворівневої моделі оцінювання, яка передбачає перевірку мінімально допустимих значень критичних показників і подальший розрахунок інтегрального показника для порівняння альтернативних рішень.

Отже, оцінювання ефективності цифрових технологій у протидії торгівлі людьми має ґрунтуватися на комплексному, багатокритеріальному та

доказовому підході з обов’язковим урахуванням вимог кібербезпеки, захисту персональних даних і дотримання прав людини. Результати автоматизованого аналізу повинні підлягати перевірці уповноваженими фахівцями та розглядатися як засіб підтримки прийняття рішень. Практичне застосування запропонованих методологічних положень створює основу для обґрунтованого вибору цифрових інструментів, удосконалення інформаційно-аналітичних систем і підвищення результативності заходів із попередження, виявлення та розслідування випадків торгівлі людьми.

ВИСНОВКИ

Проведений у монографії аналіз засвідчує, що використання сучасних інформаційних технологій змінює підходи до протидії торгівлі людьми на різних етапах – від виявлення можливих ознак вербування до документування цифрових матеріалів, аналізу зв'язків між інформаційними об'єктами, оцінювання ризиків і організації допомоги постраждалим особам. Водночас сама наявність цифрових даних не гарантує правильного розуміння подій. Оголошення про працевлаштування, контактні відомості, зображення, географічні позначки та фінансові операції можуть містити важливу інформацію, проте кожен такий об'єкт потребує перевірки походження, достовірності й контексту. Тому основне завдання інформаційно-аналітичної роботи полягає не в накопиченні якомога більшого обсягу відомостей, а в їх обґрунтованому зіставленні та формуванні висновків, які можна перевірити.

Розгляд теоретико-правових засад протидії торгівлі людьми дав змогу визначити нормативні та організаційні передумови використання цифрових технологій у цій сфері. Їх застосування має узгоджуватися із законодавством України, міжнародними стандартами, вимогами захисту персональних даних і правами людини. Ці вимоги стосуються не лише збирання інформації, а й усього подальшого процесу її оброблення, зберігання, передавання та використання. Отже, правомірність і безпека роботи з даними мають розглядатися як невід'ємні складові інформаційно-аналітичної діяльності, а не як додаткові умови, які враховуються після отримання результатів.

Аналіз інформаційних технологій виявлення торгівлі людьми показав, що різні методи виконують взаємодоповнювальні функції. OSINT дає змогу збирати й перевіряти відомості з відкритих джерел; аналіз великих даних – опрацьовувати значні масиви різнорідної інформації; геоінформаційні технології – досліджувати просторові закономірності; графовий аналіз – встановлювати можливі зв'язки між обліковими записами, контактами, оголошеннями та іншими об'єктами; машинне навчання й штучний інтелект – автоматизувати окремі завдання класифікації, виявлення аномалій і групування даних.

Поєднання цих методів дозволяє сформувати цілісніше аналітичну картину, ніж ізольоване використання одного джерела або алгоритму. Однак виявлений збіг, кластер чи статистична аномалія є підставою для подальшої перевірки, а не самостійним підтвердженням злочинної діяльності.

Окреме значення має належне документування цифрових матеріалів. Їх використання в розслідуванні потребує збереження первинних даних, фіксації джерела та обставин отримання, контролю цілісності й простежуваності операцій із ними. Інструменти хешування, метадані, часові позначки та реєстрація дій із цифровими об’єктами допомагають перевірити, чи змінювався матеріал і яким шляхом було отримано аналітичний результат. Водночас технічне підтвердження цілісності не визначає автоматично процесуального статусу інформації. Питання її достовірності, належності та допустимості вирішуються з урахуванням конкретних обставин і вимог процесуального законодавства. Таким чином, аналітична інформація може спрямовувати перевірку версій, але не підміняє процесуального оцінювання доказів.

Розглянуті у монографії практичні кейси демонструють можливості поєднання OSINT, просторового аналізу, інтеграції різнорідних даних і виявлення аномалій у межах спільного аналітичного процесу. Приклади охоплюють аналіз оголошень про працевлаштування, встановлення повторюваних контактних даних, дослідження просторового розподілу інформаційних сигналів, інтеграцію даних за архітектурою Lakehouse та пошук нетипових транзакцій. Їх значення полягає в демонстрації логіки застосування відповідних методів і взаємодії технологічних компонентів. Водночас використання модельних і синтетичних даних обмежує можливості перенесення отриманих результатів на реальні провадження. Наведені приклади не дають достатніх підстав стверджувати, що запропоновані рішення вже забезпечили вимірюване підвищення результативності протидії торгівлі людьми в практичній діяльності правоохоронних органів.

