Міністерство внутрішніх справ України
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Навчальний посібник

Колектив авторів

Дніпро
2024

УДК 004.056.5+531.74
І-74

Рекомендовано до друку Науково-методичною радою Дніпровського державного університету внутрішніх справ (протокол № 11 від 22.05.2024)

РЕЦЕНЗЕНТИ:
Дмитро Данченко – капітан поліції, начальник 7-го відділу управління протидії кіберзлочинам в Дніпропетровській області Департаменту кіберполіції Національної поліції України;
кандидат юридичних наук **Ігор Федчак** –доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів Львівського державного університету внутрішніх справ;
доктор юридичних наук, професор **Ігор Пиріг** – професор кафедри криміналістики та домедичної підготовки Дніпровського державного університету внутрішніх справ.

І-74 Інформаційно-аналітичне забезпечення правоохоронної діяльності: навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 181 с.

ISBN 978-617-560-035-1

Навчальний посібник призначений для вивчення дисципліни "Інформаційно-аналітичне забезпечення правоохоронної діяльності". У ньому розглянуті основні загрози інформаційній безпеці, які виникають в сучасному суспільстві та на виробництвах, висвітлені питання протидії комп'ютерним вірусам та захист інформації у комп'ютерних мережах. Особливу увагу приділено системі управління інформаційною безпекою, в тому числі її нормативно-правовим забезпеченням. Після кожної теми передбачені контрольні запитання. Надається загальний перелік використаних джерел.

Розрахований на здобувачів вищої освіти.

АВТОРИ

Едуард Рижков – професор кафедри економічної та інформаційної безпеки Дніпровського державного університету внутрішніх справ, кандидат юридичних наук, професор; **Юлія Синиціна** – доцент кафедри економічної та інформаційної безпеки Дніпровського державного університету внутрішніх справ, кандидат технічних наук, доцент; **Сергій Прокопов** – старший викладач кафедри економічної та інформаційної безпеки Дніпровського державного університету внутрішніх справ; **Андрій Гребенюк** – завідувач кафедри економічної та інформаційної безпеки Дніпровського державного університету внутрішніх справ, кандидат технічних наук, доцент; **Людмила Рибальченко –** доцент кафедри економічної та інформаційної безпеки Дніпровського державного університету внутрішніх справ, кандидат економічних наук, доцент.

ISBN 978-617-560-035-1

ЗМІСТ

ВСТУП

Інформаційно-аналітичне забезпечення правоохоронної діяльності є одним із базисів, що лежить в основі якісного виконання правоохоронцями своїх функцій із захисту суспільства. Стрімкий розвиток інформаційних технологій призвів до накопичення та зберігання значних обсягів інформації. Створення зручного та багатофункціонального програмного забезпечення для введення, зберігання та пошуку необхідної інформації має велике значення для поліцейських організацій. Відповідно до статей 25, 26 та 27 Закону України "Про Національну поліцію" та пункту 40 статті 4 Положення про Національну поліцію, затвердженого постановою Кабінету Міністрів України № 877 від 28 жовтня 2015 року, з метою організації інформаційно-аналітичного забезпечення поліції Міністерство внутрішніх справ України видало наказ № 676 від 03 серпня 2017 року "Про затвердження Положення про інформаційно-комунікаційну систему "Інформаційний портал Національної поліції".

Система "Інформаційний портал Національної поліції України" є складовою частиною Єдиної інформаційної системи Міністерства внутрішніх справ (далі – ЄІС МВС). Найбільш поширеною та універсальною є інтегрована інформаційно-пошукова система Національної поліції. Найбільш успішним і перспективним є інформаційно-технологічний комплекс "Цунамі", який забезпечує організаційну та інформаційну підтримку реагування підрозділів поліції на інциденти.

Одним із результатів роботи цього комплексу є електронна картка реагування на подію. Ця картка покращує якість збору та фіксації первинної інформації на місці події та унеможливлює маніпулювання первинною інформацією з боку корумпованих чиновників. Не менш важливим для правоохоронних органів є комунікаційний доступ до інформаційних баз даних. Він має бути зручним та швидким.

Центральні та місцеві підрозділи Національної поліції України відіграють провідну роль у створенні, впровадженні та використанні інформаційних систем – як міжвідомчих, так і внутрішньовідомчих. Це вимагає від персоналу володіння відповідними знаннями та навичками у сфері новітніх інформаційних технологій.

Удосконалення діяльності Національної поліції України наразі неможливе без забезпечення доступу всіх підрозділів правоохоронних органів до єдиної автоматизованої бази даних облікової, оперативно-

розшукової, слідчої, криміналістичної та іншої інформації, а також забезпечення диференційованого доступу до цієї інформації.

Працівники Національної поліції, які мають своєчасний доступ до необхідної достовірної та вичерпної інформації, можуть цілком достеменно аналізувати ситуацію та приймати відповідні рішення щодо виконання своїх обов'язків, що значно підвищить ефективність їхньої діяльності.

Посібник складається з шести розділів. У розділі 1 викладено основні правові документи, які регламентують організації розвідувального забезпечення діяльності Національної поліції України ([1]). В інших розділах розглядається та детально описуються автоматизовані інформаційні системи, що використовуються в діяльності Національної поліції. Розділ 1 (Ю. Синиціна), Розділи 2, 3, 4.1, 4.2 (Л. Рибальченко), (С. Прокопов), Розділ 6 (Е. Рижков), Розділ 7 (С. Прокопов), Розділи 2.2, 2.6 і 3.2 (А. Гребенюк), (Л. Рибальченко), (Ю. Синиціна).

Спеціальність "Інформаційно-аналітичне забезпечення правоохоронної діяльності" викладається в Дніпровському державному університеті внутрішніх справ.

Розділ 1
ПРАВОВЕ РЕГУЛЮВАННЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Актуальність теми полягає в тому, що сучасні технології і високий рівень цифровізації суспільства створюють нові виклики і можливості для правоохоронних органів. Національна поліція веде інформаційно-аналітичну діяльність, спрямовану на забезпечення громадської безпеки, запобігання злочинності, розкриття злочинів та забезпечення правового порядку. Задля ефективного функціонування цієї діяльності потрібне відповідне правове регулювання, що забезпечує законність, прозорість та захист прав громадян.

1.1. Загальні принципи та методи інформаційно-аналітичної діяльності Національної поліції України

Інформаційно-аналітична діяльність Національної поліції України є основною складовою її роботи. Вона охоплює збір, обробку, аналіз та використання різноманітної інформації для забезпечення громадського порядку, протидії злочинності та забезпечення безпеки громадян. Завдяки інформаційно-аналітичній діяльності поліція може ефективно прогнозувати та запобігати злочинам, розкривати злочини швидше та ефективніше, а також сприяти здійсненню кримінального переслідування. Важливою складовою цієї діяльності є аналіз отриманої інформації з використанням сучасних методів та технологій, що дозволяє отримати об'єктивну та достовірну картину ситуації. Правове регулювання цієї діяльності забезпечується деякими законодавчими актами, які встановлюють принципи, процедури та вимоги до збору, обробки та збереження інформації. Інформаційно-аналітична діяльність Національної поліції України є необхідною складовою для забезпечення правопорядку та безпеки у країні.

Основні принципи інформаційно-аналітичної діяльності Національної поліції України базуються на законності, об'єктивності та конфіденційності. Передусім ця діяльність здійснюється відповідно до вимог законодавства, що гарантує права та свободи громадян. Об'єктивність є важливим принципом, оскільки інформаційно-аналітична робота повинна ґрунтуватися на об'єктивних даних та фактах,

а не на особистих уподобаннях чи поглядах. Конфіденційність інформації є невід'ємною частиною цієї діяльності, оскільки дотримання конфіденційності забезпечує довіру громадськості та захищає права та інтереси громадян. Крім того, принципи професіоналізму та компетентності важливі для забезпечення якісної інформаційно-аналітичної роботи. Працівники Національної поліції повинні мати високий рівень професійної підготовки та володіти сучасними методами аналізу та обробки інформації. Інформаційно-аналітична діяльність також ґрунтується на принципі системності та комплексності, оскільки для ефективного вирішення завдань необхідно аналізувати інформацію з різних джерел та враховувати різні аспекти ситуації. Дотримання цих принципів дозволяє Національній поліції України забезпечувати ефективну та об'єктивну роботу в галузі інформаційно-аналітичної діяльності.

Основні методи інформаційно-аналітичної діяльності Національної поліції України розроблені з урахуванням сучасних технологій та методів аналізу інформації. Першочергово це включає збір та обробку різноманітної інформації, яка надходить з різних джерел, таких як свідчення очевидців, оперативні дані, статистика злочинності тощо. Крім того, аналітики поліції використовують різні аналітичні методи та інструменти, щоб виявити закономірності та тенденції в злочинності, наприклад, методи аналізу даних, статистичні моделі, географічний аналіз тощо.

Ще одним важливим методом є проведення ризико-орієнтованого аналізу, коли аналітики визначають об'єкти або області з високим ризиком вчинення злочинів та розробляють стратегії їх запобігання. Також використовуються методи прогнозування, щоб передбачити можливі події та ризики, що виникають у сфері правопорядку.

Важливою складовою є інформаційно-аналітична робота в інтернеті та соціальних мережах, де аналітики відстежують та аналізують інформацію щодо можливих злочинів, організацій злочинного середовища, а також взаємодіють з громадськістю.

Зрештою важливою складовою є співпраця з іншими правоохоронними органами та міжнародними партнерами, адже обмін інформацією та досвідом дозволяє ефективніше боротися із злочинністю, особливо в умовах транскордонних злочинних мереж.

Ці методи інформаційно-аналітичної діяльності Національної поліції України допомагають забезпечити ефективність та об'єктивність її діяльності в боротьбі зі злочинністю та забезпечити безпеку громадян.

1.2. Алгоритм правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Алгоритм правового регулювання інформаційно-аналітичної діяльності Національної поліції України включає декілька ключових етапів, що детально регламентуються відповідними законодавчими актами та нормативно-правовими документами.

Першим етапом є визначення завдань та цілей інформаційно-аналітичної діяльності поліції відповідно до законодавства. На цьому етапі визначається обсяг і характер інформації, яку необхідно збирати, аналізувати та зберігати для забезпечення безпеки громадян та правопорядку.

Другим етапом є встановлення правил збору, обробки та зберігання інформації. Це, насамперед, визначення процедур збирання даних, використання спеціалізованих програмних засобів для аналізу даних, а також встановлення термінів зберігання інформації.

Третім етапом є розробка і впровадження внутрішніх нормативно-правових актів, які регулюють проведення інформаційно-аналітичної діяльності. Ці документи встановлюють конкретні правила та процедури роботи поліції у цій сфері та забезпечують відповідність її діяльності вимогам законодавства.

Четвертим етапом є надання правового захисту особистих даних громадян. Згідно зі статтею 32 Конституції України, кожен громадянин має право на захист своїх персональних даних, тому важливо встановлювати механізми захисту цих даних під час проведення інформаційно-аналітичної роботи [1, 2].

Стаття 32. Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.

Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.

Кожному гарантується судовий захист права спростовувати

недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації [1, 2].

Тож алгоритм правового регулювання інформаційно-аналітичної діяльності Національної поліції України включає в себе визначення цілей та завдань діяльності, встановлення правил збору та обробки інформації, розробку внутрішніх нормативно-правових актів та захист особистих даних громадян (рис 1.1).

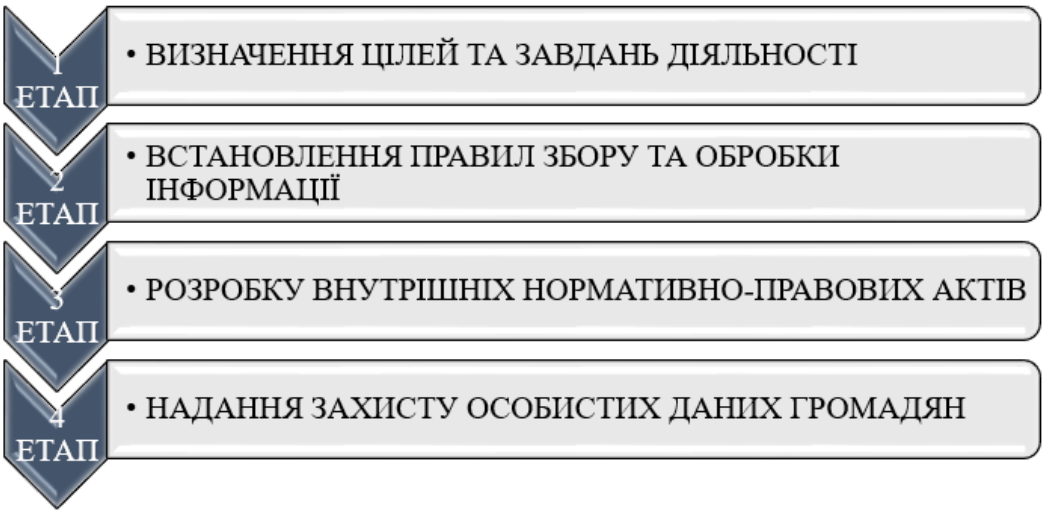


Рис. 1.1. Алгоритм правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Цей алгоритм допомагає забезпечити ефективне та законне виконання поліцейських функцій у сфері інформаційно-аналітичної діяльності.

1.3. Сучасні схеми та основні механізми правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Основні механізми правового регулювання інформаційно-аналітичної діяльності Національної поліції України визначаються рядом законодавчих актів та нормативно-правових документів, які встановлюють правила та процедури роботи поліції в цій сфері.

По-перше, це Закон України «Про поліцію», який визначає завдання, повноваження та принципи функціонування Національної

поліції.

Він встановлює правила збору, обробки та зберігання інформації, а також процедури ведення аналітичної роботи з метою забезпечення правопорядку та безпеки громадян.

Крім того, важливим механізмом є постанови Кабінету Міністрів України, які регулюють питання організації інформаційно-аналітичної діяльності Національної поліції, встановлюють порядок взаємодії з іншими органами влади та обміну інформацією.

Також велике значення мають нормативні документи, які видає Національна поліція, зокрема накази та інструкції, що встановлюють конкретні правила проведення інформаційно-аналітичної роботи, внутрішні процедури та стандарти.

Крім того, правове регулювання інформаційно-аналітичної діяльності Національної поліції України відповідає міжнародним стандартам та угодам, що визначають правила обробки та захисту персональних даних громадян.

Сучасні схеми правового регулювання інформаційно-аналітичної діяльності Національної поліції України базуються на комплексному підході до забезпечення правопорядку та безпеки громадян (рис. 1.2).

Основними документами, що визначають ці схеми, є законодавчі акти, нормативно-правові документи та міжнародні стандарти.

По-перше, Закон України «Про Національну поліцію» встановлює загальні принципи та завдання поліції, а також визначає основні правила збору, обробки та зберігання інформації. Цей закон встановлює основи функціонування інформаційно-аналітичної діяльності поліції та визначає права та обов'язки поліцейських у цій сфері.

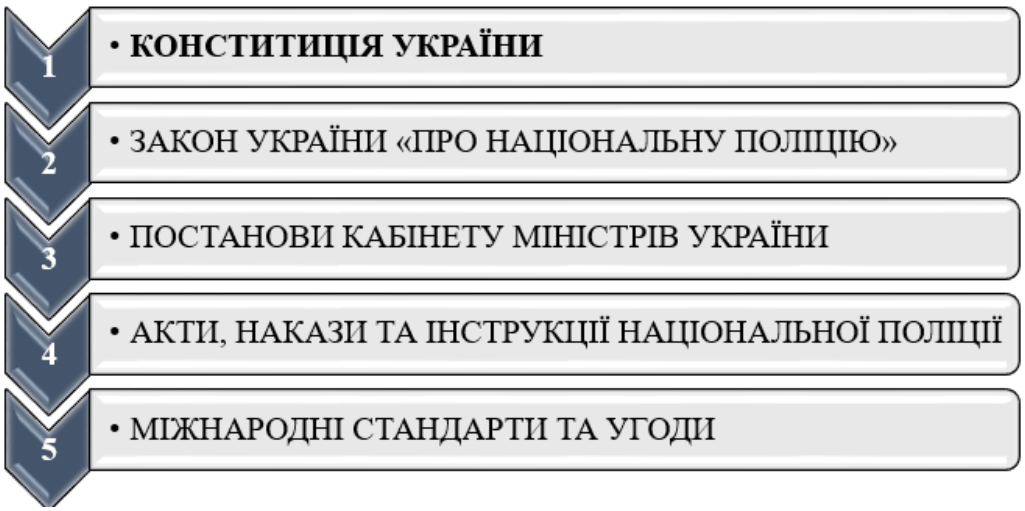


Рис. 1.2. Комплексний підхід правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Додатково, роль у правовому регулюванні відіграють постанови Кабінету Міністрів України, які встановлюють конкретні правила і процедури ведення інформаційно-аналітичної роботи. Ці документи визначають порядок організації діяльності поліції, взаємодії з іншими відомствами та обміну інформацією.

Значну роль у сучасних схемах правового регулювання відіграють також внутрішні нормативно-правові акти Національної поліції, зокрема накази та інструкції, які встановлюють конкретні вимоги та стандарти ведення інформаційно-аналітичної роботи.

Крім того, сучасні схеми правового регулювання враховують міжнародні стандарти та угоди, які визначають правила обробки та захисту персональних даних громадян. Це дозволяє уникнути порушень прав людини та забезпечує відповідність діяльності поліції міжнародним нормам.

Усі ці елементи утворюють систему сучасних схем правового регулювання інформаційно-аналітичної діяльності Національної поліції України, яка сприяє забезпеченню ефективного функціонування правоохоронних органів та забезпеченню безпеки громадян.

Загалом механізми правового регулювання інформаційно-аналітичної діяльності Національної поліції України забезпечують здійснення цієї діяльності в рамках закону та з урахуванням вимог до захисту прав та свобод громадян.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України базується на кількох ключових нормативних актах. Основними з них є:

Конституція України. Вона визначає загальні принципи правозахисту, включаючи право на інформацію та правові гарантії щодо її надходження та обробки.

Закони про поліцію та правоохоронну діяльність. Закони, зокрема «Про Національну поліцію», та інші відповідні нормативно-правові акти визначають правові засади функціонування та компетенцію Національної поліції, включаючи її право на здійснення інформаційно-аналітичної діяльності з метою забезпечення громадського порядку і безпеки.

Постанови Кабінету Міністрів України та накази Міністерства внутрішніх справ. Ці нормативно-правові акти можуть містити деталізовані вказівки та процедури щодо здійснення інформаційно-аналітичної роботи в Національній поліції.

Міжнародні конвенції та угоди. Україна, як держава-учасниця різних міжнародних організацій, може також дотримуватися

міжнародних стандартів та зобов'язань щодо інформаційно-аналітичної діяльності правоохоронних органів.

Ці нормативні акти забезпечують правову базу для здійснення інформаційно-аналітичної діяльності Національної поліції, а також встановлюють механізми контролю та забезпечення дотримання прав та свобод громадян у процесі збору, обробки та використання інформації.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України ґрунтується на Конституції України. Згідно зі статтею 3 Основного Закону, Україна є правовою, демократичною та соціальною державою, яка забезпечує права та свободи громадян. Стаття 34 гарантує право на інформацію, але це право може бути обмежене в інтересах національної безпеки, охорони прав та свобод людини. Щодо правового регулювання діяльності органів влади стаття 19 Конституції України визначає, що органи державної влади, включаючи поліцію, здійснюють свою діяльність в межах, ***що передбачені Конституцією та законами України***. Таким чином, інформаційно-аналітична робота поліції повинна ґрунтуватися на чіткій правовій базі, що визначена законодавством України.

Стаття 3. Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. *Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави [1, 2].*

Стаття 34. Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань.

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, *територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [1, 2].*

Стаття 19. Правовий порядок в Україні ґрунтується на засадах, відповідно до яких ніхто не може бути примушений робити те, що не передбачено законодавством.

Органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України *[1, 2].*

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України базується на ряді законів, зокрема «Про Національну поліцію» та інших нормативно-правових актах про правоохоронну діяльність. Згідно зі статтею 25 Закону «Про Національну поліцію» поліція здійснює інформаційно-аналітичну діяльність для запобігання та виявлення злочинів, забезпечення громадського порядку тощо [3]. Стаття 18 цього Закону встановлює правові гарантії збереження конфіденційності отриманої інформації та обмеження доступу до неї [3]. Також інформаційно-аналітична діяльність поліції повинна ґрунтуватися на принципах законності, об'єктивності та недопущення порушення прав та свобод громадян, що визначені відповідно до законодавства України про правоохоронну діяльність.

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення.

1. Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених цим Законом.

2. Поліція в рамках інформаційно-аналітичної діяльності:

1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

3. Поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

4. Діяльність поліції, пов’язана із захистом і обробкою персональних

даних, здійснюється на підставах, визначених Конституцією України, Законом України "Про захист персональних даних", іншими законами України.

5. Поліція зобов'язана письмово інформувати органи доходів і зборів про виявлення нецільового використання та/або передачі транспортних засобів особистого користування, тимчасово ввезених на митну територію України чи поміщених у митний режим транзиту, у володіння, користування або розпорядження особам, які не ввозили такі транспортні засоби на митну територію України або не поміщували в митний режим транзиту, а також про виявлення розкомплектування таких транспортних засобів [3].

Стаття 18. Основні обов'язки поліцейського.

1. Поліцейський зобов'язаний:

1) неухильно дотримуватися положень Конституції України, законів України та інших нормативно-правових актів, що регламентують діяльність поліції, та Присяги поліцейського;

2) професійно виконувати свої службові обов'язки відповідно до вимог нормативно-правових актів, посадових (функціональних) обов'язків, наказів керівництва;

3) поважати і не порушувати прав і свобод людини;

4) надавати невідкладну, зокрема домедичну і медичну, допомогу особам, які постраждали внаслідок правопорушень, нещасних випадків, а також особам, які опинилися в безпорадному стані або стані, небезпечному для їхнього життя чи здоров'я;

5) зберігати інформацію з обмеженим доступом, яка стала йому відома у зв'язку з виконанням службових обов'язків;

6) інформувати безпосереднього керівника про обставини, що унеможливлюють його подальшу службу в поліції або перебування на займаній посаді.

2. Поліцейський на всій території України незалежно від посади, яку він займає, місцезнаходження і часу доби в разі звернення до нього будь-якої особи із заявою чи повідомленням про події, що загрожують особистій чи публічній безпеці, або в разі безпосереднього виявлення таких подій зобов'язаний вжити необхідних заходів з метою рятування людей, надання допомоги особам, які її потребують, і повідомити про це найближчий орган поліції.

3. Звертаючись до особи, або у разі звернення особи до поліцейського, поліцейський зобов'язаний назвати своє прізвище, посаду, спеціальне звання та пред'явити на її вимогу службове посвідчення,

надавши можливість ознайомитися з викладеною в ньому інформацією, не випускаючи його з рук.

4. Додаткові обов'язки, пов'язані з проходженням поліцейським служби в поліції, можуть бути покладені на нього виключно законом [3].

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України визначається рішеннями Кабінету Міністрів України, в яких встановлюються правила та процедури збору, обробки та використання інформації. Зокрема, постанова Кабінету Міністрів України від 14 листопада 2018 року № 591 «Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб'єктів» встановлює основні функції та завдання інформаційно-аналітичної роботи поліції [4]. Згідно зі статтею 6 цієї постанови єдина інформаційна система МВС призначена для автоматизації та технологічного забезпечення обміну даними між суб'єктами єдиної інформаційної системи МВС, зокрема в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави. Крім того, відповідно до статті 3, інформаційно-аналітичні дані мають бути конфіденційними, а доступ до них обмежується відповідно до закону [4]. Таким чином, постанови Кабінету Міністрів України встановлюють правові основи для проведення інформаційно-аналітичної діяльності Національної поліції та гарантують дотримання принципів законності та конфіденційності.

Стаття 6. Єдина інформаційна система МВС призначена для автоматизації та технологічного забезпечення обміну даними між суб'єктами єдиної інформаційної системи МВС, зокрема в інтересах національної безпеки, захисту прав та законних інтересів громадян, суспільства і держави у сферах:

- ***забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку;***
- *захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні;*
- *цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації наслідків надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної та техногенної безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;*

- *міграції (імміграції та еміграції), зокрема протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів [4].*

Стаття 3. Власником і розпорядником єдиної інформаційної системи МВС є держава в особі МВС.

Володільцем інформації, що обробляється в центральній підсистемі єдиної інформаційної системи МВС, є МВС.

Володільцями інформації, що обробляється у функціональних підсистемах єдиної інформаційної системи МВС, є відповідні суб'єкти єдиної інформаційної системи МВС, які забезпечують захист інформації від випадкової втрати або знищення, незаконної обробки та незаконного доступу до інформації.

Мета обробки інформації у функціональних підсистемах єдиної інформаційної системи МВС установлюється нормативно-правовими актами, які регулюють діяльність відповідних суб'єктів єдиної інформаційної системи МВС, окремо для кожного визначеного електронного інформаційного ресурсу єдиної інформаційної системи МВС [4].

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України визначається наказами Міністерства внутрішніх справ. Згідно з «Положенням про єдину інформаційну систему Міністерства внутрішніх справ», затвердженим постановою Кабінету Міністрів України від 14 листопада 2018 р. № 1024 (в редакції постанови Кабінету Міністрів України від 15 серпня 2023 р. № 866), інформаційно-аналітична діяльність має на меті забезпечення громадського порядку та боротьбу зі злочинністю. Згідно зі статтею 8 цього Положення інформація, яка надходить в результаті аналізу, має бути достовірною та об'єктивною. До роботи з інформацією повинні бути допущені лише уповноважені працівники.

Стаття 8. Функціями єдиної інформаційної системи МВС є:

- *інтеграція електронних інформаційних ресурсів єдиної інформаційної системи МВС;*
- *обробка інформації, що формується у процесі діяльності суб'єктів єдиної інформаційної системи МВС, з використанням центральної підсистеми єдиної інформаційної системи МВС;*
- *перевірка своєчасності внесення,* ***достовірності та повноти інформації****, яка відповідно до законодавства обробляється суб'єктами єдиної інформаційної системи МВС;*

- систематизація та узагальнення інформації, перетворення її до формату, придатного для проведення подальшого аналізу та забезпечення роботи автоматизованих підсистем підтримки прийняття рішень, сигнальних та контрольних сервісів;

- автоматизація та верифікація процесів інформаційної діяльності суб'єктів єдиної інформаційної системи МВС в інтерактивному режимі реального часу;

- забезпечення електронного документообігу у випадках, передбачених законодавством, між суб'єктами єдиної інформаційної системи МВС з використанням центральної підсистеми єдиної інформаційної системи МВС;

- забезпечення електронної інформаційної взаємодії суб'єктів єдиної інформаційної системи МВС сервісами (засобами) центральної підсистеми єдиної інформаційної системи МВС та/або системи електронної взаємодії державних електронних інформаційних ресурсів "Трембіта";

- розмежування прав доступу та надання контрольованого доступу користувачам єдиної інформаційної системи МВС до функціональних підсистем та електронних інформаційних ресурсів суб'єктів єдиної інформаційної системи МВС;

- забезпечення резервного копіювання, зберігання та комплексного захисту інформації, що міститься в електронних інформаційних ресурсах єдиної інформаційної системи МВС.

Також згідно з ІІ розділом «Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України», затвердженим наказом Національної поліції України від 31.01.2020 року № 77 (зі змінами 13.11.2020 № 885), Департамент інформаційно-аналітичної підтримки (ДІАП) є структурним підрозділом центрального органу управління поліції. Його завданням є організація та координація діяльності у сферах цифрової інфраструктури, цифрової трансформації процесів службової діяльності, інформаційно-аналітичної роботи та забезпечення зв'язку між структурними підрозділами поліції, встановлення конкретних процедур та вимог до проведення інформаційно-аналітичної роботи. Таким чином, накази МВС України встановлюють правові основи для інформаційно-аналітичної діяльності Національної поліції та забезпечують дотримання принципів законності, об'єктивності та конфіденційності [5].

Розділ ІІ. *Завдання ДІАП:*

1. Організовує та бере участь у забезпеченні реалізації в Національній поліції України державної політики у сфері цифрової інфраструктури та цифрової трансформації в частині заходів з охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання публічної безпеки і порядку, а також надання поліцейських послуг.

2. Здійснює інформаційно-аналітичну та інформаційно-пошукову діяльність поліції, забезпечує інтероперабельність при формуванні електронних інформаційних ресурсів, що утворюються в процесі службової діяльності поліції, функціонуванні та розвитку інформаційних технологій, систем зв'язку та телекомунікаційних мереж.

3. Забезпечує розроблення, упровадження та функціонування:

- центрального та резервного (резервних) програмно-технічних комплексів;

- інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (далі – системи ІПНП);

- програмно-технічних засобів взаємодії системи ІПНП функціональної підсистеми з центральною та іншими підсистемами Єдиної інформаційної системи Міністерства внутрішніх справ України (далі – ЄІС МВС), іншими інформаційно-телекомунікаційними системами;

- відомчого сегменту телекомунікаційних мереж та засобів доступу до Інтернету;

- електронної пошти органів (підрозділів) поліції;

- корпоративного файлового хостингу;

- програмних засобів для корпоративного обміну миттєвими повідомленнями (корпоративний чат);

- систем дистанційного навчання;

- програмно-технічного комплексу офіційного вебпорталу Національної поліції України;

- засобів телефонного, радіо- та супутникового зв'язку;

- систем відеоспостереження, відеоаналітики, архівування відео- та аудіоінформації;

- систем аудіовізуального супроводження спеціальних заходів;

- засобів селекторного та відеоконференцзв'язку для забезпечення проведення нарад керівництва Національної поліції України;

- систем оповіщення;

- систем контролю за місцезнаходженням осіб, які в установленому

законом порядку зобов'язані носити електронні засоби контролю;

- систем організації прийому повідомлень за скороченим номером екстреного виклику поліції «102».

- системи моніторингу рухомих об'єктів Національної поліції України з геоінформаційною прив'язкою;

- систем забезпечення функціонування Call-центру та управління забезпечення діяльності Ситуаційного центру Департаменту організаційно-аналітичного забезпечення та оперативного реагування Національної поліції України;

- систем антивірусного захисту.

1.4. Міжнародні основи правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Міжнародні документи є важливою частиною правової бази для інформаційно-аналітичної діяльності Національної поліції, оскільки вони встановлюють міжнародні стандарти та принципи, які мають бути дотримані у діяльності правоохоронних органів. Правове регулювання інформаційно-аналітичної діяльності Національної поліції України базується на міжнародних конвенціях. Зокрема, Конвенція про права людини та основні свободи, прийнята Радою Європи (дата підписання: 04.11.1950; дата ратифікації Україною: 17.07.1997; дата набрання чинності для України: 11.09.1997), надає гарантії щодо права на особисту та конфіденційну інформацію, а також стаття 8 Конвенції про права людини та основні свободи гарантує право на повагу до приватного та сімейного життя, що може включати конфіденційність інформації [6].

Стаття 1. Конвенція про захист прав людини і основоположних свобод

Зобов'язання поважати права людини.

Високі Договірні Сторони гарантують кожному, хто перебуває під їхньою юрисдикцією, права і свободи, визначені в розділі I цієї Конвенції.

Розділ I

Стаття 8. Право на повагу до приватного і сімейного життя

1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції.

2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно

із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб.

Стаття 10. Свобода вираження поглядів

1. Кожен має право на свободу вираження поглядів. ***Це право гарантує дотримання своїх поглядів, одержання і передавання інформації та ідеї без втручання органів державної влади і незалежно від кордонів****. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.*

2. Здійснення цих свобод, оскільки воно пов'язане з обов'язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законодавством і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України має міжнародні основи через ратифікацію ряду міжнародних угод. Зокрема, Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності визначає принципи обміну інформацією між державами-учасницями (ст. 43), сприяючи таким чином інформаційній співпраці між правоохоронними органами. Конвенція ООН проти корупції (ст. 46) зобов'язує держави-учасниці забезпечувати конфіденційність інформації, яка міститься в актах з протидії корупції. Крім того, Конвенція про боротьбу з корупцією, прийнята ООН, встановлює міжнародні стандарти щодо запобігання корупції та викриття злочинів. Такі конвенції, як Конвенція про боротьбу з тероризмом та Конвенція про організовану злочинність також містять положення щодо обміну інформацією та співпраці між правоохоронними органами різних країн. Конвенція ООН проти корупції (ст. 13) зобов'язує учасників забезпечувати конфіденційність інформації, що міститься в актах з протидії корупції. Крім цього, Конвенція ООН проти транснаціональної організованої злочинності (ст. 43) визначає обмін інформацією та співпрацю між державами-учасницями. Ці міжнародні стандарти відображаються у національному законодавстві, забезпечуючи дотримання прав людини, конфіденційності та

міжнародної співпраці у сфері правоохоронної діяльності [7].

Глава II Заходи щодо запобігання корупції

Стаття 13. Участь суспільства

1. *Кожна держава-учасниця вживає належних заходів у межах своїх можливостей і згідно з основоположними принципами свого внутрішнього права для сприяння активній участі окремих осіб і груп за межами державного сектора, таких як громадянське суспільство, неурядові організації та організації, що функціонують на базі громад, у запобіганні корупції й боротьбі з нею та для поглиблення розуміння суспільством факту існування, причин і небезпечного характеру корупції, а також загроз, що створюються нею. Цю участь слід зміцнювати за допомогою таких заходів, як: повага, заохочення та захист свободи пошуку, отримання, опублікування та поширення інформації про корупцію.*

Глава III Криміналізація та правоохоронна діяльність

Стаття 33. Захист осіб, які повідомляють інформацію

Кожна держава-учасниця розглядає можливість включення до своєї внутрішньої правової системи належних заходів для забезпечення захисту будь-яких осіб, які добросовісно й на обґрунтованих підставах повідомляють компетентним органам про будь-які факти, пов'язані зі злочинами, передбаченими цією Конвенцією, від будь-якого несправедливого поводження.

Стаття 37. Співробітництво з правоохоронними органами

1. Кожна держава-учасниця вживає відповідних заходів для заохочення осіб, які беруть чи брали участь у вчиненні будь-якого злочину, визначеного цією Конвенцією, до надання інформації, корисної для компетентних органів з метою розслідування й доказування, а також до надання фактичної конкретної допомоги компетентним органам, яка може сприяти позбавленню злочинців доходів, здобутих злочинним шляхом, і вжиттю заходів для повернення таких доходів.

4. Захист таких осіб, mutatis mutandis, здійснюється в порядку, передбаченому статтею 32 цієї Конвенції.

Стаття 38. Співробітництво між національними органами

Кожна держава-учасниця вживає таких заходів, які можуть бути необхідними для заохочення, відповідно до її внутрішнього права, співробітництва між, з одного боку, її державними органами, а також державними посадовими особами та, з іншого боку, своїми органами, відповідальними за розслідування та переслідування у зв'язку з кримінальними злочинами. Таке співробітництво може включати:

а) надання таким відповідальним органам з власної ініціативи

інформації, якщо є обґрунтовані підстави вважати, що був вчинений будь-який зі злочинів, визначених статтями 15, 21 та 23 цієї Конвенції;

b) надання таким відповідальним органам на відповідний запит усієї необхідної інформації.

Стаття 39. Співробітництво між національними органами та приватним сектором

1. Кожна держава-учасниця вживає таких заходів, які можуть бути необхідними для заохочення, відповідно до її внутрішнього права, співробітництва між національними слідчими органами й органами прокуратури та організаціями приватного сектора, зокрема фінансовими установами, з питань вчинення злочинів, визначених цією Конвенцією.

2. Кожна держава-учасниця розглядає питання про те, щоб заохочувати своїх громадян та інших осіб, які зазвичай проживають на її території, повідомляти національним слідчим органам й органам прокуратури про вчинення будь-якого злочину, визначеного цією Конвенцією.

Глава IV Міжнародне співробітництво

Стаття 43. Міжнародне співробітництво

1. Держави-учасниці співпрацюють в кримінально-правових питаннях відповідно до статей 44 - 50 цієї Конвенції. Коли це доцільно й відповідає їхній внутрішній правовій системі, держави-учасниці розглядають можливість надання одна одній сприяння в розслідуванні та провадженні з цивільно-правових та адміністративних питань, пов'язаних з корупцією.

Стаття 46. Взаємна правова допомога

1. Держави-учасниці надають одна одній найширшу взаємну правову допомогу в розслідуванні, кримінальному переслідуванні та судовому розгляді справ за злочинами, визначеними цією Конвенцією:

e) надання інформації, речових доказів та висновків експертів;

f) надання оригіналів або засвідчених копій відповідних документів та матеріалів, у тому числі урядових, банківських, фінансових, корпоративних або комерційних документів.

5. Передача інформації відповідно до частини 4 цієї статті здійснюється без шкоди для розслідування та кримінального провадження в державі, компетентні органи якої надають інформацію.

Компетентні органи, що одержують інформацію, виконують прохання про збереження конфіденційності цієї інформації, навіть тимчасово, або про обмеження щодо її використання. Це, однак, не перешкоджає державі-учасниці, що одержує інформацію, розкрити

під час провадження ту інформацію, яка виправдовує обвинуваченого. У такому випадку до розкриття інформації держава-учасниця, що одержує інформацію, повідомляє державі-учасниці, що надає інформацію, та, на прохання, проводить консультації з державою-учасницею, що надає інформацію. Якщо у виняткових випадках попереднє повідомлення неможливе, то держава-учасниця, що одержує інформацію, має невідкладно повідомити про таке розкриття державі-учасниці, що надає інформацію.

Стаття 48. Співробітництво між правоохоронними органами

1. Держави-учасниці тісно співпрацюють одна з одною, діючи відповідно до своїх внутрішніх правових та адміністративних систем, з метою підвищення ефективності правоохоронних заходів для боротьби зі злочинами, визначеними цією Конвенцією.

Держави-учасниці, зокрема, вживають ефективних заходів, спрямованих на:

а) зміцнення або, в разі необхідності, встановлення каналів зв'язку між їхніми компетентними органами, установами та службами для забезпечення безпечного і швидкого обміну інформацією про всі аспекти злочинів, що визначені цією Конвенцією, у тому числі, якщо заінтересовані держави-учасниці будуть вважати це за необхідне, зв'язки з іншими видами злочинної діяльності.

Стаття 50. Спеціальні методи розслідування

З метою ефективної боротьби з корупцією кожна держава-учасниця, тією мірою, якою це допускається основними принципами її правової системи, і за умов, встановлених її внутрішнім правом, вживає у межах своєї компетенції таких заходів, які можуть бути необхідними, щоб дозволити проведення її компетентними органами контролю над поставками й, у тих випадках, коли вона вважає це доречним, використання інших спеціальних методів розслідування, таких як електронне спостереження або інші форми спостереження, або таємні операції, на своїй території, а також визнання доказів, зібраних за допомогою таких методів, в суді.

Глава VI Технічна допомога й обмін інформацією

Стаття 60. Підготовка кадрів і технічна допомога

4. Держави-учасниці розглядають можливість сприяння одна одній у проведенні оцінок, вивчення та дослідження видів, причин, наслідків та збитків, завданих корупцією у своїх країнах, з метою розроблення, за участю компетентних органів і суспільства, стратегій і планів дій щодо боротьби з корупцією.

Стаття 61. Збирання та аналіз інформації про корупцію та обмін такою інформацією

1. Кожна держава-учасниця розглядає можливість проведення, консультуючись з експертами, аналізу тенденцій в галузі корупції на своїй території, а також умов, в яких здійснюються корупційні злочини.

2. Держави-учасниці з метою розроблення, наскільки це можливо, загальних визначень, стандартів і методологій розглядають можливість розширення статистичних даних, аналітичних знань щодо корупції та інформації, у тому числі про оптимальні види практики у справі запобігання корупції й боротьби з нею, та обміну ними через посередництво міжнародних і регіональних організацій.