У частині розвитку інформаційної інфраструктури обґрунтовано доцільність розгляду аналітичної платформи як середовища для впорядкованого

опрацювання різнорідних даних. Архітектура Lakehouse дає змогу поєднувати збереження первинної інформації з формуванням підготовлених для аналізу наборів даних, а також передбачати контроль їх якості та походження. Важливими умовами такої організації є узгодження форматів, розмежування доступу, визначення відповідальності за дані, контроль операцій і забезпечення можливості відтворення аналітичного процесу. У монографії також розглянуто перспективи інтеграції відповідних рішень у національну систему протидії торгівлі людьми, міжвідомчої взаємодії та міжнародного обміну інформацією. Їх реалізація, однак, залежить не лише від технічної сумісності систем, а й від правових підстав передавання даних, організаційної готовності учасників та належного захисту інформації.

Кримінологічний аналіз і моделювання ризиків у цифровому середовищі доповнюють технологічний підхід розглядом закономірностей, чинників і взаємозв'язків, які можуть мати значення для виявлення торгівлі людьми. Застосування описового, діагностичного, прогнозного та прескриптивного рівнів аналізу дає змогу послідовно переходити від узагальнення наявних відомостей до з'ясування можливих причин і зв'язків, оцінювання ймовірних ризиків та підготовки обґрунтованих варіантів подальших дій. При цьому прогноз не слід ототожнювати з установленням факту правопорушення, а ризикову оцінку – з висновком про винуватість конкретної особи. Надійність результатів залежить від повноти й репрезентативності даних, коректності обраних методів, урахування обмежень моделей і професійної перевірки отриманих висновків.

Важливою складовою протидії торгівлі людьми є цифрова профілактика та організація безпечного доступу до допомоги. Їх ефективність не визначається лише кількістю інформаційних матеріалів, онлайн-сервісів або автоматизованих функцій. Вирішальне значення має те, чи допомагають вони людині перевірити сумнівну пропозицію, безпечно звернутися по підтримку, отримати необхідну послугу та зберегти контроль над власними даними й засобами комунікації. Цифрові канали мають враховувати можливі ризики спостереження або контролю з боку кривдника, потребу в конфіденційності, доступності сервісів

для різних груп користувачів і недопущенні повторної травматизації. Запропонована в монографії модель індивідуального цифрового плану безпеки орієнтує на вибір дій відповідно до конкретної ситуації, а не на застосування однакових технічних рекомендацій до всіх випадків. Автоматизовані засоби можуть підтримувати інформування та маршрутизацію звернень, але рішення, що істотно впливають на безпеку людини й доступ до допомоги, мають залишатися під контролем компетентних фахівців.

Розгляд методології оцінювання ефективності цифрових технологій дав змогу систематизувати показники, необхідні для аналізу якості їх роботи. До них належать точність і повнота виявлення, співвідношення хибнопозитивних і хибнонегативних результатів, час виявлення та реагування, якість прогнозування, масштабованість, економічні характеристики й придатність отриманих матеріалів до подальшого використання. Окремо необхідно враховувати кіберстійкість систем, захист персональних даних і дотримання прав людини. Жоден показник сам по собі не дає повної оцінки результативності: наприклад, збільшення повноти виявлення може супроводжуватися зростанням кількості хибних сигналів. Тому в монографії обґрунтовано комплексний підхід, що передбачає порівняння технологічних рішень, перевірку критичних показників і врахування правових та безпекових обмежень. Для підтвердження практичної ефективності потрібні контрольовані випробування, верифіковані дані, повторюваність оцінювання та незалежна експертна перевірка.