3. Кожна держава-учасниця розглядає можливість здійснення контролю за своєю політикою і за практичними заходами боротьби з корупцією, а також проведення оцінки їхньої ефективності й дієвості.

Ці міжнародні угоди встановлюють стандарти та принципи, які Національна поліція України повинна дотримувати в своїй інформаційно-аналітичній роботі, сприяючи тим самим підвищенню рівня правозахисту та міжнародної співпраці в області правоохоронної діяльності.

1.5. Основні фактори актуальності, пріоритетності напрямів та перспективи розвитку правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Основні фактори актуальності правового регулювання інформаційно-аналітичної діяльності Національної поліції України: цифрові технології, прозорість та захист прав громадян, ефективність та результативність, інноваційний розвиток (рис. 1.3).

Тож дослідження та аналіз правового регулювання інформаційно-аналітичної діяльності Національної поліції є дуже актуальними у контексті забезпечення ефективної роботи правоохоронних органів у сучасному інформаційному суспільстві.

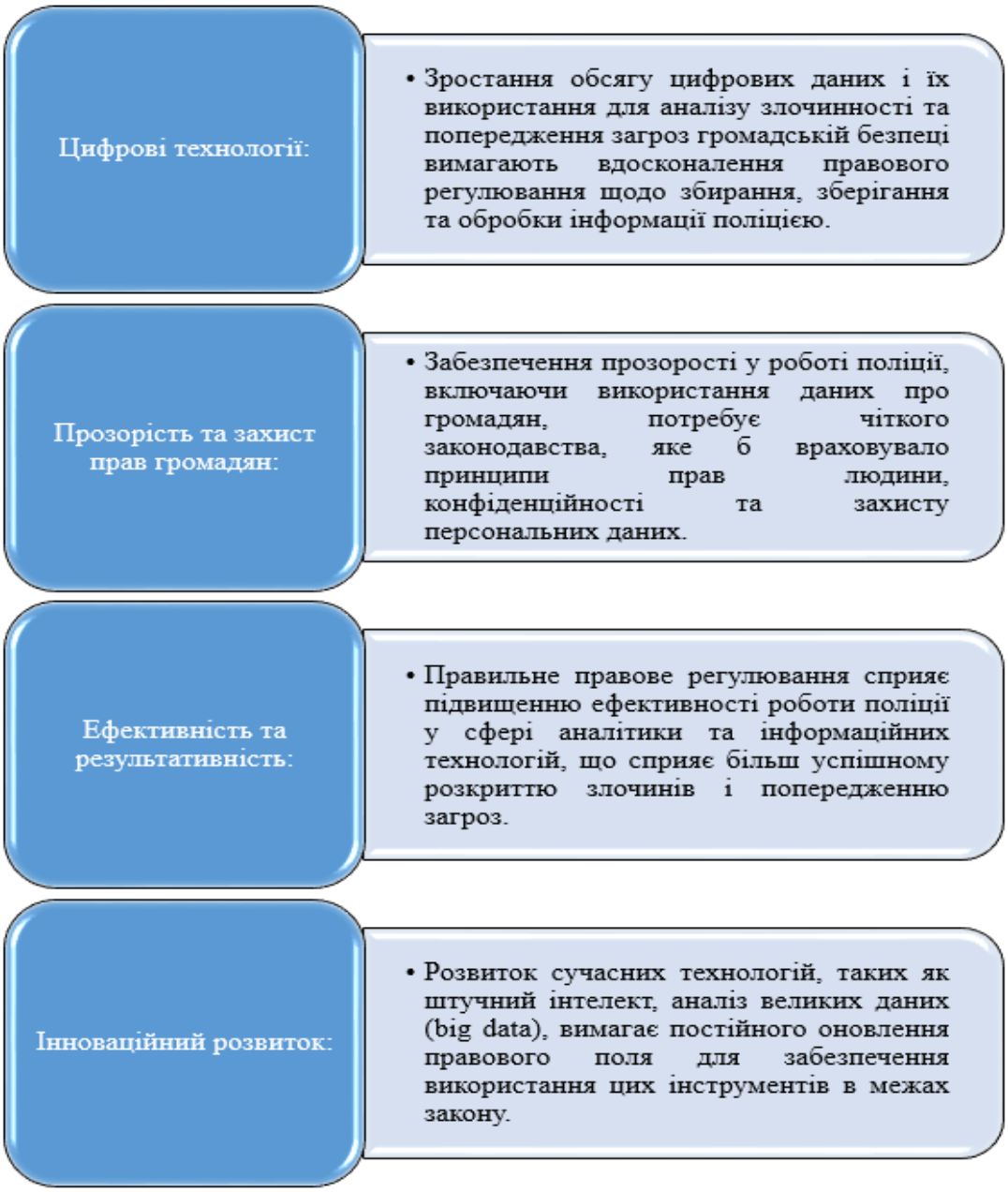


Рисунок 1.3. Основні фактори актуальності правового регулювання інформаційно-аналітичної діяльності Національної поліції України

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням цифрових технологій визначається рядом законодавчих актів, які враховують сучасні технологічні можливості та забезпечують захист прав громадян. Згідно зі статтею 27 Закону України «Про Національну поліцію» [3] поліція має право на отримання доступу до інформації в інформаційно-телекомунікаційних системах та мережах. Статті 25, 26 [3] цього Закону визначають право на збереження та обробку інформації про діяльність

поліції, зокрема, з використанням цифрових технологій. Застосування цифрових технологій в інформаційно-аналітичній діяльності Національної поліції відображається у використанні сучасних програмних засобів для збору, обробки та аналізу великих обсягів даних. Це дозволяє забезпечити швидкий та ефективний аналіз інформації, виявлення закономірностей та тенденцій у злочинності, а також прогнозування можливих кримінальних подій. Застосування цифрових технологій також допомагає у взаємодії з іншими правоохоронними органами та міжнародними партнерами через терміновий обмін інформацією. Це створює сприятливі умови для підвищення ефективності роботи поліції та забезпечення безпеки громадян.

Стаття 25. Повноваження поліції у сфері інформаційно-аналітичного забезпечення

1. Поліція здійснює інформаційно-аналітичну діяльність винятково для реалізації своїх повноважень, визначених законодавством.

2. Поліція в рамках інформаційно-аналітичної діяльності:

1) формує реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

2) користується реєстрами та базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями;

5) надає до Єдиного державного реєстру призовників, військовозобов'язаних та резервістів в електронній формі та в обсягах даних, зазначених у статтях 7, 14 Закону України "Про Єдиний державний реєстр призовників, військовозобов'язаних та резервістів", відомості, необхідні для забезпечення ведення військового обліку призовників, військовозобов'язаних та резервістів.

3. Поліція може створювати власні реєстри та бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до закону, та інформаційно-аналітичні системи (у тому числі міжвідомчі), необхідні для виконання покладених на неї повноважень.

4. Діяльність поліції, пов'язана із захистом і обробкою

персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України "Про захист персональних даних", іншими законами України.

5. Поліція зобов'язана письмово інформувати митні органи про виявлення нецільового використання та/або передачі транспортних засобів особистого користування, тимчасово ввезених на митну територію України чи поміщених у митний режим транзиту, у володіння, користування або розпорядження особам, які не ввозили такі транспортні засоби на митну територію України або не поміщували в митний режим транзиту, а також про виявлення розкомплектування таких транспортних засобів.

Стаття 26. Формування інформаційних ресурсів поліцією

1. Поліція засобами інформаційно-комунікаційної системи наповнює та підтримує в актуальному стані реєстри та бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України, стосовно:

1) осіб, щодо яких поліцейські здійснюють профілактичну роботу;

2) виявлених кримінальних та адміністративних правопорушень, осіб, які їх учинили, руху кримінальних проваджень; обвинувачених, обвинувальний акт щодо яких направлено до суду;

3) розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання або вироку суду, або від виконання обов'язків, визначених законом для суб'єктів пробації;

4) розшуку осіб, зниклих безвісти;

5) установлення особи невпізнаних трупів та людей, які не можуть надати про себе будь-яку інформацію у зв'язку з хворобою або неповнолітнім віком;

6) зареєстрованих в органах внутрішніх справ і поліції кримінальних або адміністративних правопорушень, подій, які загрожують особистій чи публічній безпеці, надзвичайних ситуацій;

7) осіб, стосовно яких поліцією застосовано адміністративне затримання, затримання в порядку, передбаченому Кримінальним процесуальним кодексом України, або інше законне затримання; осіб, підданих адміністративному арешту, домашньому арешту; осіб, яким повідомлено про підозру в учиненні кримінального правопорушення;

8) осіб, які скоїли адміністративні правопорушення, провадження у справах здійснюється поліцією або територіальними центрами комплектування та соціальної підтримки;

9) зареєстрованих корупційних кримінальних правопорушень, адміністративних правопорушень, пов'язаних з корупцією, а також осіб,

які їх учинили, та результатів розгляду цих правопорушень у судах;

10) іноземців та осіб без громадянства, затриманих поліцією за порушення визначених правил перебування в Україні;

11) викрадених номерних речей, цінностей та іншого майна, які мають характерні ознаки для ідентифікації, або речей, пов'язаних із учиненням правопорушень, відповідно до заяв громадян;

12) викрадених (втрачених) документів за зверненням громадян;

13) знайдених, вилучених предметів і речей, у тому числі заборонених або обмежених в обігу, а також документів з ознаками підробки, які мають індивідуальні (заводські) номери;

14) транспортних засобів, які розшукуються, у тому числі у зв'язку з безвісним зникненням особи, виявлених безхазяйних транспортних засобів, а також викрадених, втрачених номерних знаків;

15) виданих дозвільних документів у сфері безпеки дорожнього руху та дозволів на рух окремих категорій транспортних засобів;

16) зброї, що перебуває у володінні та користуванні фізичних і юридичних осіб, яким надано дозвіл на придбання, зберігання, носіння, перевезення зброї;

17) викраденої, втраченої, вилученої, знайденої зброї, а також добровільно зданої зброї, зокрема тієї, що незаконно зберігалася;

18) бази даних, що формуються в процесі здійснення оперативно-розшукової діяльності відповідно до законодавства;

19) дорожньо-транспортних пригод з їх оформленням.

2. При наповненні реєстрів та баз (банків) даних, визначених у пункті 7 частини першої цієї статті, поліція забезпечує збирання, накопичення мультимедійної інформації (фото-, відео-, звукозаписи) та біометричних даних (відцифрований образ обличчя особи, відцифровані відбитки пальців рук, дактилокартки).

Збирання, накопичення, зберігання, використання та знищення біометричних даних здійснюються відповідно до вимог законодавства в порядку, встановленому Міністерством внутрішніх справ України.

Збирання, накопичення, зберігання, використання та знищення відомостей про генетичні ознаки людини (геномну інформацію людини) здійснюється також відповідно до законодавства..

3. Поліція забезпечує внесення відомостей до Єдиного реєстру осіб, зниклих безвісти за особливих обставин, та здійснює підтримку таких відомостей в актуальному стані в межах, визначених законодавством.

Стаття 27. Використання поліцією інформаційних ресурсів

1. Поліція має безпосередній оперативний (у тому числі

автоматизований) доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України "Про захист персональних даних".

2. Інформація про доступ до реєстру та бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про особу, яка отримала доступ, та про обсяг даних, доступ до яких було отримано.

3. Кожна дія особи щодо отримання інформації з інформаційних ресурсів, передбачених статтями 25-27 цього Закону, фіксується у спеціальному електронному архіві інформаційно-комунікаційної системи, за допомогою якої отримано відомості.

В електронному архіві фіксуються прізвище, ім'я, по батькові, посада та номер спеціального жетона (в разі наявності), вид отриманої інформації, реєстр, з якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації особи, яка отримувала інформацію з інформаційних ресурсів, реєстрів та баз (банків) даних.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням прозорості та захисту прав громадян базується на ряді законодавчих актів, що визначають правила та принципи роботи правоохоронних органів.

Згідно зі статтею 34 Конституції України, кожен має право на свободу думки та слова, а також право шукати, отримувати та поширювати інформацію будь-яким законним способом. Це означає, що поліція зобов'язана дотримуватися вимог закону та забезпечувати відкритість своєї діяльності перед громадськістю.

Крім того, Закон України «Про Національну поліцію» визначає принципи прозорості та відкритості у роботі поліції. Згідно зі статтею 9 [3] цього Закону поліція забезпечує публічний доступ до інформації про свою діяльність, за винятком випадків, передбачених цим Законом.

Стаття 34. Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань [1].

Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Здійснення цих прав може бути обмежене законодавством в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших

людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Стаття 9. Відкритість та прозорість [3]

1. Поліція здійснює свою діяльність на засадах відкритості та прозорості в межах, визначених Конституцією та законами України.

2. Поліція забезпечує постійне інформування органів державної влади та органів місцевого самоврядування, а також громадськості про свою діяльність у сфері охорони та захисту прав і свобод людини, протидії злочинності, забезпечення публічної безпеки і порядку.

3. Поліція забезпечує доступ до публічної інформації, володільцем якої вона є, у порядку та відповідно до вимог, визначених законодавством.

4. Поліція може оприлюднювати (поширювати) інформацію з обмеженим доступом лише у випадках та в порядку, визначених законодавством.

5. Нормативно-правові акти, що регламентують діяльність поліції, обов'язково оприлюднюються на веб-порталі центрального органу управління поліції. Нормативно-правові акти з обмеженим доступом оприлюднюються у випадках та в порядку, визначених законодавством.

6. Проєкти нормативно-правових актів, що стосуються прав та свобод людини, обов'язково проходять громадське обговорення в порядку, визначеному Міністром внутрішніх справ України.

Однак Національна поліція також зобов'язана дотримуватися принципів захисту прав громадян, включаючи конфіденційність особистих даних та інформації. Згідно зі ст. 30, 31 Конституції України, кожен має право на недоторканність свого житла, переписки, телефонних розмов та інших засобів комунікації [1]. Поліція зобов'язана дотримуватися цих принципів під час здійснення своїх повноважень.

Стаття 30. Кожному гарантується недоторканність житла [1].

Не допускається проникнення до житла чи до іншого володіння особи, проведення в них огляду чи обшуку інакше як за вмотивованим рішенням суду.

У невідкладних випадках, пов'язаних із врятуванням життя людей та майна чи з безпосереднім переслідуванням осіб, які підозрюються у

вчиненні злочину, можливий інший, встановлений законодавством, порядок проникнення до житла чи до іншого володіння особи, проведення в них огляду і обшуку.

Стаття 31. *Кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законодавством, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.*

Таким чином, правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням прозорості та захисту прав громадян визначається низкою законодавчих актів, які забезпечують баланс між публічною відкритістю та конфіденційністю особистих даних.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням принципів ефективності та результативності базується на ряді законодавчих актів, які визначають стандарти та вимоги до роботи правоохоронних органів.

Згідно зі статтею 26 Закону України «Про Національну поліцію» поліція має забезпечувати ефективне використання ресурсів та досягати конкретних результатів у сфері забезпечення правопорядку та безпеки громадян [3].

Досягнення результативності в роботі поліції потребує використання сучасних методів та технологій аналізу інформації. Застосування цифрових технологій, таких як системи аналітики даних та машинного навчання, дозволяє поліції швидко та ефективно обробляти великі обсяги інформації, виявляти закономірності та тенденції у сфері злочинності, а також прогнозувати можливі кримінальні події.

Стаття 27 Закону "Про Національну поліцію" визначає вимоги до збереження та обробки інформації про діяльність поліції, що також сприяє підвищенню її ефективності. За допомогою аналізу цієї інформації поліція може виявляти слабкі місця у своїй діяльності та вдосконалювати стратегії протидії злочинності [3].

Таким чином, правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням принципів ефективності та результативності є ключовим для забезпечення безпеки громадян та правопорядку в країні.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням інноваційного розвитку

базується на законодавчих актах, що визначають стратегії та напрями використання передових технологій та методів в роботі правоохоронних органів.

Стаття 25 вищезгаданого Закону надає право поліції на використання інноваційних методів та засобів в інформаційно-аналітичній діяльності для ефективного забезпечення правопорядку та безпеки громадян [3].

Одним з пріоритетних напрямів інноваційного розвитку є застосування штучного інтелекту та аналіз великих обсягів даних. Згідно зі статтею 40 цього Закону поліція має право використовувати сучасні програмні засоби для автоматизації процесів аналізу та обробки інформації [3].

Стаття 40. Застосування технічних приладів, технічних засобів та спеціалізованого програмного забезпечення

1. Поліція для виконання покладених на неї завдань та здійснення повноважень може застосовувати такі технічні прилади, технічні засоби та спеціалізоване програмне забезпечення:

1) фото- і відеотехніку, у тому числі техніку, що працює в автоматичному режимі, технічні прилади та технічні засоби з виявлення та/або фіксації правопорушень;

2) технічні прилади та технічні засоби з виявлення радіаційних, хімічних, біологічних та ядерних загроз;

3) безпілотні повітряні судна та спеціальні технічні засоби протидії їх застосуванню;

4) спеціальні технічні засоби перевірки на наявність стану алкогольного сп'яніння;

5) спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото- і відеоінформації, у тому числі для встановлення осіб та номерних знаків транспортних засобів.

Технічні прилади та технічні засоби, передбачені пунктами 1 і 2 цієї частини, поліція може закріплювати на однострої, у/на безпілотних повітряних суднах, службових транспортних засобах, суднах чи інших плавучих засобах, у тому числі тих, що не мають кольорографічних схем, розпізнавальних знаків та написів, які свідчать про належність до поліції, а також монтувати/розміщувати їх по зовнішньому периметру доріг і будівель.

Поліція може використовувати інформацію, отриману за допомогою фото- і відеотехніки, технічних приладів та технічних засобів, що перебувають у чужому володінні.

2. *Інформація про змонтовані/розміщені технічні прилади,*

технічні засоби повинна бути розміщена на видному місці.

3. Строки та порядок зберігання матеріалів фото- і кінозйомки, відеозапису та результатів їх аналізу встановлюються Міністерством внутрішніх справ України.

До інших інноваційних методів можна віднести використання систем розпізнавання образів, голосових технологій, біометричних систем та інших технологій для швидкого та точного ідентифікування осіб та виявлення злочинців.

Стаття 25 Закону «Про Національну поліцію» визначає зобов'язання поліції забезпечувати інформаційно-аналітичну діяльність з використанням інноваційних методів з урахуванням захисту прав та свобод людини [3].

Таким чином, правове регулювання інформаційно-аналітичної діяльності Національної поліції України із застосуванням інноваційного розвитку сприяє покращенню ефективності та результативності діяльності поліції, забезпечуючи безпеку та захист прав громадян.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України з використанням штучного інтелекту визначається певною кількістю законодавчих актів, які враховують сучасні технологічні можливості та забезпечують захист прав громадян.

Відповідно до розділу ІІ Зміст і напрями реформування органів правопорядку п. 5 комплексного стратегічного плану реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки, схваленого Указом Президента України від 11 травня 2023 року № 273/2023, запропоновано використання штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень в правоохоронній діяльності [8].

5. Комплексна цифрова трансформація

5.1. Здійснення консолідованої поетапної цифрової трансформації органів правопорядку та прокуратури на основі інструментів стратегічного менеджменту, які відповідають найкращим практикам ЄС.

5.2. Подальше впровадження в діяльність органів правопорядку та прокуратури інноваційних технологічних досягнень, що забезпечують гнучкість операційних процесів, ІТ-рішення, цифрову спроможність оперативно реагувати на події та зміни й здобувати результат, орієнтований на інтереси суспільства.

5.3. Поетапне впровадження електронної системи управління

кримінальними провадженнями шляхом комплексної заміни та модернізації обладнання, забезпечення сумісності ІТ-систем, безперебійності роботи, доступу усіх учасників кримінального провадження та інтероперабельності.

5.4. Підвищення ефективності діяльності органів правопорядку та прокуратури через забезпечення більшої доступності й повноти інформації, розроблення і впровадження сервісів на Єдиному державному вебпорталі електронних послуг.

5.5. Впровадження заходів безпеки і захисту персональних даних відповідно до стандартів ЄС.

5.6. Удосконалення та впровадження більш безпечних, гнучких, спроможних і доступних систем зв'язку між усіма органами правопорядку та іншими екстреними службами (включаючи цифрове радіо: голосовий зв'язок і широкосмугове передавання даних).

5.7. Запровадження в усіх органах правопорядку та прокуратури уніфікованої системи особистої автентифікації та системи біометричного зіставлення із поступовим забезпеченням її сумісності з європейськими системами. ***Широке використання під час здійснення досудового розслідування, а також для обробки даних та аналітичної діяльності органів правопорядку і прокуратури штучного інтелекту, блокчейну, хмарних обчислень та інших інноваційних рішень.***

5.8. Оновлення операційних процесів за допомогою ІТ-систем, придатних для обміну даними з інституціями ЄС відповідно до стандартів ЄС.

5.9. Надання органам правопорядку та прокуратури для забезпечення виконання покладених на них функцій права на безпосередній спільний доступ до автоматизованих інформаційних і довідкових систем, реєстрів і баз даних, держателем (адміністратором) яких є інші державні органи.

Також штучний інтелект дозволяє автоматизувати процеси аналізу значних обсягів даних, виявлення закономірностей та тенденцій у злочинності, а також прогнозування можливих кримінальних подій.

Наприклад, відповідно до ч.ч. 1, 3 ст. 9 Закону України «Про пробацію» досудова пробація – це забезпечення суду формалізованою інформацією, що характеризує обвинуваченого, з метою прийняття судом рішення про міру його відповідальності. Досудова доповідь про обвинуваченого повинна містити: соціально-психологічну характеристику; оцінку ризиків учинення повторного кримінального правопорушення; висновок про можливість виправлення без обмеження

волі або позбавлення волі на певний строк [9]. Згідно з ч.ч. 1, 2 ст. 314–1 Кримінального процесуального кодексу України з метою забезпечення суду інформацією, що характеризує обвинуваченого, а також прийняття судового рішення про міру покарання представник уповноваженого органу з питань пробації складає досудову доповідь за ухвалою суду. Досудова доповідь складається щодо особи, обвинуваченої у вчиненні злочину невеликої або середньої тяжкості, або тяжкого злочину, нижня межа санкції якого не перевищує п'яти років позбавлення волі. Досудова доповідь щодо неповнолітнього обвинуваченого віком від 14 до 18 років складається незалежно від тяжкості вчиненого злочину, крім випадків, передбачених Кримінальним процесуальним кодексом України [10].

Таким чином, використання штучного інтелекту у роботі Національної поліції України є важливим елементом забезпечення безпеки та правопорядку, а правове регулювання цього процесу здійснюється відповідно до вимог законодавства з метою захисту прав та свобод громадян.

Правове регулювання інформаційно-аналітичної діяльності Національної поліції України з використанням аналізу великих даних (big data) визначається серією законодавчих актів, що враховують сучасні технологічні можливості та забезпечують захист прав громадян.

Статті 25, 26, 27 Закону України «Про Національну поліцію» надають поліції право на використання аналізу даних з метою забезпечення правопорядку та безпеки громадян.

Використання аналізу значних даних дозволяє поліції швидко та ефективно обробляти великі обсяги інформації, виявляти закономірності та тенденції в злочинності, а також прогнозувати можливі кримінальні події.

Стаття 40 цього Закону визначає право поліції на використання сучасних програмних засобів для автоматизації процесів аналізу та обробки інформації, включаючи системи аналізу даних [3].

Використання аналізу значних даних у роботі Національної поліції повинно здійснюватися з дотриманням цього принципу та урахуванням конфіденційності особистих даних громадян.

Тож правове регулювання інформаційно-аналітичної діяльності Національної поліції України з використанням аналізу великих даних спрямоване на підвищення ефективності та результативності роботи правоохоронного органу та забезпечення безпеки громадян.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які принципи інформаційно-аналітичної діяльності Національної поліції України забезпечують її ефективність та об'єктивність?
2. Які основні методи інформаційно-аналітичної діяльності Національної поліції України використовуються для боротьби зі злочинністю та забезпечення безпеки громадян?
3. Які головні етапи включає алгоритм правового регулювання інформаційно-аналітичної діяльності Національної поліції України?
4. Які основні нормативні акти забезпечують правове регулювання інформаційно-аналітичної діяльності Національної поліції України?
5. Які функції виконує єдина інформаційна система МВС?
6. Які основні завдання Департаменту інформаційно-аналітичної підтримки (ДІАП)?
7. Які основні документи міжнародного правового регулювання інформаційно-аналітичної діяльності Національної поліції України?
8. Перелічіть основні фактори актуальності правового регулювання інформаційно-аналітичної діяльності Національної поліції України. Обґрунтуйте відповідь.
9. Назвіть основні перспективні напрями правового регулювання інформаційно-аналітичної діяльності Національної поліції України. Обґрунтуйте відповідь.
10. Які існують повноваження поліції у сфері інформаційно-аналітичного забезпечення?

ЛІТЕРАТУРА ЗА РОЗДІЛОМ:

1. Конституція України від 28.06.1996: станом на 01.01.2020 URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення 10.05.2024).
2. Офіційне інтернет-представництво «Президент України» URL: http://surl.li/uhubf (дата звернення 09.05.2024).
3. Про Національну поліцію: Закон України від 02.07.2015: № 580-VIII: станом на 18 травн. 2024 URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення 10.05.2024).
4. Про затвердження Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку пріоритетних електронних інформаційних ресурсів її суб’єктів: Постанова Кабінету Міністрів України від 14 листопада 2018 р. № 1024 станом на 22 серп. 2023, URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#Text (дата звернення 08.05.2024).
5. Положення про Департамент інформаційно-аналітичної підтримки Національної поліції України, Наказ Національної поліції України від 31.01.2020 року № 77 URL: https://www.npu.gov.ua/pro-policiyu/struktura-

nacionalnoyi-policiyi/departament-informacijno-analitichnoyi-pidtrimki (дата звернення 10.05.2024).

6. Європейська конвенція з прав людини: ратифіковано Законом № 475/97-ВР від 17.07.97: станом на 01.08.2021 URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення 09.05.2024).

7 Конвенція Організації Об'єднаних Націй проти корупції: Ратифіковано від 18.10.2006 URL: https://zakon.rada.gov.ua/laws/show/995_c16#Text (дата звернення 10.05.2024).

8. Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023-2027 роки: Указ Президента України від 11.05.2023 року № 273/2023 URL: https://zakon.rada.gov.ua/laws/show/273/2023#Text (дата звернення 08.05.2024).

9. Про пробацію: Закон України від 05.02.2015 № 160-VIII; станом на 28 бер. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/160-19#Text (дата звернення 10.05.2024).

10. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI: станом на від 19 травн. 2024. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення 09.05.2024).

Розділ 2
ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ

2.1. Загальна характеристика роботи з аналізу інформації

Безперечно, що ефективність правоохоронної діяльності залежить від аналізу отриманої інформації. Метою та засобом професійного реагування на загрози в правоохоронній діяльності при залученні та створенні усіх необхідних вимог щодо захисту інформації, її обробки, передачі та аналізу, є рівень її безпеки. Існуючі нормативно-правові акти повною мірою відображають сутність інформаційно-аналітичного забезпечення правоохоронної діяльності.

Інформаційний аналіз працює шляхом об’єднання різнорідної інформації в систему логічних залежностей (просторово-часових, причинно-наслідкових та інших), щоб усю сукупність фактів і кожен факт окремо можна було правильно оцінити.

Інформаційно-аналітична робота полягає в отриманні нових знань (вихідної інформації), що є складним процесом, який передбачає дослідження і має певну логічну послідовність. Проведення інформаційно-аналітичних досліджень розуміється як взаємопов'язана операційна система, що утворює технологічний цикл відбору, групування інформації про події, явища, процеси, в якому кожен факт знаходить своє місце і співвідноситься з попереднім у просторі та часі, ситуативна кореляція та причинно-наслідкова залежність.

Основні функції інформаційно-аналітичної діяльності

В інформаційно-аналітичній діяльності особлива увага приділяється таким функціям:

- *сигнальна функція – зосередження на причинах і проявах терористичних характеристик;*

- *інформаційна функція – інформування підрозділів про поточний час;*

- *забезпечувальна – забезпечення аналітичної підтримки діяльності підприємства;*

- *функція прогнозування – передбачення розвитку ситуації на певний період;*

- *функція ведення бази даних.*

2.2 Формулювання принципів інформаційно-аналітичної діяльності

Розробка принципів інформаційно-аналітичної роботи дозволяє аналітикам зрозуміти один з них і підвищити якість своєї роботи. Розглянемо окремі з них.

Відповідність обраного методу меті аналізу Спосіб вирішення того чи іншого завдання, що стоїть перед аналітиком, залежить від мети і характеру використання кінцевого результату.

Під час аналізу використовуйте один концептуальний інструмент. Існує потреба в єдиній термінології для одних і тих самих процесів чи явищ, що характеризують господарську діяльність.

Повнота аналізу. Ретельне вивчення всіх джерел, з яких доступна інформація, з сайтом з'ясування можливих і використання кожного джерела, визначення того, скільки інформації, яку вони надають, підтверджує або запитує одну одну і, за необхідності, може порівнювати з попередніми даними обмежено або порівнювати подібні дані (наприклад, дані інших відділів).

Глибина аналізу. Визначити деструктивність, причини та наслідки інциденту та розробити чітке рішення, щоб кінцевий користувач мав чітке уявлення про ситуацію, що склалася, та можливий напрям її подальшого розвитку.

Обґрунтованість аналітики на діалектичному рівні. Визначати тенденції розвитку ситуації, прогнозувати можливі події та давати рекомендації щодо подальшої поведінки кінцевих користувачів інформації з урахуванням суттєвих факторів.

Об'єктивність аналізу. Особисті здібності аналітиків, громадська думка та інші суб'єктивні фактори керуються лише наявною інформацією, щоб зробити результати якомога ближчими до об'єктивних фактів.

Урахування імовірнісного характеру отриманих висновків. Завжди необхідно показувати, наскільки вірогідно отримана вихідна інформація відповідає об'єктивним фактам.

Своєчасність. Ці явища та процеси вивчаються, а результати їх аналізу можна використовувати в режимі реального часу.

Формулювання у звіті лаконічних чітких висновків. Використання, зрозуміле кінцевим користувачам і відповідне відповідним цілям і завданням господарської діяльності.

Інформаційний аналіз – це процес пізнання об'єктивної реальності

на основі законів діалектики та формальної логіки та з використанням загальнонаукових методів дослідження. Закони і методи психологічної діяльності, а також технічні засоби становлять засоби інформаційно-аналітичної роботи, на основі яких більш якісно обробляються фактичні дані, щоб з них можна було витягнути все, що вони пропонують.

Як відомо, процес розуміння об'єктивної реальності представлений в єдиній формі перцептивного або перцептивного (сприйняття, відчуття) і раціонального або логічного аспектів. Крім того, поділ когнітивних процесів на сприйняття, уявлення та поняття не передбачає незалежного існування кожної форми іменування. Усе це взаємопроникає, утворюючи складний комбінований образ.

2.3. Суть процесу мислення в інформаційній роботі

Процес мислення та аналізу інформаційної роботи полягає в тому, щоб отримати деяку початкову інформацію, ідентифікувати інформацію, яка недоступна, і як тільки ця інформація отримана (незалежно або за допомогою бізнес-підрозділу), отримати чітке розуміння того, що відбувається. Глибоке проникнення в природу речей вимагає виявлення внутрішніх зв'язків, закономірностей та істотних властивостей речей. Воно здійснюється за допомогою розумових операцій – аналізу та синтезу.

Аналіз (від грец. αναλυσις – розкладання) – розкладання об’єкта на складові елементи з метою розуміння їх місця в системі, виділення в ній найважливіших (первинних) елементів. Іншими словами, це «роздроблення» конкретної теми чи явища на окремі частини. Аналіз може бути об'єктивним, логічним або образним (найбільш широко використовується при вивченні суспільних явищ).

Синтез (від грец. комбінація – склад), на відміну від аналізу, матеріальне або уявне поєднання частин предмета, яке виявляє внутрішні необхідні зв’язки між ними та закономірний характер предмета. Синтез – це побудова цілого з аналітично визначених елементів і розуміння того, як ціле складається з елементів і як відбувається їх взаємодія в рамках цілого.

Аналіз та синтез єдині, тому що предмет і його складові (сторони) унікальні. Вони є моментами взаємодії в єдиному аналітичному синтезі наукового знання. Їх зв'язок простий: немає синтезу без аналізу, і немає сутнісного аналізу без синтезу. План заходів щодо впровадження поточної дієвої економічної інформації, оцінка доказів, характеристика

отриманих даних тощо – все в синтетичній формі, без якої інформація, зокрема, є механічним набором даних, не організованих в єдину систему. Один із методів вивчення руху і розвитку об'єктів полягає в тому, що їх внутрішній зв'язок – від абстрактного до конкретного початку.

Абстракція (від латинського «abstractio», тобто відволікання) – результат уявного відволікання від одних сторін (особливостей, якостей) предмета і виділення інших, що є необхідним і важливим на даному етапі дослідження. Таким чином, формуються абстрактні поняття, що є важливою формою логічного пізнання. Часто абстрагування здійснюється для того, щоб провести більш ретельне дослідження явища, спираючись на попередній аналіз і синтез. На відміну від абстракції, конкретне є результатом поєднання понять, вибраних у процесі абстрагування, в одну загальну річ. Конкретне – це предмет мислення, втілений у єдності своїх компонентів, зв'язків і відносин. Як логічні категорії абстрактність і конкретність мають свою основу в об'єктивній дійсності – єдності і повноті предметів і явищ, наявності певних складових, частин і сторін. При цьому пізнання предмета (наприклад, пізнання спеціальної мети розвідувальної діяльності конкурента) походить від найпростіших елементарних понять, що відтворюють ті або інші частини, сторони предмета до більш складних понять, що відображають об’єкт у всій його повноті.

В інформаційно-аналітичній діяльності активно застосовуються індукція та дедукція. Індукція (від латинського «in-ductio», тобто наведення) – це процес руху думки від поодиноких явищ до загальних висновків, засіб отримання загального знання про окремі аспекти (предмети, явища). Індукція дозволяє отримувати нове знання завдяки тому, що отримані знання з її допомогою поширюються на коло нових, ще невивчених предметів. Однак поширюючи знання про один клас предметів на інший, ширший, вона переважно не змінює самого змісту понять, що свідчить про неповноту (обмеженість) індукції. Виникає необхідність доповнення її іншими прийомами дослідження, такими як аналіз, синтез, узагальнення тощо.

Дедукція (латинське deductio, від deduco – «збиваю, забираю») – рух думки від загального до одиничного. Якщо існують знання про цілу категорію предметів загалом, ці знання можна поширити шляхом дедукції на будь-який предмет у цій категорії. Дедукція використовується як спосіб побудови теорії. Як аналіз і синтез, індукція і дедукція пов’язані. Щоб отримати знання про універсалії, необхідно знати одиничне і навпаки.

З цього можна зробити висновок, що мислення – це процес

породження умов за допомогою логічних операцій. Інтелектуальна діяльність людини включає два основних види – **алгоритмічний та евристичний**. Перший показує як конкретно досягти поставленої мети. Другий передбачає вирішування нестандартних завдань, рішення яких дослідникові невідомі і з якими він не стикався на практиці. Алгоритмічна та евристична діяльність не виключають, а радше доповнюють одна одну.

Евристична діяльність – це складна, багатоаспектна та різнобічна інтелектуальна діяльність людини, яка відбувається, прихована і непридатна для об'єктивного дослідження та опису в рамках науки. Евристика значною мірою базується на інтуїції. Таємниця інтуїції неодноразово спонукала писати про неї дослідників, філософів, поетів. Найчастіше це вважається містичним, надприродним способом розуміння істини, який сам по собі не підлягає жодному раціональному поясненню.

Емоції можуть втрутитися і змінити процес мислення. Однак емоції не тільки спотворюють, але й стимулюють мислення. Відомі приклади як люди під впливом загострених емоцій здатні вирішувати проблеми несподіваним і незвичайним способом. Емоції особливо виражені в процесі мислення, коли людина знаходить рішення складного завдання, де воно виконує евристичну та регулятивну функції. Евристична функція емоцій полягає у виділенні деякої оптимальної області пошуку, в межах якої знаходиться вирішення поставленого завдання. Регулююча функція емоцій у мисленні може активізувати пошук правильного рішення, якщо вона спрямована в правильному напрямі, або уповільнити пошук правильного рішення, якщо інтуїція підкаже, що обраний процес мислення є неправильним.

Одну з класифікацій типів психологічної діяльності людини, засновану на ознаках екстравертності та інтроверсії, домінування раціональності або інтроверсії. ірраціонального, емоційного та логічного в процесах мислення, запропонував психолог К.Г. Юнг. Він виділив такі типи людей за характером мислення:

- *інтуїтивний тип: характеризується перевагою емоцій над логікою та домінуванням правої півкулі над лівою;*
- *раціональний тип: характеризується раціональністю, домінуванням лівої півкулі над правою, логіки над інтуїцією та емоціями.*

2.4 Основні етапи інформаційно-аналітичної діяльності

Першим етапом інформаційно-аналітичної діяльності завжди є визначення завдання. Завдання визначає передусім керівництво компанії або керівники відділів. Це твердження випливає з того факту, що аналіз інформації покликаний сприяти успішному існуванню будь-якої економічної діяльності. Завдання можуть бути поставлені при отриманні додаткової інформації (отриманої різними способами, в тому числі оперативної економічної).

Другим етапом є організація видобутку, збору та первинна обробка вихідних даних. Аналітик може збирати інформацію безпосередньо з баз даних і відкритих джерел або за допомогою оперативних підрозділів для проведення первинного збору. Інформаційна робота базується на ідеї, що дані можуть бути знайдені та використані для вирішення будь-якої теми дослідження в максимально можливому обсязі. Щоб досягти успіху, необхідно правильно осмислювати й оцінювати події, а також розглядати їх під різними кутами зору, в тому числі з точки зору конкурентів і партнерів.

Оцінити інформацію. Мета полягає в тому, щоб перевірити, чи відповідає вона критеріям оцінки. «Офіційна діяльність керується мотивами, що стоять за нею, тому офіційна мета, яка пов’язана з мотивом, стає уявним образом цінності, яку створює службовець, що є тим, чого від нього вимагає його службовий обов’язок». Отже, критерії оцінки, які використовує працівник, мають значну цінність у початковій інформації, яка є вирішальною в процесі її вивчення, оцінки та застосування (наприклад, використання методів наукового дослідження або отримання інформації за допомогою конкурентної розвідки). Процес збору, перевірки та зважування інформації для покращення господарської діяльності починається з моменту її отримання і завершується прийняттям остаточного рішення. Загалом, перевірка інформації передбачає дослідження, уточнення та додаткові заходи, такі як порівняння та усунення протиріч.

Зібрані відомості повинні перевірятися та оцінюватися за критеріями вірогідності, цінності, об'єктивності, повноти, актуальності.

***Вірогідність* інформації** – це індикатор достовірності, доведеної істинності чи хибності інформації, індикатор того, чи заслуговує довіри інформація щодо її правдивості. Достовірною вважається інформація, яка обґрунтована логічними чи практичними методами. На практиці

використовуються такі методи підтвердження:

а) оцінка відомостей з погляду здорового глузду;

б) оцінка надійності джерел відомостей;

в) повторний огляд відомостей через інші незалежні джерела інформації.

Здоровий глузд – це сукупність знань, умінь і навичок, які використовують співробітники в практичній діяльності. Вони не завжди мають строге наукове обґрунтування.