Узагальнюючи результати дослідження, слід зазначити, що інформаційні технології створюють можливості для системнішого виявлення, аналізу та документування ознак торгівлі людьми, але не усувають невизначеності, властивої роботі з неповними й неоднозначними даними. Практична цінність цифрових рішень залежить від поєднання технологічних засобів із належними процедурами перевірки, професійною компетентністю працівників, захистом інформації та дотриманням прав людини. Запропоновані в монографії підходи формують методологічну основу для подальшого вдосконалення інформаційно-аналітичної діяльності, однак їх широке впровадження має спиратися на

результати окремої практичної апробації. Подальші дослідження доцільно спрямувати на перевірку розглянутих моделей на законно отриманих і верифікованих даних, порівняльне оцінювання технологічних рішень, визначення прийнятних рівнів помилок та уточнення організаційних і правових умов їх застосування. Саме послідовна перевірка аналітичної користі, безпеки й правомірності цифрових технологій дасть змогу обґрунтовано визначати можливості їх використання у протидії торгівлі людьми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. New York : United Nations, 2000. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons (дата звернення: 24.09.2026).

2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341–III. База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 07.09.2026).

3. McAuliffe M., Triandafyllidou A., eds. *World Migration Report 2022*. Geneva : International Organization for Migration, 2021.

4. Council of Europe. *Convention on Action against Trafficking in Human Beings*. Warsaw, 16 May 2005.

5. U.S. Department of State. *2023 Trafficking in Persons Report*. Washington, DC: U.S. Department of State, 2023.

6. Про протидію торгівлі людьми : Закон України від 20.09.2011 № 3739-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/3739-17 (дата звернення: 26.09.2026).

7. Міністерство соціальної політики, сім'ї та єдності України. *Протидія торгівлі людьми.* URL: https://www.msp.gov.ua/about/klyuchovi-napryamy/protydiya-torhivli-lyudmy (дата звернення: 26.09.2026).

8. Casey E. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. 3rd ed. Waltham : Academic Press, 2011.

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). P. 1–88.

10. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2297-17 (дата звернення: 26.09.2026).

11. Kulldorff M. A spatial scan statistic. *Communications in Statistics – Theory and Methods*. 1997. Vol. 26, No. 6. P. 1481–1496.

12. Ester M., Kriegel H.-P., Sander J., Xu X. A density-based algorithm for discovering clusters in large spatial databases with noise. *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96)*. 1996. P. 226–231.

13. Birant D., Kut A. ST-DBSCAN: An algorithm for clustering spatial–temporal data. *Data & Knowledge Engineering*. 2007. Vol. 60, No. 1. P. 208–221. DOI: 10.1016/j.datak.2006.01.013

14. Wasserman S., Faust K. *Social Network Analysis: Methods and Applications*. Cambridge : Cambridge University Press, 1994.

15. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey. *ACM Computing Surveys*. 2009. Vol. 41, No. 3. Art. 15.

16. Box G. E. P., Jenkins G. M., Reinsel G. C., Ljung G. M. *Time Series Analysis: Forecasting and Control*. 5th ed. Hoboken : Wiley, 2015.

17. Keim D. A., Mansmann F., Schneidewind J., Thomas J., Ziegler H. Visual analytics: Scope and challenges. *Visual Data Mining*. Lecture Notes in Computer Science. Berlin : Springer, 2008. Vol. 4404. P. 76–90.

18. European Union Agency for Fundamental Rights. *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*. Luxembourg : Publications Office of the European Union, 2019.

19. Sculley D., Holt G., Golovin D. et al. Hidden technical debt in machine learning systems. *Advances in Neural Information Processing Systems*. 2015. Vol. 28. P. 2503–2511.

20. ISO/IEC 25012:2008. *Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model*. Geneva : ISO, 2008.

21. ISO/IEC 11179-1:2023. *Information technology – Metadata registries (MDR) – Part 1: Framework*. Geneva : ISO, 2023.

22. Bitol. *Open Data Contract Standard (ODCS)*, v3.2.0. URL: https://github.com/bitol-io/open-data-contract-standard (дата звернення: 27.09.2026).

23. Great Expectations. *GX Core: Open Source Data Quality Platform* Great Expectations. URL: https://greatexpectations.io/ (дата звернення: 26.09.2026).

24. OpenLineage. *Open Standard for Lineage Metadata Collection.* URL: https://openlineage.io/ (дата звернення: 26.09.2026).

25. Silverman B. W. *Density Estimation for Statistics and Data Analysis*. London : Chapman and Hall, 1986.

26. QGIS Project. *QGIS 3.44 Documentation. Heatmap (kernel density estimation).* URL: https://docs.qgis.org/3.44/en/docs/user_manual/processing_algs/qgis/interpolation.html (дата звернення: 27.09.2026).