Надійність різних джерел інформації оцінюється за допомогою різних показників. Так, надійність технічних засобів як джерел інформації визначається їх тактико-технічними характеристиками. Надійність же людей містить наступні складові:

а) ***політичну надійність*** – характеристику відданості справі забезпечення безпеки підприємства і підтверджувальних її практичних дій;

б) ***інтелектуальну надійність*** – характеристику стану загальних і спеціальних знань, а також здібностей реалізовувати їх практично;

в) ***психологічну*** **і** ***фізичну надійність*** – характеристику розумового і фізичного розвитку, загального психічного і фізичного стану, стану психіки, її здатності адекватно відображати і використовувати реальність.

Існує кілька причин, які сприяють змінюванню інформації. Одну з цих помилок називають "помилкою перспективою". Суть її полягає в тому, що одні й ті ж події можуть розцінюватися по-різному залежно від часових рамок. Зазвичай недавнє забувається швидко, тоді як свіжа або давня подія легко запам'ятовується. Це справедливо через психофізіологічний механізм негативної індукції, який описаний в літературі. Крім того, спотворення інформації може бути пов'язане з проявом негативних емоцій, таких як гнів, страх, переляк та інші, які впливають на сприйняття подій.

Психологи також вказують на "ефект випромінювання", коли найближчі події можуть суттєво змінити сприйняття минулих подій. Абсолютно надійних джерел інформації не існує. Точність визначення достовірності інформації в значній мірі залежить від усвідомлення співробітниками надійності їх джерел. Коли джерелом є людина, істинність інформації зберігається, якщо вона передається об'єктивно, без власних інтерпретацій.

Оцінка якості джерел інформації може бути представлена системою умовних позначок: "дуже надійне джерело" означає, що отриманій від нього інформації можна цілком довіряти; "надійне джерело" – інформації

можна довіряти до 90%; "дуже серйозне джерело" – можна довіряти на 75% і так далі. У своїй науковій праці "Strategic Intelligence Production: Basic Principles" американський розвідник В. Плетт описує буквено-цифрову систему визначення надійності джерела і вірогідності інформації. Надійність джерела позначається буквами від A до F, тоді як вірогідність інформації – цифрами від 1 до 6.

A – абсолютно надійне джерело;

B – звичайно надійне джерело;

C – досить надійне джерело;

D – не завжди надійне джерело;

E – ненадійне джерело;

F – надійність джерела не можна визначити.

Цифрові позначення вірогідності інформації, які ставляться після літер, що позначають надійність джерела, розшифровуються так:

1 – вірогідність відомостей підтверджується даними з інших джерел;

2 – відомості, імовірно правильні;

3 – відомості, можливо правильні;

4 – сумнівні відомості;

5 – відомості неправдоподібні;

6 – вірогідність відомостей не можна встановити.

При систематизації наявної інформації та перевірці через інші незалежні джерела співробітники повинні зрозуміти, що отримана інформація має підтверджувати або спростовувати лише основні вихідні дані. Важливо, щоб деталі узгоджувалися практично. Інакше сумніви щодо достовірності інформації можуть лише зростати.

Є ймовірність, що співробітники опиняються у ситуації дезінформації через різні канали. Висновки про достовірність інформації визначають питання про його правдивість або помилковість. Сумніви у достовірності залишають питання відкритими, оскільки на момент оцінки відсутні достатні логічні чи практичні засоби доведення.

Для співробітників аналітичної служби, які приділяють увагу запобіганню діям конкурентів, дуже важливо своєчасно передавати отриману інформацію до конкретного підрозділу підприємства, який може остаточно визначити її цінність та вжити заходів для перешкоджання планам конкурентів. Все це здійснюється з урахуванням зв'язків конкурентів, матеріальних можливостей та потаємного характеру їх діяльності. Тому для оцінки первинної інформації цікавлять такі критерії, як ставлення до конкретного питання та причина, пов'язана з її значущістю.

Цінність – важливість для кінцевого користувача (оперативного органу), тобто, наскільки отримана інформація дозволяє йому наблизитися до вирішення власних цілей і завдань. Віднесена за належністю така інформація є високого ступеня цінності, оскільки вона дозволяє вжити запобіжних заходів, спрямованих на ліквідацію умов, що детермінують або сприяють заподіянню шкоди конкурентами.

Об'єктивність – ступінь абстрагування джерела від особистих почуттів, мотивів, інтересів. Об'єктивність аналітичних матеріалів високою мірою залежить від професіоналізму аналітика.

Повнота – те, якою мірою отримані дані знижують рівень ентропії аналізованої проблеми, і те, якою мірою вони охоплюють різні аспекти ситуації, що склалася.

Актуальність – оперативність та своєчасність отриманої інформації для потреб сьогодення. Найважливішим моментом, на який необхідно звернути увагу, є падіння з часом цінності інформації. Фахівці вважають, що оперативно-тактична інформація втрачає цінність приблизно по 10% на день. Інформація стратегічного, довготривалого характеру – приблизно по 10% на місяць. Інформація про постійні об'єкти – приблизно по 15% на рік. Цінність інформації може зменшуватися з часом та у зв'язку з різкою зміною оперативної обстановки. Оцінка наявних відомостей за вищеописаними критеріями дозволяє виявити відсутні вихідні дані та зайнятися їх отриманням.

Після одержання всіх можливих вихідних даних аналітик переходить до **третього етапу інформаційно-аналітичної діяльності – аналізу.** Його основу становить знаходження причинно-наслідкових зв'язків між різними фактами, процесами, одержання нової інформації, що не було раніше, що носить характер висновків, шляхом використання методів аналітики. Можна сказати, що це процес, пов'язаний з узагальненням, сортуванням, відбором і концентрацією інформації для вирішення поставлених перед аналітиком завдань. Залежно від цілей і рівнів застосування – стратегічного, оперативного й(або) тактичного, він виступає як *загальний або особливий*. Аналіз інформації базується на системному підході в дослідженні явищ і процесів, охоплених економічним простором, у статиці і динаміці, у всіх їх значимих зв'язках, відносинах і протиріччях.

В інформаційно-аналітичній діяльності виділяють три різновиди аналізу:

- **ретроспективний** (аналіз минулого);
- **сучасний**;
- **прогностичний** (аналіз майбутнього).

Ретроспективний аналіз здійснюється, перш за все, в інтересах оцінки виконаних дій, їх ефективності, а також, за необхідності, в ході вивчення історії виникнення та вирішення тих чи інших проблем.

Сучасний аналіз характеризується тим, що отримані під час виконання проміжні результати – узагальнені висновки містять інформацію про сучасний стан економічної ситуації.

Прогностичний аналіз відрізняється від двох попередніх різновидів тим, що не лише отримані в процесі його кінцеві результати – рекомендації (пропозиції), а й узагальнені висновки мають прогностичний характер.

Результати прогностичного аналізу (прогнози) можуть містити інформацію двох видів:

- *по-перше*, відомості про майбутній стан реально існуючих ситуацій,
- *по-друге*, відомості про майбутній стан потенційних ситуацій, які в момент аналізу реально не існують, але можуть або мають виникнути у майбутньому.

Прогностичний аналіз є найбільш складним для співробітників різновидом роботи й *становить найбільший інтерес* для практики економічної діяльності.

На основі аналізу даних, що містяться в інформації, та подальшого синтезу, виявленого в результаті аналізу особливостей, специфіки раніше розрізнених даних, виявляються закономірності, які дозволяють зробити висновки. Необхідно враховувати, що в процесі аналізу аналітик має справу з припущеннями, які є недостатньо надійними фактами, тому багато висновків даються з певним ступенем ймовірності. Проте довільні висновки в аналітичних оцінках неприпустимі. Твердження, які викликають сумніви, необхідно обговорювати.

З вищевикладеного можемо зробити висновок, що аналітика в процесі здійснення діяльності щодо забезпечення економічної безпеки відіграє інформаційно-орієнтуючу, узагальнюючу роль та роль прогностичного апарату. Таким чином, аналіз та оцінка інформації не можуть здійснюватися без урахування відображених у ній причинно-наслідкових зв'язків та явищ. Завдання аналізу – виявлення причин, що зумовлюють перебіг події та розвиток оперативних ситуацій. Інакше він буде відірваний від дійсності і не відповідатиме своєму призначенню.

Отримана інформація може бути класифікована залежно від подальшого використання відомостей на наступні категорії:

- *сигнальна* (попереджуюча) інформація;
- інформація, що використовується для одержання *нової*

інформації;

- *тактична* інформація (що передбачає негайне реагування);
- *доказова* інформація;
- *перевірочна* інформація.

І, нарешті, **четвертий етап інформаційно-аналітичної діяльності – виборче поширення отриманої інформації**. Цей етап містить у собі складання підсумкового документа за результатами аналізу (звіт, прогноз і т.п.) і його надання кінцевому користувачеві інформації. В аналітичному звіті, як в основній формі надання інформації, повинні розглядатися невідомі питання, пов'язані з досліджуваним об'єктом, явищем, процесом, але в нетрадиційному ракурсі. Основне призначення звіту – підвищити рівень знання досліджуваного питання.

Звіт може носити характер поточного документа з окремого питання або представляти капітальне, всебічне дослідження. Найважливішими властивостями, які він повинен мати, – це **корисність та своєчасність**. Вчасно добута розвідувальна інформація створює можливість попередження і припинення дій конкурентів та інших негативних процесів. Для того, щоб реалізувати інформацію, вона повинна бути узагальнена і повідомлена в правильно сприйнятій формі. Тому вимогою, пропонованою до інформації у звіті, слід вважати ***лаконічність повідомлень при максимальному змістовному навантаженні.*** Лаконічність підвищує насиченість, скорочує час на передачу і сприйняття інформації.

Неодмінною умовою сприйняття текстової інформації є **логічність викладу**. Вона передбачає послідовність, доказовість, переконливість (за рахунок усунення суперечливих даних), відсутність непотрібних деталей, пропорційність місця, відведеного у повідомленні того чи іншого питання, значущість цього питання, ясність мети, досягнення якої покликане для найкращого аналізу отриманої інформації.

Таким чином, можна сформулювати наступне визначення інформаційно-аналітичної діяльності (ІАД) – це вид інтелектуальної та розумової діяльності людини. Тобто в процесі інтелектуальної та розумової діяльності людини відбувається генерування нової інформації в результаті певного алгоритму послідовних дій з пошуку, зберігання, обробки та аналізу первинної інформації. Отримана таким чином нова, вторинна аналітична інформація, генерується у вигляді аналітичних записок, звітів, оглядів, прогнозів тощо.

Певною мірою інформаційно-аналітична діяльність захищає та убезпечує керівників і менеджерів від сучасних ризиків, небезпек та викликів. А це впливає на прийняття ефективних управлінських рішень,

сприяє запобіганню та передбаченню можливих наслідків будь-яких загроз, що можуть мати негативний характер. Саме прийняття ефективних управлінських рішень щодо убезпечення несприятливих ризикових подій є важливим елементом при підготовці аналітичних звітів і прогнозів в правоохоронній діяльності.

Розглянемо деякі методи, які використовуються в інформаційно-аналітичній діяльності.

Метод експертних оцінок – це узагальнена думка групи експертів, яка приймається як вирішення проблеми. Існує два види експертного оцінювання: індивідуальне та колективне.

Колективне експертне оцінювання базується на принципі виявлення колективної експертної думки щодо перспектив розвитку аналізованого об'єкта.

Методи індивідуального експертного оцінювання ґрунтуються на думці незалежних експертів у відповідній галузі.

Експертна методологія нині широко використовується і базується на роботі спеціальних комісій – обговореннях групами експертів. Узгодження думок за "круглими столами" та формулювання єдиної думки сьогодні використовується при роботі експертних комісій при обговоренні та прийнятті відповідних рішень, що підвищує ймовірність прийняття правильного рішення.

Метод мозкового штурму – це сукупність прийомів генерування нових ідей, серед яких формується нова ідея шляхом творчої співпраці організованої групи експертів.

Метод колективної генерації ідей спрямований на отримання великої кількості ідей, в тому числі ідей від людей, які є обізнаними, але зазвичай неохоче висловлюють власну думку.

Метод дискусії. Це підготовка до прийняття рішень із залученням широкого кола учасників, які ведуть відкриту дискусію щодо поставленої проблеми та аналізують усі фактори, що в той чи інший час мали вплив на певну подію.

Відбувається відкрите групове обговорення поставленого питання, основні завдання, наслідки, обговорюються та уточнюються позиції усіх учасників. А вже після цього приймається відповідне рішення.

Метод ключових питань. Цей метод підходить для збору додаткової інформації в проблемних ситуаціях. Поставлені запитання дають поштовх для формування стратегії і тактики вирішення даної проблеми.

Метод аналогії. Цей метод використовується в певній організації, де мали місце подібні ситуації, та аналізуються рішення, які були

прийняті в тій ситуації, та їх результативність.

Метод Дельфі. Тривалий час проводиться опитування групи експертів, після чого залишаються лише ті пропозиції, які були унікальними. Зберігається анонімність експертів, що дає можливість отримати найбільш ґрунтовні та найкращі судження, їх обґрунтування та прогнозування їхньої подальшої діяльності.

Інформаційно-аналітична діяльність – це процес, що включає збір, аналіз і оцінку інформації з метою формування корисних знань, розуміння поточної ситуації і прийняття свідомих рішень. У сучасних умовах специфіка інформаційно-аналітичної роботи полягає в забезпеченні особи, яка приймає рішення (управлінця), необхідною і достатньою кількістю аналітичної інформації для прийняття єдино правильного, ефективного в умовах непередбаченості і кризових явищ управлінського рішення.

Аналітиком є експерт в певній галузі знань, який володіє інтелектуальним інструментарієм та має широкий досвід практичної діяльності в деяких сферах. Аналітик професійно володіє комплексними методами застосування інтелектуальних технологій, які дають можливість виявляти основні тенденції їх розвитку, аналізувати та прогнозувати майбутні явища та процеси для створення ефективних управлінських рішень.

Важливу роль в діяльності спеціалістів, які виконують аналітичну роботу, відіграє їх підвищення кваліфікації та методологічного рівня, практичні навички в інформаційно-аналітичній роботі, використання ними інформаційних технологій, автоматизованих інформаційних систем та інформаційно-аналітичного інструментарію.

ПИТАННЯ ТА ЗАВДАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Необхідність інформаційної аналітики в правоохоронній діяльності.
2. Функції інформаційно-аналітичної діяльності.
3. Принципи інформаційно-аналітичної діяльності.
4. Призначення інформаційно-аналітичної роботи в правоохоронній діяльності.
5. Методи, які використовуються в інформаційно-аналітичній діяльності.
6. Різновиди інформаційно-аналітичної діяльності.
7. Етапи інформаційно-аналітичної діяльності.
8. Назвіть види аналізів інформаційних процесів і явищ, які є найпоширенішими.
9. Дайте характеристику основним методам збору інформації.
10. Дайте визначення таким поняттям як «прогноз» та «прогнозування». Їх відмінності.

ЛІТЕРАТУРА ЗА РОЗДІЛОМ:

1. Варенко В.М. Інформаційно-аналітична діяльність: Навч. посіб. / В. М. Варенко. – К.: Університет «Україна», 2014. – 417 с.
2. Інформаційно-аналітична діяльність [Електронний ресурс] : курс лекцій / укладач Шкіцька І.Ю. – Тернопіль : ТНЕУ, 2018. – Режим доступу: http://library.tneu.edu.ua/index.php/uk/nmkd/2638- 2013-12-19-10-42-55.
3. Палій С. Сучасні тенденції розвитку інформаційно-аналітичного забезпечення у контексті прийняття ефективних управлінських рішень (на прикладі органів державної влади України). Український журнал з бібліотекознавства та інформаційних наук. 2022. № 10. С. 166–174.
4. Бакуменко Р. Інформаційно-аналітичне забезпечення органів військового управління: стан, проблеми та підготовка фахівців. Військова освіта. 2019. № 1 (39). С. 8–16.
5. Бойко, Н. В. (2020). Інформаційно-аналітична діяльність органів місцевого самоврядування – важлива складова процесу прийняття управлінських рішень. Бібліотекознавство. Документознавство. Інформологія, (1), 65-71. Вилучено з: file:///C:/Users/bozhe/Downloads/bdi_2020_1_12.pdf.
6. Ганцюк Т. Д. Інформаційно-аналітичне забезпечення діяльності органів публічної влади в Україні: джерелознавчий аналіз дискурсного поля [Електронний ресурс] / Т. Д. Ганцюк // Електронне видання “Державне управління: удосконалення та розвиток”. № 8. 2018. Режим доступу: http://www.dy.nayka.com.ua/?op=1&z=1287.

Розділ 3
ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ ДІЯЛЬНОСТІ СУБ'ЄКТІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Інформаційно-аналітичне забезпечення в діяльності Національної поліції України посідає дуже важливе місце і є її організаційно-правовим та технічним комплексом. Засоби, які забезпечують збір, приймання, оброблення, поширення та використання інформаційних ресурсів при виконанні необхідних завдань та функцій правоохоронними органами, здійснюються за визначеним чинним законодавством.

У своїй роботі органи поліції використовують інформацію не тільки про безпекову та криміногенну ситуацію на певній території, але й інформацію про організацію роботи поліції, її підрозділи, засоби та їх сили призначення. Інспектори поліції, працівники чергових частин та оперативних підрозділів, дільничні інспектори під час своєї роботи створюють бази даних оперативно-розшукового призначення, які стосуються громадян, що мали злочини, правопорушення, були власниками вогнепальної зброї, зброї, яка була в розшуку, були власниками автотранспортних засобі, на яких вчинили кримінальний злочин чи угон та інше. Така інформація використовується працівниками різних підрозділів для своєчасного її опрацювання та прийняття ефективних необхідних засобів при боротьбі із злочинністю, її упередженням та зменшенням рівня злочинності і правопорушення у майбутньому.

3.1. Загальні поняття, визначення, основна мета та вимоги аналітичної роботи органів Національної поліції

Інформація – чи не головна цінність у сучасному світі. Через значні різновиди терміну «інформація» його єдиного визначення немає, але є багато різних думок.

Інформація – це:

– будь-які відомості, які приймаються і передаються, які зберігаються різними джерелами;

– значущі відомості про будь-що, коли форма їх подання також є інформацією;

– відомості, роз'яснення, виклад.

– дані або відомості, незалежно від форми їх подання, тощо.

Тож узагальнене поняття інформації (від лат. informatio – виклад, роз'яснення), в широкому сенсі це – відомості, що передаються одними людьми іншим усним, письмовим або будь-яким іншим способом, а також сам процес передачі або отримання цих відомостей.

У Законі України «Про інформацію» законодавець визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [3].

Інформація органів Національної поліції – це відомості, які показують стан злочинності та охорони громадського порядку, характеризують сили та засоби органів Національної поліції, способи і методи впливу на об'єкти управління, результати впливів, умови та прояви зовнішнього середовища, які впливають на стан та ефективність їх функціонування.

Інформаційні ресурси (Information resources) – документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, депозитаріях тощо). Інформаційні ресурси є суб'єктом аналітичної діяльності.

Аналітична діяльність – одна з областей людського мислення, метою якої є смислова обробка інформації для визначення якісно нових знань і підготовки основи для прийняття оптимальних управлінських рішень.

На підставі наведених понять можна зробити висновок, що інформаційно-аналітична діяльність – це специфічний різновид інтелектуальної, розумової діяльності людини, в процесі якої внаслідок певного алгоритму послідовних дій з пошуку, накопичення, зберігання, обробки, аналізу первинної інформації утворюється нова, вторинна аналітична інформація.

Інформаційно-аналітична діяльність здійснюється у всіх сферах державної діяльності. Процес аналітичної діяльності спрямований на вирішення практичних завдань. Він також носить прогностичний характер, дозволяючи випередити деякі явища і визначити майбутній стан об'єкта дослідження.

Інформаційно-аналітична робота – це окремий напрям управлінської діяльності в органах поліції, яку Національна поліція здійснює виключно для реалізації своїх повноважень, визначених Законом України «Про Національну поліцію України». Аналітична робота в органах Національної поліції – це постійна дослідна діяльність, що охоплює широкий комплекс організаційних заходів і методичних прийомів для вивчення і оцінки інформації про стан злочинності та

громадського порядку, результати практичної діяльності органів щодо виконання поставлених перед ними завдань, а також про умови, в яких ці завдання виконуються, і яка забезпечує цілеспрямоване управління та оцінку ефективності управляючих впливів.

Призначення аналітичної роботи полягає у вивченні закономірностей практично всіх процесів і явищ суспільного життя, які тією чи іншою мірою впливають на діяльність органів Національної поліції та у використанні здобутих відомостей і знань для забезпечення ефективності цієї діяльності. Аналітична робота служить засобом виявлення і оцінки значущості проблем, що виникають перед конкретною системою, формулювання її цілей, визначення об'єктивно необхідних функцій, обґрунтування структури та підвищення ефективності діяльності задля виконання поставлених завдань

Адміністративно-правове регулювання інформаційно-аналітичного забезпечення Національної поліції здійснюється в рамках Законів України «Про Національну поліцію України», «Про інформацію», «Про захист персональних даних», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», а також на підставі підзаконних нормативно-правових актів, зокрема Наказу Міністерства внутрішніх справ «Про затвердження Положення про контроль за станом технічного захисту інформації в органах і підрозділах Національної поліції України» № 139 від 29.02.2006 р. тощо.

Закон України «Про Національну поліцію України» у частині 2 статті 25 визначає, що поліція в рамках інформаційно-аналітичної діяльності формує бази (банки) даних, здійснює інформаційно-пошукову та інформаційно-аналітичну роботу, здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями.

Основними вимогами до аналітичної роботи в органах Національної поліції є:

– достовірність та повнота інформації, що використовується (відомості мають бути отримані з офіційних джерел);

– всебічність, системність та плановість інформації, коли дані, що аналізуються, охоплюють всі аспекти питання та відповідають дійсності;

– співставність – інформація, що підлягає аналітичній обробці, має відповідати певним спільним критеріям;

– комплексність – інформація повинна розглядатися без відриву від інших споріднених даних;

– комплексне використання різноманітних методів аналізу з метою уникнення прогалин або неточностей.

Основна мета аналітичної роботи органів Національної поліції:

- забезпечення безперервного спостереження за оперативною обстановкою і результатами службової діяльності; систематичне інформування органів влади та управління, керівництва МВС, ГУМВС, УМВС, УМВСТ про фактичний стан правопорядку і завдання органів Національної поліції щодо його зміцнення;

- своєчасне застосування заходів щодо посилення боротьби зі злочинністю та охорони громадського порядку (щоденне реагування);

- підвищення якісного рівня боротьби зі злочинністю та іншими правопорушеннями шляхом своєчасного і цілеспрямованого прийняття управлінських рішень на рівні керівництва МВС, УМВС, УМВСТ, їх галузевих служб та підрозділів на місцях (реалізація комплексних та перспективних завдань);

- підготовка змістовних матеріалів та пропозицій, на підставі яких можливе прийняття ефективних законодавчих актів з боку владних структур держави та органів місцевого самоврядування.

Напрями інформаційно-аналітичної роботи Національної поліції:

1. Робота щодо забезпечення повсякденного оперативного управління, що полягає у безперервному вивченні оперативної обстановки з метою вжиття своєчасних заходів з удосконалення організаційно-аналітичної роботи.

2. Дослідження інформації, яка надійшла до підрозділу за певний період, спрямована на вивчення відомостей, що надійшли протягом місяця, року чи іншого терміну, з метою встановлення динаміки штатних змін, стану штатної дисципліни тощо.

3. Планування та прогнозування подальшої роботи організаційно-аналітичних підрозділів, що полягає в дослідженні інформації задля визначення перспектив штатного забезпечення та штатної дисципліни.

При виконанні своїх службових обов'язків працівники різних підрозділів поліції накопичують широкий спектр інформації для своєчасного вжиття практичних заходів щодо боротьби зі злочинністю та правопорушеннями. Така інформація має бути надійно захищена та обмежена у доступі до сторонніх та третіх осіб.

Інформаційно-аналітичною діяльністю працівників поліції є:

- створення бази даних, яка належить до інформаційної системи МВС України;

- використання інформаційно-аналітичної роботи та інформаційно-пошукової діяльності;

- створення та використання баз даних МВС України, а також даних різних державних органів влади;

- проведення інформаційно-пошукової та аналітичної роботи;
- створення взаємодії щодо обміну інформацією з іншими органами державної влади, правоохоронними органами України та міжнародними організаціями.

Інформація, що отримується та використовується посадовими особами Національної поліції України, має бути систематизована для її подальшого використання. Тому поліція України впровадила в свою професійну діяльність автоматизовану інформаційно-аналітичну систему (АІС) для боротьби зі злочинністю. За допомогою автоматизованої інформаційної системи працівники інформаційної служби можуть систематизувати інформацію, постійно поповнювати базу даних новою інформацією, аналізувати існуючу та оновлювати її. Це дає можливість оперативно надавати необхідну інформацію за відповідним запитом у найкоротші терміни, що відповідає найголовнішій меті роботи підрозділів Національної поліції України при виконанні службових завдань та ефективної боротьби із злочинністю і різними правопорушеннями.

3.2. Автоматизовані інформаційні системи, що використовуються правоохоронними органами

Автоматизована інформаційна система (АІС) визначається як організаційно-технічна система, що реалізує технологію обробки інформації за допомогою технічних і програмних засобів.

Автоматизовані інформаційні системи, що використовуються правоохоронними органами у своїй діяльності, можна класифікувати наступним чином:

- АІС, які призначені для збору та обробки облікової, реєстраційної та статистичної інформації;
- АІС, які призначені для обробки інформації оперативного призначення;
- АІС, які використовуються для оперативно-розшукової діяльності;
- АІС, які використовуються для криміналістичного опрацювання інформації;
- АІС, що використовуються для експертної діяльності;
- АІС для адміністративного призначення.

Автоматизовані інформаційні системи за рівнем складності обробки інформації можуть мати певну класифікацію:

- автоматизовані інформаційно-довідкові системи (АІДС);
- автоматизовані системи управління (АСУ);
- автоматизовані робочі місця (АРМ);
- автоматизовані інформаційно-пошукові системи (АІПС);
- автоматизовані системи обробки даних (АСОД);
- експертні системи (ЕС), експертні консультаційні системи, а також системи підтримки прийняття управлінських рішень.

Відповідно до чинного Закону України "Про Національну поліцію" від 02.07.2025 №580-VIII, «Поліція здійснює інформаційно-аналітичну діяльність виключно для реалізації своїх повноважень, визначених законом». Засобами реалізації інформаційно-аналітичної діяльності є системи передачі даних та зв'язку, створення баз даних правової інформації, застосування інформаційно-телекомунікаційних технологій та інформаційних систем, використання правових, технічних, програмних, інформаційних та організаційних засобів.

Системою інформаційного забезпечення Національної поліції України є сукупність взаємодіючих та взаємопов'язаних технічних засобів та організаційних елементів, які здійснюють інформаційне забезпечення діяльності поліції України.

В основу системи інформаційного забезпечення поліції покладено формування галузевих та відомчих інформаційних підсистем, які функціонують за такими принципами:

- нормативно-правового забезпечення;
- достовірності даних;
- розширення та розвитку;
- функціонального призначення (слідчого призначення, оперативно-розшукового призначення, інформаційної підсистеми кримінального призначення, підсистеми розвідки, інформаційної підсистеми, що становить основу системи інформаційного забезпечення Національної поліції України).

Основним органом, відповідальним за формування інформаційної підсистеми поліції, є Департамент інформатизації Міністерства внутрішніх справ України. Відповідно до законодавства України та нормативно-правових актів центральних органів виконавчої влади, цей Департамент виступає структурним підрозділом апарату МВС, який здійснює та веде організацію, яка спрямована на інформаційно-аналітичне забезпечення правоохоронної діяльності в органах і підрозділах Міністерства внутрішніх справ України та захист персональних даних під час їх обробки.

Органом, який відповідає за формування розвідувальних ресурсів

національної поліції в регіонах, є Департамент інформаційно-аналітичного забезпечення (ДІАЗ). Він є структурним підрозділом обласних головних управлінь Національної поліції України (далі – ГУНП).

Департамент інформаційно-аналітичного забезпечення є структурним підрозділом Головного управління Національної поліції в області (ГУНП) і організовує та здійснює заходи, спрямовані на забезпечення правоохоронної діяльності поліції області.

Основними спрямуваннями його діяльності є:

- збір, обробка, зберігання та архівування статистичної, слідчої, оперативної, довідкової, криміналістичної та облікової інформації;
- організація створення, розвитку та експлуатації автоматизованих та інтелектуальних інтегрованих інформаційних систем;
- розробка корпоративної інформаційної мережі для обласних управлінь поліції;
- інформаційне забезпечення органів поліції, надання інформації фізичним та юридичним особам;
- облік правопорушників, скоєних злочинів, ведення кримінальної статистики злочинності;
- інформаційна підтримка органів поліції щодо зберігання та захисту ділової документації;
- впровадження сучасних інформаційних технологій та інформаційних систем у діяльність Головного управління поліції;
- підготовка національних та галузевих статистичних звітів про стан діяльності в області, регіоні та країні.

Оптимізація вирішення завдань пошуку, відбору та систематизації інформації, необхідної для діяльності поліції, є ключовим елементом системи МВС.

3.3. Інформаційний простір системи МВС України

Інформаційний простір системи МВС України можна визначити наступним чином. Він базується на побудові єдиного інформаційного простору системи МВС України, суб'єктів інформаційно-аналітичної діяльності, технології ведення та використання спеціалізованих баз даних, а також на інформаційно-комунікаційних системах та мережі банку даних, які мають єдиний принцип функціонування та побудови для забезпечення інформаційної взаємодії системи Міністерства внутрішніх справ України.

Інформаційно-аналітичне забезпечення є одним із засобів виявлення проблем, їх оцінювання та ефективності впроваджених в діяльність органів поліції змін. Із зростанням рівня злочинності в Україні у діяльності правоохоронних органів та в Національній поліції запроваджено сучасні інформаційно-аналітичні системи. Саме застосування сучасних технологій при виконанні інформаційно-аналітичної роботи мінімізує витрачений робочий час оперативного працівника та підвищує якість його роботи.

Інформаційно-аналітичне забезпечення є важливим елементом діяльності Національної поліції України, зокрема кримінального аналізу. Це включає організаційні, правові та технологічні засоби, які дозволяють збирати, обробляти, аналізувати та використовувати інформацію, необхідну для виконання завдань поліції, визначених законодавством.

Сучасне суспільство вимагає інформаційно-аналітичної діяльності як ключового чинника стабільності та життєздатності країни. Кримінальний аналіз полягає у виявленні та аналізі зв'язків між інформацією про злочини, їх виконавців і даними з різних джерел. Це дозволяє правоохоронним органам, прокуратурі та судам оцінити і використовувати цю інформацію для подальших дій. Основною метою кримінального аналізу є розробка нових підходів до ефективної слідчої роботи та досудового розслідування, а також поліпшення оперативно-розшукової та профілактичної діяльності у боротьбі зі злочинністю.

У сучасних умовах інформаційно-аналітична робота надає керівникам необхідну аналітичну інформацію для прийняття ефективних управлінських рішень в умовах нестабільності і кризових ситуацій. Вона допомагає передбачити наслідки рішень і виявити їх позитивні та негативні аспекти.

Під час проєктування та впровадження інформаційно-аналітичного забезпечення для кримінальної діяльності аналітик використовує показники для опису об'єкта аналізу, що є найефективнішим способом. Аналітичний супровід включає вимірювання показників, аналіз їх зміни та прогнозування їх значень, а також перевірку досягнення цільових показників. Така діяльність є важливою частиною інформаційно-аналітичного забезпечення кримінальної діяльності.

Інформаційні системи Департаменту інформаційно-аналітичного забезпечення Національної поліції України мають важливе значення, особливо при розслідуванні кримінальних справ в умовах недостатньої інформації, коли слідчим бракує достатніх даних для організації розслідування, виявлення слідів злочину, визначення осіб, залучених до вчинення злочину, та встановлення механізму злочину.

Підрозділи Департаменту інформаційно-аналітичного забезпечення керують роботою інформаційних систем для оперативного пошуку та надання інформації. Вони представлені територіальними відділами інформаційно-аналітичного забезпечення Головного управління Національної поліції, секторами інформаційно-аналітичного забезпечення та окремими співробітниками інформаційного забезпечення поліцейських органів в регіонах. Зазначені інформаційні системи розглядаються як автоматизовані бази даних, записи в яких стосуються певних об'єктів у різних базах даних окремих автоматизованих інформаційних систем. Інформація про ці об'єкти внесена в окремі електронні картки.

Інформаційні системи, засоби зв'язку та передачі даних, сучасна інформаційно-телекомунікаційна інфраструктура, бази даних щодо законодавства, технічні, програмні, лінгвістичні, правові та організаційні засоби є основними компонентами та інструментами для виконання інформаційно-аналітичної діяльності. Це визначено в статтях 25, 26 і 27 Закону України «Про Національну поліцію». Система інформаційного забезпечення Національної поліції України представляє собою збірну систему взаємопов'язаних і сумісних організаційних елементів та технічних засобів, які забезпечують необхідну інформаційну базу для Національної поліції України.

3.4. Використання інформаційних технологій (ІТ) в Національній поліції України

У сучасному світі інформаційні технології відіграють досить важливу роль у всіх сферах життя, включаючи правоохоронну діяльність. Інформаційні технології допомагають поліції у вирішенні багатьох завдань, таких як збір та аналіз даних, розслідування злочинів, підтримка громадського порядку та забезпечення безпеки. Проте використання інформаційних технологій в поліції завдають і певних труднощів, які виникають через те, що інформаційні технології можуть використовуватися для збору та зберігання величезних обсягів особистих даних, для автоматизованого прийняття рішень, що впливають на життя людей та для здійснення спостереження. Важливо зазначити, що ці питання є складними. Різні люди можуть мати несхожі думки. Тому важливо вести відкритий та чесний діалог з усіма зацікавленими сторонами, щоб знайти рішення, які б відповідали потребам суспільства.

Збір та аналіз даних є одними з найважливіших завдань, які виконує

поліція. Інформаційні технології допомагають поліції збирати дані з різних джерел, таких як записи про злочини, звіти про правопорушення, дані з камер відеоспостереження та інформація з соціальних мереж. Ці дані потім аналізуються для виявлення закономірностей, прогнозування злочинів та розслідування злочинів.

Використання інформаційних технологій відбувається під час збору та аналізу даних, при веденні відеоспостереження, при зберіганні особистих даних, використанні біометричних даних. Саме для забезпечення прозорості при зборі та аналізі даних має бути використано захист даних від несанкціонованого доступу, забезпечено контроль за надійним збереженням даних громадян. Використання інформаційних технологій для збору та аналізу даних повинно бути потужним інструментом для боротьби зі злочинністю та забезпечення безпеки, але лише за умови етичного та відповідального використання.

Штучний інтелект стає все більш потужним інструментом, який використовується в багатьох сферах, включаючи правоохоронну діяльність. Він може використовуватися для аналізу даних, розпізнавання образів, прогнозування злочинів та прийняття автоматизованих рішень. Проте використання штучного інтелекту в поліції спричинює й певні питання, які включають алгоритмічну упередженість та дискримінацію, автоматизоване прийняття рішень, що впливає на життя людей, відповідальність за помилки, допущені системами штучного інтелекту. Для вирішення цих питань важливо забезпечити прозорість та підзвітність систем штучного інтелекту, розробити методи виявлення та усунення упередженості в них, встановити чіткі правила щодо використання, а також забезпечити підзвітність за помилки, допущені цими системами.

Штучний інтелект може бути потужним інструментом для боротьби зі злочинністю та забезпечення безпеки, але лише за умови використання відповідного інструментарію. Тільки так ми зможемо захистити права та свободи громадян, а також забезпечити ефективну правоохоронну діяльність.

Розпізнавання облич є технологією, що дозволяє автоматично ідентифікувати або верифікувати особу на основі зображення або відео її обличчя. Ця технологія широко використовується в різних сферах, зокрема в правоохоронній діяльності, системах контролю доступу та спостереження. Серед переваг використання розпізнавання облич можна відзначити підвищення рівня безпеки, зокрема у здійсненні ідентифікації злочинців та терористів, а також у запобіганні проникненню несанкціонованих осіб на захищені об'єкти.

Також вона забезпечує зручність у процесі доступу до будівель, комп'ютерних систем та автоматизує такі завдання, як реєстрація в аеропортах. Крім того, розпізнавання облич допомагає у розслідуванні злочинів шляхом ідентифікації підозрюваних та свідків, а також у пошуку зниклих безвісти людей. Однак з використанням цієї технології пов'язані деякі питання. Наприклад, можливе вторгнення в приватне життя людей через відстеження їх активності без їхньої згоди. Також системи розпізнавання облич можуть бути неточними, що призводить до помилкових ідентифікацій та можливої дискримінації.

Існує ризик зловживання цією технологією для авторитарного контролю та придушення інакомислення. Для вирішення цих питань важливо встановити чіткі правила та норми використання розпізнавання облич, що базуються на принципах поваги до приватного життя, захисту даних від несанкціонованого доступу. Також необхідно забезпечити прозорість та підзвітність у використанні цих систем, захисту даних від зловживань. Громадяни повинні мати право на контроль над своїми даними, включаючи доступ, виправлення та видалення.

Кібербезпека є критично важливою сферою для правоохоронних органів в наш час, особливо коли інформаційні технології відіграють все більш важливу роль в їх роботі, а саме захисту поліцейських систем, даних та інформації від кібератак, які можуть призвести до крадіжки даних, втрати конфіденційності, порушення роботи систем та інших негативних наслідків. Загрози кібербезпеки для поліції включають втручання в слідство, оприлюдлення конфіденційних даних, дезінформацію та пропаганду, шантаж та вимагання, атаки на критичну інфраструктуру.

Втручання в слідство може призвести до зміни доказів та перешкоджати розслідуванню злочинів. Витоки даних становлять загрозу конфіденційності, включаючи особисту інформацію та дані про злочини. Дезінформація та пропаганда можуть підірвати довіру громадян до поліції, а шантаж може виникнути через зашифрування даних та вимагання викупу.

Атаки на критичну інфраструктуру можуть призвести до перешкод у роботі систем зв'язку та управління поліції. Для забезпечення кібербезпеки поліція повинна застосовувати заходи захисту мереж та систем, навчати персонал кібербезпеці, регулярно резервно копіювати дані та співпрацювати з іншими організаціями. Ефективна кібербезпека дозволяє захищати конфіденційні дані, підтримувати ефективність розслідувань, зберігати довіру громадян та запобігати збоям у роботі систем.

Використання технологій відстеження у правоохоронній діяльності стає все більш поширеним явищем. Ці технології можуть використовуватися для відстеження пересування людей, їхньої онлайн-активності та інших аспектів їхнього життя. GPS-трекери дозволяють відстежувати пересування людей в режимі реального часу при умові, якщо їх встановити на транспортних засобах, носіях або вмонтувати в мобільні телефони.

Технологія розпізнавання облич ідентифікує людей за зображеннями або відео їхніх облич, використовуючи це для відстеження у натовпі, моніторингу громадських місць або розслідування злочинів. Відстеження мобільних телефонів дозволяє отримувати дані про місце перебування абонентів та їх комунікаційні записи.

Онлайн-відстеження включає в себе аналіз трафіку, використання файлів cookie та моніторинг соціальних мереж для відстеження активності осіб. Використання цих технологій має свої переваги. Вони допомагають у запобіганні злочинам шляхом ідентифікації підозрюваних та відстеження їхніх рухів, розслідуванні злочинів за допомогою збору доказів та ідентифікації свідків, пошуку зниклих безвісти осіб, а також захисту вразливих груп.