27. Fortunato S., Hric D. Community detection in networks: A user guide. *Physics Reports*. 2016. Vol. 659. P. 1–44.

28. Elmasri R., Navathe S. B. *Fundamentals of Database Systems*. 7th ed. Boston : Pearson, 2016.

29. Robinson I., Webber J., Eifrem E. *Graph Databases*. 2nd ed. Sebastopol, CA : O'Reilly Media, 2015.

30. Financial Action Task Force. *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*. Paris : FATF, 2020. URL: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html (дата звернення: 26.09.2026).

31. Feldman R., Sanger J. *The Text Mining Handbook: Advanced Approaches in Analyzing Unstructured Data*. Cambridge : Cambridge University Press, 2007.

32. Manning C. D., Raghavan P., Schütze H. *Introduction to Information Retrieval*. Cambridge : Cambridge University Press, 2008.

33. Devlin J., Chang M.-W., Lee K., Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding. *Proceedings of NAACL-HLT 2019*. Minneapolis, 2019. P. 4171–4186.

34. Jurafsky D., Martin J. H. *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition with Language Models*. 3rd ed. Online manuscript released 19 August 2026. URL: https://web.stanford.edu/~jurafsky/slp3/ (дата звернення: 26.09.2026).

35. Aggarwal C. C. *Outlier Analysis*. 2nd ed. Cham : Springer, 2017.

36. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest. *2008 Eighth IEEE International Conference on Data Mining*. Pisa : IEEE, 2008. P. 413–422.

37. Breunig M. M., Kriegel H.-P., Ng R. T., Sander J. LOF: Identifying density-based local outliers. *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data*. 2000. P. 93–104.

38. Schölkopf B., Platt J. C., Shawe-Taylor J., Smola A. J., Williamson R. C. Estimating the support of a high-dimensional distribution. *Neural Computation*. 2001. Vol. 13, No. 7. P. 1443–1471.

39. Jain A. K. Data clustering: 50 years beyond K-means. *Pattern Recognition Letters*. 2010. Vol. 31, No. 8. P. 651–666.

40. MacQueen J. Some methods for classification and analysis of multivariate observations. *Proceedings of the Fifth Berkeley Symposium on Mathematical Statistics and Probability*. Berkeley : University of California Press, 1967. Vol. 1. P. 281–297.

41. Campello R. J. G. B., Moulavi D., Sander J. Density-based clustering based on hierarchical density estimates. *Advances in Knowledge Discovery and Data Mining*. Berlin ; Heidelberg : Springer, 2013. P. 160–172.

42. Xu D., Tian Y. A comprehensive survey of clustering algorithms. *Annals of Data Science*. 2015. Vol. 2, No. 2. P. 165–193.

43. Karame G. O., Androulaki E. *Bitcoin and Blockchain Security*. Boston ; London : Artech House, 2016.

44. ISO/IEC 27037:2012. *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*. Geneva : ISO, 2012.

45. Sammons J. *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. 2nd ed. Waltham : Syngress, 2014.

46. Stallings W. *Cryptography and Network Security: Principles and Practice*. 8th ed. Harlow : Pearson, 2020.

47. Sandhu R. S., Coyne E. J., Feinstein H. L., Youman C. E. Role-based access control models. *Computer*. 1996. Vol. 29, No. 2. P. 38–47.

48. Casey E., ed. *Handbook of Digital Forensics and Investigation*. Burlington : Academic Press, 2010.

49. Council of Europe. *Convention on Cybercrime*. Budapest, 23 November 2001. ETS No. 185.

50. pHash.org. *pHash How To.* URL: https://phash.org/docs/howto.html (дата звернення: 27.09.2026).

51. Krawetz N. *A Picture's Worth: Digital Image Analysis and Forensics*. Black Hat USA Briefings. Las Vegas, 2007.

52. Farid H. *Photo Forensics*. Cambridge, MA : MIT Press, 2016.

53. Korshunov P., Marcel S. Deepfakes: A new threat to face recognition? Assessment and detection. *arXiv*. 2018. arXiv:1812.08685.

54. Mittelstadt B. D., Russell C., Wachter S. Explaining explanations in AI. *Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency*. New York : ACM, 2019. P. 279–288.

55. INTERPOL. *Guidelines for Digital Forensics First Responders: Best Practices for Search and Seizure of Electronic and Digital Evidence*. Singapore : INTERPOL Innovation Centre, 2021.

56. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

penalties. *Official Journal of the European Union and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*. OJ L 119, 4.5.2016, pp. 89–131.

57. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 27.09.2026).

58. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 27.09.2026).

59. Council of Europe Convention on Action against Trafficking in Human Beings. Warsaw, 16 May 2005. CETS No. 197. URL: https://www.coe.int/en/web/conventions/full%E2%80%93list?module=treaty-detail&treatynum=197 (дата звернення: 24.09.2026).

60. Global Report on Trafficking in Persons 2024. Vienna : United Nations Office on Drugs and Crime, 2024. 176 p. ISBN 978–92–1–106989–1. URL: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP24_special_points_final.pdf (дата звернення: 24.09.2026).

61. Policy action to address technology–facilitated trafficking in human beings. Vienna : OSCE Office of the Special Representative and Co–ordinator for Combating Trafficking in Human Beings, 2024. URL: https://cthb.osce.org/cthb/579190 (дата звернення: 24.09.2026).

62. Ukraine: organized crime dynamics in the context of war. Vienna : United Nations Office on Drugs and Crime, 2025. 81 p. URL: https://www.unodc.org/documents/data-and-analysis/Ukraine/Ukraine_OC_Study.pdf (дата звернення: 24.09.2026).

63. Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools. Vienna : OSCE Office of the Special

Representative and Co–ordinator for Combating Trafficking in Human Beings, 2020. URL: https://cthb.osce.org/cthb/455206 (дата звернення: 24.09.2026).

64. Technology in human trafficking. OSCE Office of the Special Representative and Co–ordinator for Combating Trafficking in Human Beings. URL: https://cthb.osce.org/cthb/technology (дата звернення: 24.09.2026).

65. Workshop for CSOs and frontline responders on identifying and responding to technology–facilitated trafficking in Context of Ukraine. OSCE Office for Democratic Institutions and Human Rights, 2026. URL: https://odihr.osce.org/event/662410 (дата звернення: 24.09.2026).

66. New frontiers: The use of generative artificial intelligence to facilitate trafficking in persons. Vienna : OSCE Office of the Special Representative and Co–ordinator for Combating Trafficking in Human Beings; Regional Support Office of the Bali Process, 2024. URL: https://cthb.osce.org/cthb/579715 (дата звернення: 25.09.2026).

67. ILO Indicators of Forced Labour. Geneva : International Labour Office, Special Action Programme to Combat Forced Labour, 2012. URL: ilo.org (дата звернення: 25.09.2026).

68. Following the Money 2.0: A Collaborative Approach to Human Trafficking Investigations Involving Virtual Assets : OSCE Office of the Special Representative and Co–ordinator for Combating Trafficking in Human Beings, 2026. URL: https://cthb.osce.org/sites/default/files/documents/publications/2026/04/FollowingTheMoney_2026_screen_260407.pdf (дата звернення: 25.09.2026).

69. Ratcliffe J. H. Intelligence–Led Policing. 2nd ed. Abingdon : Routledge, 2016. 224 p.

70. United Nations Office on Drugs and Crime. *Criminal Intelligence Manual for Front–line Law Enforcement*. Vienna : United Nations, 2010. 100 p.

71. Поліщук О. Д. Центральність у складних мережах та посередництво у мережевих системах. *Математичне та комп'ютерне моделювання. Серія: Фізико-математичні науки.* Випуск 19. с. 119. URL: https://mcm-math.kpnu.edu.ua/article/view/174199/174152 (дата звернення: 07.09.2026).

72. Федчак І.А. Сучасна аналітична розвідка : *підручник*. Львів : Львівський державний університет внутрішніх справ, 2026. 456 с.

73. Traag V. A., Waltman L., van Eck N. J. From Louvain to Leiden: guaranteeing well–connected communities. *Scientific Reports.* 2019. Vol. 9. Article 5233. URL: https://www.nature.com/articles/s41598-019-41695-z (дата звернення: 07.09.2026).

74. Albert R., Jeong H., Barabási A.–L. Error and attack tolerance of complex networks. *Nature.* 2000. Vol. 406. P. 378–382. URL: https://www.nature.com/articles/35019019 (дата звернення: 07.09.2026).

75. Hyndman R. J., Athanasopoulos G. Forecasting: Principles and Practice. 3rd ed. Melbourne : OTexts, 2021. 442 p. URL: https://otexts.com/fpp3/ (дата звернення: 01.10.2026).