Однак використання цих технологій спричинює порушення права на приватне життя через вторгнення у приватність та можливість неправильного використання даних, що може призвести до помилкових рішень та зловживання владою. Для вирішення цих питань важливо встановлювати чіткі правила та норми використання технологій відстеження, які базуються на принципах поваги до приватного життя, захисту даних та недопущення дискримінації. Також необхідно забезпечувати прозорість та підзвітність у використанні цих технологій, захищати дані від несанкціонованого доступу та забезпечувати громадянам контроль над своїми особистими даними.

Дрони, також відомі як безпілотні літальні апарати, стають все більш потужним інструментом, який використовується в правоохоронній діяльності. Їх можна використовувати для різних цілей, таких як спостереження та розвідка, пошук і рятування, переслідування злочинців, знешкодження вибухівки та контроль трафіку. Використання дронів має свої переваги, такі як підвищена безпека, розширені можливості спостереження, підвищена ефективність та зниження витрат. Однак воно також породжує такі питання, як вторгнення в приватне життя, неточність даних та зловживання. Тому мають бути вирішені питання щодо встановлення чітких правил та норм використання дронів, які базуються на принципах поваги до приватного життя, захисту даних

та конфіденційності. Забезпечення прозорості використання цих технологій, захисту даних від несанкціонованого доступу, а також забезпечення контролю за існуючими даними громадян має бути застосовано для виконання ефективної правоохоронної діяльності.

Використання інформаційних технологій (ІТ) в поліції є потужним інструментом для боротьби зі злочинністю та забезпечення безпеки. Але питання застосування інформаційних технологій в поліції містять втручання в приватне життя, неточність та упередженість даних, зловживання владою та питання відповідальності за шкоду, завдану внаслідок використання ІТ-систем. Для розв'язання цих проблем мають бути застосовані певні чіткі правила та норми використання інформаційних технологій в поліції, які базуються на принципах поваги до приватного життя, захисту персональних даних та конфіденційності.

Побудова безпечного інформаційного простору із застосуванням інформаційних технологій в правоохоронній діяльності є важливим завданням для України під час воєнного стану, після його завершення, розвитку та відбудови країни у майбутньому.

Розглядаючи структуру інформаційно-аналітичної діяльності, необхідно вказати, що вона містить інформаційне забезпечення, інформаційно-аналітичну обробку, створення баз даних, включаючи інформаційно-пошукові, та методи їх використання. Оптимізація процесів пошуку, відбору та систематизації інформації, необхідної для діяльності поліції, ґрунтується на структурі єдиного інформаційного простору системи Міністерства внутрішніх справ України. Ця система включає спеціальні бази даних та банки даних, технології їх управління та використання, інформаційно-телекомунікаційні системи та мережі, підрозділи інформаційно-аналітичної діяльності, які функціонують на єдиних принципах і відповідно до загальних правил, забезпечуючи інформаційний обмін між системою Міністерства внутрішніх справ України та громадянами.

Таким чином, для вирішення сучасних питань щодо здобуття високого рівня діяльності правоохоронних органів та застосування належного інформаційного забезпечення підрозділів поліції, необхідно провести його комплексний аналіз шляхом створення багатоцільової системи інформаційного забезпечення, удосконалення кадрового та організаційного забезпечення інформаційних підрозділів, налагодження взаємодії між поліцією та громадськістю, забезпечення надійного захисту персональних даних, збереження та опрацювання інформації, захисту від несанкціонованого доступу та витоку інформації, інтеграція та систематизація інформаційних обліків на всіх рівнях, забезпечення

цілісності, надійності, достовірності та безпеки інформаційних обліків, встановлення сучасної та потужної комп'ютерної техніки в інформаційній сфері.

ПИТАННЯ ТА ЗАВДАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Дайте визначення автоматизованим інформаційним системам.
2. Що собою представляє інформаційний простір системи МВС України?
3. Що є основними напрямами діяльності інформаційно-аналітичного забезпечення Національної поліції України?
4. Класифікація автоматизованих інформаційних систем в правоохоронній діяльності.
5. Особливості інформаційно-аналітичної діяльності працівників поліції.
6. Назвіть автоматизовані інформаційні системи, які використовуються під час обробки інформації в правоохоронній діяльності.
7. Яке основне призначення працівників поліції при виконанні інформаційно-аналітичної діяльності?
8. Що собою являє інформаційний простір системи МВС України?
9. Назвіть найпоширеніші види аналізів інформаційних процесів і явищ.
10. Охарактеризуйте основні методи збору інформації.
11. Назвіть типові помилки при написанні та оформленні аналітичної роботи.

ЛІТЕРАТУРА ЗА РОЗДІЛОМ:

1. Про Національну поліцію: Закон України від 02.06.2014 р. № 580-VIII. Дата оновлення: 16.08.2024. URL: https://zakon.rada.gov.ua/laws/show/580-19#Text (дата звернення: 04.10.2024).
2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення: 27.07.2023. URL https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 04.10.2024).
3. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. Дата оновлення: 27.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text t (дата звернення: 04.10.2024).
4. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 04.10.2024).
5. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.06.1994 р. № 80/94-ВР. Дата оновлення: 28.06.2024. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 04.10.2024).

Розділ 4
ЗАХИСТ ІНФОРМАЦІЇ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

4.1. Методи захисту інформації

Система управління інформаційною безпекою ґрунтується на трьох фундаментальних принципах управління:

• принцип розімкнутого керування;

• принцип компенсації;

• принцип зворотного зв'язку.

За принципом розімкнутого управління створюються власні політики безпеки, виконання яких контролюється відповідальними особами. Зараз більшість компаній виділяє для особи, відповідальної за розробку і реалізацію політик ІБ, позицію CISO (Chief Information Security Officer) – керівника відділу IT-безпеки або директора з IT-безпеки. Переважно CISO очолює керуюча рада з питань ІБ.

Принцип компенсації означає, що якщо є будь-яке відхилення від встановленої політики безпеки або зовнішніх факторів (з’явилися нові загрози, нові співробітники приходять і полишають роботу, з’явилися нові програмні продукти), необхідно вжити відповідних заходів для поточного коригування алгоритму управління з метою компенсації негативних наслідків зовнішнього впливу.

Тому для вашого підприємства важливо не тільки аналізувати інциденти, які вже відбулися, але й створювати системи активного захисту, здатні протистояти атакам до виникнення проблем і навіть до доведення яскравих проблем і вразливостей.

Важливо дотримуватися принципу зворотного зв'язку, що дозволяє управляти ІБ у замкнутому циклі. За цим принципом створено багато систем ІБ.

Наявність зв’язків зворотного зв’язку в системах управління інформаційною безпекою не тільки виявляє окремі загрози, але й реагує на багато подій, які, на перший погляд, не пов’язані між собою. Продукти, які забезпечують централізоване відображення даних журналу подій від мережевих пристроїв і системи безпеки в режимі реального часу, можуть допомогти досягти цього, автоматично відображаючи дані

та висвітлюючи події та загрози безпеки, які вимагають рішучих дій, наприклад Check Point Eventia Analyzer.

Побудова системи ІБ з урахуванням перерахованих принципів дозволяє використовувати існуючі методи оптимізації для підвищення різноманітних показників якості системи, таких як стійкість управління, швидкість реакції на існуючі та невідомі загрози.

Розробка комплексу організаційних засобів захисту інформації повинна належати до компетенції служби безпеки.

Експерти з безпеки повинні:

- розробити внутрішні документи, що встановлюють правила використання комп'ютерної техніки та конфіденційної інформації;
- навчання та регулярні перевірки персоналу, ініціювання підписання додаткового договору до трудового договору, які передбачають відповідальність за розголошення або неправомірне використання інформації, яка стала відомою під час роботи;
- розмежувати зони відповідальності, щоб усунути ситуацію, коли один співробітник має доступ до визначених наборів даних, організувати роботу в загальній програмі управління документами та переконатися, що критичні файли не зберігаються поза мережевими дисками;
- впроваджувати програмні продукти, які захищають дані від копіювання або знищення будь-яким користувачем, включаючи вище керівництво організації;
- розробляти план відновлення системи, якщо вона з будь-якої причини виходить з ладу.

Якщо компанія не має спеціалізованих ІТ-служб, рішенням буде залучено експертів із безпеки на аутсорсинг. Ці співробітники проводять аудит ІТ-інфраструктури компанії та дають їй рекомендації щодо захисту від зовнішніх і внутрішніх загроз. Крім того, ІТ-аутсорсинг використовує спеціальні процедури захисту інформаційної компанії.

На практиці використовується кілька груп методів захисту, серед яких:

- Створювати перешкоди на шляху ймовірного викрадання фізичними та програмними засобами;
- Керувати або впливати на захищені елементи системи;
- Дані традиційно маскуються або перетворюються за допомогою шифрування;
- Регулювати інноваційно-правові акти та комплекс заходів, спрямованих на стимулювання відповідної поведінки користувачів, які взаємодіють нормативно з базою даних;

• Застосовувати або створювати умови, які змушують користувачів використовувати правила обробки даних;

• Мотивація користувачів до відповідних дій або створення умов для таких дій.

Кожен метод захисту інформації реалізується за допомогою різних категорій засобів. Основними інструментами є організаційні та технічні засоби.

Правила інформаційної безпеки – це внутрішні документи організації, які враховують бізнес-процеси, інформаційну інфраструктуру та архітектуру системи.

Інформація може бути захищена від несанкціонованого доступу апаратними, програмними, біометричними, технічними та адміністративними засобами.

Апаратне та програмне забезпечення:

- може шифрувати інформацію, створювати цифрові підписи та автентифікувати користувачів (автентифікація – це процес ідентифікації користувача, пристрою або іншої одиниці, що бере участь в обміні інформацією, до того, як необхідно отримати дозвіл на доступ до даних);

- смарт-картки – це магнітні картки для зберігання приватних ключів і шифрування паролів;

- пристрої ActivCard для введення паролів (паролі обчислюються без введення (динамічні паролі)) та SmartReader для зчитування паролів; ці пристрої містять мікропроцесор і зберігають секретний код. Введений користувачем пароль (чотири цифри) перераховується комп'ютером і створюється спеціальний код.

Програмні заходи:

• вбудовані у програми функції захисту даних. Наприклад, система Netware після трьох спроб користувача ввійти в мережу з неправильним паролем блокує ідентифікатор цього користувача, і тільки адміністратор мережі має змогу розблокувати доступ;

• спеціальні криптографічні розробки. За принципом побудови існуючі засоби захисту інформації, в яких використовуються криптографічні методи захисту, можна поділити на два типи:

• засоби, в основі роботи яких лежать симетричні алгоритми для побудови ключової системи і системи аутентифікації;

• засоби, основу роботи яких складають асиметричні алгоритми, що застосовуються для тих самих цілей.

У засобах першого типу обов'язковою є наявність центру розподілу ключів, що відповідає за їх створення, розповсюдження та вилучення. При цьому носії ключової інформації передаються абонентам із

використанням фізично захищених каналів зв'язку. Ключі повинні змінюватися досить часто, кількість абонентів має бути значною, тому ці засоби негнучкі та дорогі. Питання аутентифікації вирішується довір'ям користувачів один одному, цифровий підпис неможливий. Центр розподілу ключів контролює всю інформацію. Захист інформації дуже низький.

У засобах другого типу ключі для шифрування автоматично генеруються, розповсюджуються і вилучаються для кожного сеансу зв'язку. Функції служби розповсюдження ключів виконує сертифікаційний центр, де користувач реєструється, встановлюється його аутентифікація, після чого ключі вилучаються. В таких засобах можливими є організація цифрового підпису та його перевірка. Протокол установлення аутентичного зв'язку відповідає певному стандарту. Аутентифікація є простою та суворою. При простій аутентифікації відбувається обмін паролями між абонентами, які встановили зв'язок, із подальшою перевіркою відповідності цих паролів еталонним. При суворій аутентифікації кожен абонент має два криптографічних ключі – секретний, відомий тільки даному абоненту, та відкритий – той, що передається в банк. Використовуючи секретний ключ і спеціальний алгоритм, абонент формує цифровий підпис – послідовність бітів, яка однозначно відповідає документу, що підписується. Перевірка відповідності підпису виконується за допомогою відкритого ключа.

Біометричні засоби:

- візерунки сітчатки ока;
- відбитки пальців;
- геометрія руки;
- динаміка підпису.

Адміністративні заходи:

• системи електронних перепусток для персоналу і відвідувачів;

• системи відеоспостереження та відеореєстрації, що дають змогу вести цілодобовий візуальний нагляд як за периметром об'єкта, так і всередині з можливістю запису інформації на відеомагнітофон або комп'ютер;

• розподіл доступу до інформації. Тут необхідним є чітке визначення осіб, які мають право на ту чи іншу інформацію. Наприклад, програмісти не повинні мати доступу до БД, а користувачі – до програмного забезпечення;

• систематичний аналіз мережевого протоколу роботи, блокування спроб введення паролів кілька разів;

• ретельний підбір співробітників, навчання, стажування,

тренування. Кандидат повинен мати задовільні свідоцтва й атестати з попередніх робочих місць, не мати нахилу до зловживання наркотиками та алкоголем, не мати вагомих заборгованостей, не виявляти доброзичливості до наймачів.

Технічні заходи. Їх можна поділити на такі групи:

1) заходи захисту від прослуховування, що включають:

– встановлення фільтрів на лініях зв'язку; ·

– обстеження приміщень для виявлення підслуховуючих пристроїв;

– використання звукопоглинаючих стін, стелі, підлоги;

– застосування систем віброакустичного й акустичного зашумлення для захисту мовної інформації від прослуховування за допомогою акустичних мікрофонів, стетоскопів, лазерних та інфрачервоних систем відбору інформації;

2) заходи захисту від електромагнітного випромінювання, куди входять:

– використання оптоволоконного кабелю;

– застосування захисної плівки на вікнах;

– користування захищеними дисплеями;

– заходи захисту від поновлення вилучених даних.

Кожен спосіб захисту інформації реалізується за допомогою різних категорій заходів.

Найважливішими заходами є **організаційно-технічні.**

Правила забезпечення інформаційної безпеки – внутрішня документація організації, яка враховує деталі бізнес-процесів та інформаційної інфраструктури, а також архітектуру системи.

Захистити інформацію від несанкціонованого доступу можливо за допомогою апаратно-програмних, програмно-біометричних, технічних та адміністративних заходів.

Апаратні та програмні засоби:

• Спеціальна карта шифрування, вбудована в комп’ютер, яка може використовуватися для шифрування інформації, створення електронних підписів та автентифікації користувачів (автентифікація – це процес ідентифікації користувачів і пристроїв).

• SmartCard – магнітна карта для зберігання закритих ключів і шифрування паролів та пристрій ActivCard для введення пароля.

Пароль обчислюється, а не вводиться (динамічний пароль).

Ви також можете використовувати SmartReader для читання паролів.

Ці пристрої містять мікропроцесор із секретним кодом, що

зберігається у його внутрішній пам’яті.

Введений користувачем пароль (4 цифри) буде перераховано комп'ютером і буде створено спеціальний код.

Програмні заходи:

• Функції захисту даних інтегровані в програму.

Наприклад, якщо користувач намагається увійти в мережу три рази з неправильним паролем, система Netware блокує особу цього користувача. І лише адміністратор мережі може розблокувати доступ.

• Розробка спеціальної криптографії.

За принципами проєктування існуючі засоби захисту інформації з використанням методів криптографічного захисту можна розділити на два типи:

• Засоби на основі симетричних алгоритмів для побудови ключових систем і систем аутентифікації.

• Інструменти, засновані на асиметричних алгоритмах і використовуються з тією ж метою.

Для першого типу інструментів обов’язковим є створення центрального розподільчого центру, відповідального за їх створення, розповсюдження та збір.

При цьому носії важливої інформації передаються учасникам через фізично захищені канали зв'язку.

Ці інструменти є негнучкими та дорогими, оскільки ключі потрібно часто змінювати, а кількість абонентів має бути значною.

Проблеми автентифікації вирішуються, коли користувачі довіряють один одному.

Цифрові підписи неможливі. Центр розподілу ключів керує всією інформацією. Захищеність інформації дуже низька.

Другий тип інструменту автоматично генерує, розповсюджує та витягує ключі шифрування для кожного сеансу зв’язку.

Функції служби розповсюдження ключів виконує центр сертифікації, який реєструє користувачів, аутентифікує їх, а потім отримує їхні ключі.

Такі інструменти дозволяють упорядковувати та перевіряти цифрові підписи.

Протоколи встановлення автентифікованих з’єднань відповідають певним стандартам.

Сертифікація проста і складна. Проста автентифікація передбачає обмін паролями між учасниками, які встановили з’єднання, і перевірку відповідності цих паролів контрольному паролю.

При надійній автентифікації кожен учасник має два ключі

шифрування. Один – це приватний ключ, відомий лише цьому учаснику, а інший надсилається до банку.

Використовуючи особистий ключ і спеціальний алгоритм, абонент створює цифровий підпис – послідовність бітів, яка однозначно відповідає документу, що підписується.

Перевірка підпису здійснюється за допомогою відкритого ключа.

Заходи біометричної автентифікації:

• малюнок сітківки;

• відбиток пальця;

• форма руки;

• характеристика динаміки підпису.

Заходи адміністративного впливу:

• система електронних ідентифікаційних карт для персоналу та відвідувачів;

• система відеоспостереження та відеореєстрації.

Це дає змогу 24 години на добу візуально спостерігати як за оточенням, так і за внутрішнім простором об’єкта та записувати інформацію на відеореєстратор або комп’ютер.

• Розподіл доступу до інформації.

Тут потрібно чітко визначити, хто має право на конкретну інформацію. Наприклад, програмісти не можуть отримати доступ до баз даних, а користувачі – до програмного забезпечення.

• Систематично аналізуйте мережеві протоколи та блокуйте численні спроби введення пароля.

• Ретельний відбір співробітників, навчання, стажування, навчання.

Кандидати повинні мати достатні повноваження та рекомендації з попередніх місць роботи, не схильні до зловживання наркотиків або алкоголю, не повинні мати великих боргів і, зокрема, перед роботодавцем.

Технічні заходи.

Їх можна класифікувати на такі групи:

1) Заходи проти прослуховування, включаючи:

– встановлення фільтрів на лініях зв’язку;

– огляд приміщень для виявлення засобів підслуховування;

– використання звукопоглинальних матеріалів.

4.2. Засоби організації захисту інформації

На чолі систем управління інформаційною безпекою стоїть директор з інформаційної безпеки (ІБ), який очолює комітет з управління ІБ – орган високого рівня, призначений для вирішення стратегічних питань, пов'язаних із забезпеченням ІБ.

Директор з ІБ відповідає за всі процеси управління ІБ, включаючи: управління інцидентами та моніторинг безпеки, управління змінами та моніторинг безпеки, інфраструктуру безпеки (політики, стандарти, інструкції, процедури, плани та програми), управління ризиками, контроль відповідності вимогам, навчання (програми обізнаності).

Створення подібної структури управління є метою впровадження ISO 27001/17799 в організації.

Одним із основних принципів тут є «залучення лідерства».

Це означає, що таку структуру може створити тільки керівництво підприємства, яке розподіляє посади, відповідальність і контролює виконання функцій.

Іншими словами, керівництво організації створює відповідну вертикаль влади, точніше, коригує існуючу владу для задоволення потреб організації в безпеці.

ISMS можна створити лише зверху вниз.

Ще одним базовим принципом є залучення до процесу доставки ІБ усіх співробітників організації, що працюють з інформаційними ресурсами, «від директора до прибиральниці».

Брак знань про конкретних людей, які працюють з інформацією, відсутність програм навчання ІБ є основними причинами несправності конкретних систем управління.

Не менш важливо, щоб оцінка ризиків була основою кожного плану ІБ.

Відсутність процесів управління ризиками в організації призводить до прийняття неадекватних рішень і необґрунтованих витрат. Тобто оцінка ризику є основою для побудови тонкого дерева СУІБ.

Не менш фундаментальним принципом є «впровадження та підтримка WSIS своїми руками».

У багатьох випадках залучення зовнішніх консультантів на всіх етапах впровадження, експлуатації та вдосконалення СУІБ має сенс.

Крім того, це один із механізмів керування, описаних у стандарті ISO 17799.