76. McNeish D., Wolf M. G. Thinking thrice about sum scores, and then some more about measurement and analysis. *Behavior Research Methods.* 2023. Vol. 55. P. 788–809. URL: https://link.springer.com/article/10.3758/s13428-022-01849-w (дата звернення: 01.10.2026).

77. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg : National Institute of Standards and Technology, 2023. NIST AI 100–1. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (дата звернення: 01.10.2026).

78. Autio C., Schwartz R., Dunietz J., Jain S., Stanley M., Hall P., Roberts K., Tabassi E. Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile. Gaithersburg : National Institute of Standards and Technology, 2024. NIST AI 600–1. URL: https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-generative-artificial-intelligence (дата звернення: 01.10.2026).

79. United Nations Office on Drugs and Crime. Countering Trafficking in Persons in Conflict Situations. Vienna : United Nations, 2018. URL: https://www.unodc.org/documents/human-trafficking/2018/17-08776_ebook-

Countering_Trafficking_in_Persons_in_Conflict_Situations.pdf (дата звернення: 07.09.2026).

80. National Institute of Standards and Technology. *NIST AI RMF Playbook*. Gaithersburg : NIST, 2023. URL: https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook (дата звернення: 07.09.2026).

81. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. 2024. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng (дата звернення: 07.09.2026).

82. International Organization for Migration. Migrant Vulnerability to Human Trafficking and Exploitation: Evidence from the Central and Eastern Mediterranean Migration Routes. Geneva : IOM, 2017. 94 p. ISBN 978–92–9068–755–9. URL: https://publications.iom.int/books/migrant-vulnerability-human-trafficking-and-exploitation-evidence-central-and-eastern (дата звернення: 07.09.2026).

83. International Organization for Migration. *IOM Handbook on Protection and Assistance for Migrants Vulnerable to Violence, Exploitation and Abuse.* Geneva : IOM, 2019. URL: https://www.iom.int/iom-handbook-migrant-protection-and-assistance (дата звернення: 07.09.2026).

84. Europol. The Challenges of Countering Human Trafficking in the Digital Era. The Hague : Europol, 2020. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf (дата звернення: 07.09.2026).

85. Europol. A rapidly evolving criminal ecosystem: the escalating exploitation of vulnerable individuals. 5 December 2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/rapidly-evolving-criminal-ecosystem-escalating-exploitation-of-vulnerable-individuals (дата звернення: 07.09.2026).

86. INTERPOL. Inside INTERPOL's probe into cyber–enabled human trafficking. 18 December 2024. URL:

https://www.interpol.int/News-and-Events/News/2024/Inside-INTERPOL-s-probe-into-cyber-enabled-human-trafficking (дата звернення: 07.09.2026).

87. Organization for Security and Co–operation in Europe. Strengthening capacity of the National Police of Ukraine to combat trafficking in human beings, including cyber–enabled crime. URL: https://www.osce.org/osce-secretariat-exb-support-programme-for-ukraine/544150 (дата звернення: 07.09.2026).

88. Policy action to address technology-facilitated trafficking in human beings : report of the regional consultations led in 2023 by the OSCE's Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings. Vienna : OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, 2024. 44 p. ISBN 978-92-9271-405-5. URL: https://www.osce.org/files/f/documents/8/d/579190_0.pdf (дата звернення: 02.10.2026).

89. Europol. Digital sprint to disrupt sexual exploitation of Ukrainian nationals. 28 February 2025. URL: https://www.europol.europa.eu/media-press/newsroom/news/digital-sprint-to-disrupt-sexual-exploitation-of-ukrainian-nationals (дата звернення: 07.09.2026).

90. National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0). Gaithersburg : National Institute of Standards and Technology, 2023. 42 p. DOI: 10.6028/NIST.AI.100-1. URL: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (дата звернення: 02.10.2026).

91. Organization for Security and Co-operation in Europe. *Policy action to address technology-facilitated trafficking in human beings*. Office of the Special Representative and Co-ordinator for Combating *Trafficking* in Human Beings. 24 October 2024. URL: https://cthb.osce.org/cthb/579190 (дата звернення: 02.10.2026).

92. Directive (EU) 2024/1712 of the European Parliament and of the Council of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. *Official Journal of the European Union*. 24 June 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1712 (дата звернення: 02.10.2026).

93. International Organization for Migration. *Ukraine Crisis Response Plan 2025*. 2025. URL: https://crisisresponse.iom.int/response/ukraine-crisis-response-plan-2025 (дата звернення: 02.10.2026).

94. International Organization for Migration. *Ukraine and Neighbouring Countries Crisis Response Plan 2025*. 2025. URL: https://crisisresponse.iom.int/response/ukraine-and-neighbouring-countries-crisis-response-plan-2025 (дата звернення: 02.10.2026).

95. Commission on Crime Prevention and Criminal Justice. *Resolution 33/1. Countering trafficking in persons in the context of rapid technological change*. 2024. URL: https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2020-2029/2024/2024_Res_33_1_CCPCJ.pdf (дата звернення: 02.10.2026).

96. U.S. Department of State. *Survivor Engagement: Promising Practices for Governments*. Office to Monitor and Combat Trafficking in Persons. 4 November 2024. URL: https://2021-2025.state.gov/survivor-engagement-promising-practices-for-governments/ (дата звернення: 02.10.2026).

97. Про затвердження Державної цільової соціальної програми протидії торгівлі людьми на період до 2030 року : розпорядження Кабінету Міністрів України від 03.09.2026 № 875-р.

98. Про інформацію : Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 02.10.2026).

99. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 02.10.2026).

100. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 02.10.2026).

101. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text (дата звернення: 02.10.2026).

102. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 02.10.2026).

103. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 02.10.2026).

104. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури : розпорядження Кабінету Міністрів України від 19.09.2023 № 825-р. URL: https://zakon.rada.gov.ua/laws/show/825-2023-%D1%80#Text (дата звернення: 02.10.2026).

105. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 02.10.2026).

106. Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 02.10.2026).

107. Ланде Д. В., Субач І. Ю., Бояринова Ю. Є. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2018. 300 с.

108. Олещенко Л. М. Машинне навчання. Комп’ютерний практикум: навч.-метод. посіб. Київ: КПІ ім. Ігоря Сікорського, 2022. 92 с.

109. Гавриленко О. В. Навчальний посібник з дисциплін «Аналіз даних» та «Аналіз даних в управляючих системах». Київ: КПІ ім. Ігоря Сікорського, 2020. 85 с.

110. Шаповалова О. О. Інтелектуальний аналіз даних з практикумом в Deductor: навч.-метод. посіб. Харків: ХНУБА, 2020. 160 с.

111. Юсин Я. О. Програмне забезпечення інформаційно-пошукових систем. Методи організації пошуку інформації. Збірник задач та вправ: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2026. 83 с.

112. Юсин Я. О. Програмне забезпечення інформаційно-пошукових систем. Методи організації пошуку інформації. Лабораторний практикум: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2026. 95 с.

113. Стець О. В., Стець С. Ю. Вебскрейпінг та аналіз даних соціальних мереж: конспект лекцій. Київ: КПІ ім. Ігоря Сікорського, 2026. 83 с.

114. Про Національну програму інформатизації : Закон України від 01.12.2022 № 2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 02.10.2026).

115. Гурін А. Л., Тихоход В. О., Крячок О. С. Геоінформаційні системи в енергетиці: лабораторні роботи в ArcGIS 10.8: навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2024. 129 с.

116. Притискач І. В. Геоінформаційні системи в електроенергетиці. Київ: КПІ ім. Ігоря Сікорського, 2026. 125 с.

117. Організація з безпеки та співробітництва в Європі. Протидія торгівлі людьми: посіб. для дільничних інспекторів міліції. Київ: ОБСЄ, 2012. 40 с.

118. Організація з безпеки та співробітництва в Європі. Навчальний посібник у сфері протидії торгівлі людьми для суддів та прокурорів. Ознайомчі матеріали для держав-членів ЄС, асоційованих членів і держав-кандидатів на вступ. Київ: ОБСЄ, 2011. 217 с.: URL: osce.org (дата звернення: 02.10.2026).

119. Lyle J. R., Guttman B., Butler J. M., Sauerwein K., Reed C., Lloyd C. E. Digital Investigation Techniques: A NIST Scientific Foundation Review. Gaithersburg, MD : National Institute of Standards and Technology, 2022. 84 p.

120. Kent K., Chevalier S., Grance T., Dang H. Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD : National Institute of Standards and Technology, 2006. 121 p.

121. Digital Evidence Preservation: Considerations for Evidence Handlers. Gaithersburg, MD : National Institute of Standards and Technology, 2022. (NIST Interagency/Internal Report 8387). DOI: https://doi.org/10.6028/NIST.IR.8387.