Однак створення СУІБ зовнішніми консультантами неможливе, оскільки СУІБ – це набір організаційних структур, сформованих керівництвом організації, і процесів, які впроваджує персонал організації-виконавця, є повністю поінформованими щодо своїх обов'язків та набувають інформаційних навичок.

ISMS коштує багато грошей, але за будь-які кошти не можна купити досвід і знання.

Використання системного підходу дозволить уникнути зайвих витрат на подальший розвиток або навіть повну перебудову системи захисту інформації в майбутньому.

Побудова фінансових і математичних моделей системи ІБ, оцінка загроз і їх наслідків, класифікація інформації, облік активів – все це необхідно використовувати в процесі розробки систем інформаційної безпеки.

Точна оцінка ризиків дозволяє значно скоротити витрати на захист інформації. Існує багато рекомендацій і документів, що регламентують побудову систем захисту інформації.

Можливість централізованого управління є найважливішою умовою для ефективної та безперервної роботи IT-системи. Наприклад, технологія Check Point SMART, яка реалізує централізоване управління, дозволяє легко керувати навіть найскладнішими системами, значно скорочуючи як витрати на управління, так і кількість помилок, які допускають співробітники.

Використання «клаптевого» підходу до побудови інформаційної системи з часом зробить її важкою в управлінні, погано контрольованою та просто марною.

Система управління інформаційною безпекою є частиною загальної системи управління, яка базується на аналізі ризиків і призначена для розробки, впровадження, контролю, моніторингу та вдосконалення заходів у сфері безпеки конфіденційної інформації.

Система включає організаційну структуру, політику, планування дій, відповідальність, процедури, процеси та ресурси.

Основними цілями інформаційної безпеки є:

• *інформаційна безпека*, тобто необхідно ввести обмеження доступу до цієї інформації для певної групи осіб;

• *неможливий несанкціонований доступ до інформації*, тобто знання конфіденційної інформації третіх осіб;

• *цілісність інформації* та пов'язані з нею процеси (генерація, збір, обробка та вихід), включаючи її існування в неспотвореному вигляді (незмінному від фіксованого стану);

• *доступність інформації*, тобто можливість забезпечити швидкий і безперешкодний доступ людей до інформації, що їх цікавить;

• *мінімізувати ризики*, пов'язані з інформаційною безпекою, шляхом впровадження компенсаційних заходів;

• *облік усіх процесів, пов'язаних з ризиками*.

Досягнення поставлених цілей здійснюється в процесі вирішення наступних завдань:

• впровадження умов інформаційної безпеки в систему;

• класифікація джерела інформації компанії;

• визначення власника процесу, відповідального за інформаційну безпеку;

• еволюція ризиків, пов'язаних з інформаційною безпекою та їх експертиза.

Види порушень

Організаційно-правові порушення – це порушення, пов'язані з відсутністю єдиної політики підприємства у сфері захисту інформації, з недотриманням вимог нормативних документів, способів доступу, зберігання та знищення інформації.

Типи організаційних порушень включають неавторизований доступ до баз даних і таблиць даних, неавторизований доступ до активного мережевого обладнання, серверів, неправильну інтеграцію засобів захисту та помилку в управлінні, порушення адреси надсилання інформації під час обміну інформацією.

Види фізичного злому – пошкодження апаратних засобів автоматизованих систем, ліній зв'язку та засобів зв'язку, викрадення або несанкціонований доступ до вмісту носіїв інформації, їх викрадення.

До видів радіоелектронних порушень відносяться використання засобів блокування електронної інформації, збирання інформації шляхом перехоплення та декодування інформаційних потоків, створення скріншотів, нав’язування неправдивої інформації в локальних комп’ютерних мережах, лініях електропередачі та передачі даних.

Для боротьби із загрозами та запобігання порушенням у компаніях організовано процес управління ризиками, який є основою системи інформаційної безпеки компанії.

Побудова ефективної системи інформаційної безпеки є складним процесом, який мінімізує зовнішні та внутрішні загрози з урахуванням ресурсних і часових обмежень.

З точки зору процесного підходу, систему інформаційної безпеки підприємства можна візуалізувати як процес управління ризиками (рис. 5.2), що складається з наступних компонентів.

1. Опис бізнес-процесів.

Проводиться налагодження та аналіз бізнес-процесів.

Ідентифікація бізнес-процесів здійснюється за критеріями, визначеними при розробці політики ризиків.

2. Відшкодування ризику.

Виконується для визначення вразливості компанії до загроз, які можуть завдати значної шкоди.

Для цього було проведено аналіз бізнес-процесів та опитування експертів галузі. Результатом (виходом) цього процесу вважається класифікований список усіх потенційних ризиків.

До стандартних ризиків інформаційної безпеки відносяться:

- видалення конфіденційної інформації з сайту;
- навмисна фальсифікація інформації з метою її знищення;
- копіювання критично важливих документів і передача їх конкуренту;
- несанкціонований доступ до мережі компанії;
- несанкціоноване вторгнення в мережу компанії;
- знищення з технічних причин.

3. Оцінка ризиків.

Визначаються характеристики ризиків та ресурси інформаційної системи. Основним результатом (виходом) цього процесу є перелік усіх потенційних ризиків, кількісна та якісна оцінка їх шкоди та ймовірності реалізації, а також додатковий перелік ризиків, які не контролюються підприємством.

Процес оцінки ризиків складається з таких етапів:

- опис об'єкта та заходів захисту;
- ідентифікація ресурсів та визначення кількісних показників;
- аналіз загроз інформаційній безпеці;
- оцінка вразливостей;
- оцінка існуючих та запропонованих заходів захисту інформації.

4. Планування заходів протидії.

Метою планування заходів з мінімізації ризиків є визначення термінів і переліку завдань для усунення або мінімізації збитків при мінімізації ризику.

Заходи інформаційної безпеки можуть бути наступних типів:

- організаційні;
- правові;
- організаційно-правові та технічні;
- програмні;
- технічні.

5. Реалізація заходів.

Реалізація заходів з мінімізації ризиків означає виконання запланованих робіт, контроль якості результатів і термінів. Результатами цього процесу є виконана робота з мінімізації ризиків і час, витрачений на це.

6. Оцінка ефективності.

Оцінка ефективності системи управління інформаційною безпекою – це систематичний процес отримання та оцінки об'єктивних даних про поточний стан системи, дії та події, що відбуваються в системі, та встановлення відповідності визначеним критеріям.

Цілями цього процесу є:

- оцінка поточного рівня ефективності системи;
- виявлення вузьких місць у системі;
- оцінка відповідності системи підприємства існуючим стандартам інформаційної безпеки;
- розробка рекомендацій та правил для забезпечення безпеки об'єктів, які захищають.

Результати цього процесу можуть бути використані для аудиту при підготовці до сертифікації за стандартом ISO/IEC 27001:2005.

4.3. Технічні системи захисту даних

Системи захисту інформації, що обробляється технічними засобами, повинні базуватися на певних принципах. Це викликано необхідністю протидії низці загроз інформаційній безпеці.

Основним принципом протидії загрозам інформаційній безпеці є превентивний характер захисних заходів. Це пов'язано з тим, що усунення наслідків загроз вимагає значних фінансових, часових і матеріальних витрат.

Наступним основним принципом протидії загрозам є диференціація заходів захисту інформації відповідно до їх важливості, а також частоти та ймовірності виникнення загроз безпеці.

Принцип протидії загрозам також включає в себе принцип достатності заходів інформаційної безпеки, що забезпечує ефективний захист без надмірного ускладнення системи інформаційної безпеки.

Протидія загрозам інформаційній безпеці завжди є невигідною для користувачів та обслуговуючого персоналу автоматизованих систем через накладені організаційні та технічні обмеження. Тому одним із принципів протидії загрозам є принцип максимальної зручності систем

захисту інформації. При цьому слід враховувати сумісність системи, що створюється для протидії загрозам інформаційній безпеці, з операційною структурою, апаратно-програмним складом автоматизованої системи та усталеними традиціями установи.

Важливість реалізації цього принципу ґрунтується на тому, що доповнення функціонуючої незахищеної автоматизованої системи засобами захисту інформації є більш складним і витратним процесом, ніж початкове проєктування і побудова захищеної системи.

З принципу декомпозиції механізмів впливу загроз інформаційній безпеці випливають принципи самозахисту та конфіденційності систем захисту інформації. Реалізація цих принципів дозволяє контролювати цілісність системи інформаційної безпеки, управляти безпекою за допомогою менеджерів безпеки і відновлювати систему безпеки в разі порушення або виходу з ладу обладнання.

Інструменти інформаційної безпеки, які зараз доступні на ринку, можна поділити на кілька груп:

- активні та пасивні технічні заходи, які забезпечують захист від витоку інформації за різними фізичними параметрами, що виникають при використанні засобів обробки інформації;

- програмно-апаратні засоби, які розмежовують різні рівні доступу до інформації, ідентифікують та аутентифікують користувачів;

- програмно-технічні засоби, що гарантують захист інформації та перевірку її автентичності при передачі каналами зв'язку;

- програмно-технічні засоби, що забезпечують цілісність програмних продуктів та захист від несанкціонованого копіювання;

- програмні засоби, які забезпечують захист інформації від впливу вірусів та іншого шкідливого програмного забезпечення;

- фізичні та хімічні засоби захисту, що забезпечують автентичність документів, безпеку при транспортуванні та захист від копіювання.

Інша категорія – загальносистемні захищені програмні продукти, які виключають можливість використання задекларованих програмних функцій. Таких систем існує ще не так багато.

До цієї ж категорії відносяться і спеціалізовані пристрої, такі як брандмауери для захисту корпоративних мереж від вторгнення з глобальних інформаційних мереж, таких як Інтернет.

Наразі засоби і системи захисту інформації та перевірки автентичності інформації, що передається каналами зв'язку, зокрема шифрувальні пристрої, виробляє велика кількість зарубіжних компаній.

Для захисту конфіденційної інформації, що передається каналами зв'язку, можуть використовуватися скремблери та пристрої шифрування,

наприклад, Thomson-CSF (Франція), яка випускає голосові скремблери типу TRC769, що захищає телефонні канали шляхом сортування за частотою і часом зі змінним вікном. Пристрої компаній Simens (Німеччина) та Grundy & Pirtners (Великобританія) призначені для захисту конфіденційної інформації в каналах бездротових систем зв'язку.

Наприклад, шифрувальні пристрої ScaNet компанії Dowty Network Systems (Великобританія) і шифрувальні пристрої Datacryptor-64 компанії Racal Datacom (США) призначені для користувачів мереж з комутацією пакетів за протоколом X.25 ICCTT; компанія NFT Ltd (Норвегія) розробила лінійку криптографічних модулів зі швидкістю до 10 Мбіт/с для потокового шифрування і використання в локальних мережах; компанія Xerox (США) розробила Xerox Encription Unit – високоякісний пристрій шифрування даних, який захищає інформацію з обмеженим доступом в локальних мережах.

Розроблено Encription Unit; PE Systems (США) надає систему GILLAROO для передачі та захисту секретної інформації, що передається мережами та каналами зв'язку з цифровим підписом; Calmes Semiconductor (США) розробила систему GILLAROO для передачі та захисту таємної інформації, що передається мережами та каналами зв'язку; Calmes Semiconductor (США) розробила систему GILLAROO для блочного шифрування на швидкостях до 300 Кбіт/с і виробляє криптопроцесор SL34C168, який виконує блочне шифрування на швидкостях до 300 Кбіт/с. Нещодавно були запропоновані нові криптографічні алгоритми для шифрування потоків до 1 Гбіт/с, такі як NEWDES і FEAL.

Останніми роками на ринку програмно-апаратних засобів захисту інформації все більшої популярності набувають системи запобігання несанкціонованому копіюванню програмних продуктів, такі як HASP-ключі.

Багато сучасних систем запобігання несанкціонованому доступу до об'єктів безпеки та інформації базується на пристроях електронної ідентифікації. Прикладом такого пристрою є автоматичний ідентифікатор виробництва компанії DALLAS SEMICONDUCTOR, США. Цей ідентифікатор може бути вбудований в брелоки, візитки та перепустки. Залежно від застосування, автоматичний ідентифікатор може використовуватися в поєднанні з різними додатковими пристроями, такими як електронні замки або комп'ютери.

Змінна пам'ять ідентифікатора дозволяє використовувати його для широкого спектру застосувань. Їх приклади включають: зберігання персональних ключів шифрування користувача, які регулярно

змінюються, зберігання інформації про стан особистого рахунку користувача в платіжних системах, зберігання інформації про дозволений час проходу в системах контролю доступу. Комбіноване використання ідентифікаторів та електронних замків надає широкі можливості для контролю доступу користувачів до об'єктів з обмеженим доступом. Централізований оперативний моніторинг доступу на об'єкт, дистанційне керування доступом і гнучке налаштування правил доступу на об'єкт (наприклад, у певні дні та години).

Ще кілька слів про новітню технологію, яка використовує фізичні та хімічні властивості матеріалів для підтвердження автентичності документів, безпеки транспортування та запобігання копіюванню. Це спеціальний тонкоплівковий матеріал зі змінними кольорами на основі технології Advateg, що наноситься на документи, вироби або голографічні мітки. Це дозволяє однозначно ідентифікувати автентичність об'єкта та контролювати несанкціонований доступ. Крім того, на основі технології ADVATEG розроблені спеціальні конверти, пакети та інші пакувальні матеріали, які можуть гарантувати конфіденційність документів і товарно-матеріальних цінностей під час транзиту, навіть звичайними поштовими маршрутами.

Технічні засоби захисту інформації включають апаратні та програмні засоби. Основними з них є:

- регулярне резервне копіювання та віддалене зберігання найбільш важливих масивів даних у комп'ютерних системах;
- резервування та дублювання всіх мережевих підсистем, критично важливих для зберігання даних;
- створення можливості перерозподілу мережевих ресурсів у разі виходу з ладу окремих елементів;
- забезпечення можливості використання резервних систем електроживлення;
- забезпечення захисту обладнання від пожежі та пошкодження водою;
- впровадження програмного забезпечення для захисту баз даних та іншої інформації від несанкціонованого доступу.

Комплекс технічних заходів містить засоби забезпечення фізичної недоступності до об'єктів комп'ютерної мережі, наприклад, практичними способами, такими як встановлення камер та сигналізації в приміщеннях.

4.4. Механізми інформаційної безпеки

Інформаційна безпека має наступні концептуальні механізми:

- ідентифікація та автентифікація;
- контроль та управління доступом;
- ведення журналу та аудит;
- шифрування;
- контроль цілісності;
- екранування та інше.

Для надійного захисту інформації всі ці механізми повинні бути впроваджені комплексно. Деякі з них можуть бути реалізовані на більш високому рівні, інші – ні. Захист інтелектуальної власності залежить насамперед від реалізації механізмів ідентифікації та аутентифікації.

Ідентифікатор – це унікальний набір символів, який однозначно відповідає об'єкту або суб'єкту в даній системі.

Ідентифікація – це розпізнавання учасників процесу інформаційної взаємодії перед застосуванням будь-якого аспекту інформаційної безпеки.

Пароль – секретний набір символів, який підтверджує, що суб'єкт відповідає пред'явленому ідентифікатору.

Аутентифікація – забезпечення правильної ідентифікації учасників інформаційної взаємодії.

Профіль – сукупність налаштувань і конфігурацій конкретного суб'єкта або об'єкта, що визначають його поведінку в інформаційній системі.

Авторизація – це формування профілю прав конкретного учасника інформаційної взаємодії.

Суб'єкт може підтвердити свою автентичність, пред'явивши принаймні одну з наступних сутностей:

- щось відоме особі (наприклад, пароль, ключ шифрування);
- щось, що знаходиться у володінні особи (наприклад, електронний ключ, смарт-карта);
- щось, що є частиною особи (біометричні характеристики особи).

Автентифікація може бути односторонньою (зазвичай суб'єкт доводить свою автентичність системі) або двосторонньою (взаємною). Розглянемо ці характеристики.

1. Ідентифікація та автентифікація.

Надійна ідентифікація та автентифікація є складним завданням з ряду причин. Може не існувати надійного шляху між сторонами

інформаційної системи. Це, як правило, означає, що дані, надіслані суб'єктом, і дані, отримані та використані для автентифікації, можуть не збігатися.

Майже всі об'єкти автентифікації можуть бути викрадені або підроблені.

Існує конфлікт між надійністю автентифікації, з одного боку, і зручністю для суб'єкта, з іншого. Наприклад, з міркувань безпеки необхідно вимагати повторного введення автентифікаційної інформації з певною періодичністю.

Чим надійніший захід безпеки, тим вища вартість.

2. Парольна автентифікація

Основною перевагою парольної автентифікації є її простота. Недоліком є те, що це найслабший засіб автентифікації.

Основними порушеннями при створенні та використанні паролів є прості паролі. Саме використання стандартних значень, що зустрічаються в будь-якому документі, які ніколи не змінюються, написання паролів у місцях, де їх можуть прочитати, є вагомим порушенням безпеки інформації та даних.

При спільному використанні паролів з іншими співробітниками необхідно вживати відповідні заходи для підвищення надійності захисту паролем. До таких заходів належать:

- введення технічних обмежень (довжина, використання букв, цифр і символів);
- контроль термінів дії паролів;
- обмеження доступу до файлів з паролями;
- обмеження кількості невдалих спроб входу в систему;
- навчання користувачів;
- використання програмних генераторів паролів. Генеруйте складні, але легкі для запам'ятовування паролі на основі певних правил;
- одноразові паролі.

3. Одноразові паролі

Нехай задано односторонню функцію f. Ця функція відома як користувачу, так і серверу автентифікації.

Припустимо, що існує секретний ключ K, відомий лише користувачу. На початковій фазі управління користувачем функція f застосовується n разів до ключа K і результат зберігається на сервері.

Процедура автентифікації користувача відбувається наступним чином:

- сервер надсилає число (n-1) до системи користувача;
- користувач застосовує функцію f n разів до секретного ключа K

(n-1) і надсилає результат на сервер аутентифікації через мережу;

- сервер застосовує функцію f до значення, отриманого від користувача, і порівнює результат з попередньо збереженим значенням. Якщо віднайдено збіг, то автентичність користувача вважається встановленою, і сервер зберігає нове значення (надіслане користувачем) та зменшує лічильник (n) на одиницю.

Оскільки функція f є незворотною, неможливо перехопити пароль і отримати доступ до сервера автентифікації, щоб дізнатися секретний ключ K і передбачити наступний одноразовий пароль.

Інший підхід до реалізації одноразових паролів полягає в тому, щоб генерувати новий пароль через короткий проміжок часу (наприклад, кожні 60 секунд). Це можна зробити за допомогою додатку або смарт-картки. Для цього повинні бути виконані наступні умови:

1. Сервер автентифікації повинен знати алгоритм генерації пароля та відповідні параметри.

2. Годинники клієнта і сервера повинні бути синхронізовані.

3. Аутентифікація за допомогою токена можлива, якщо:

- на запит від системи токен надає секретне значення і перевіряє свою автентичність. Після перехоплення цієї відповіді зловмисник може імітувати відповідь токена;

- токен і система мають спільну систему синхронізації для генерації одноразових паролів. На запит системи токен видає пароль, який дійсний протягом певного періоду часу. У той же час система генерує власний пароль і порівнює його з отриманим паролем;

- токен реєструється в системі (йому відомі секретні параметри). Для аутентифікації токен генерує випадкове значення, яке він перетворює, використовуючи цей параметр. Система виконує аналогічне перетворення і порівнює результат з отриманим від токена. У цьому випадку зловмисник нічого не отримує від перехоплення запиту і відповіді. Немає необхідності синхронізувати токен з системою.

Можливість використання токена в поєднанні з паролем:

- пароль використовується для доступу до токену, а без пароля токен недійсний;

- параметри пароля і токена є основою для генерації одноразового пароля;

- токен генерує відповідь системі з випадковим значенням на основі своїх параметрів і пароля користувача.

4. Автентифікація за біометричними даними

Біометрія – це сукупність автоматизованих методів ідентифікації та аутентифікації людей на основі фізіологічних і поведінкових

характеристик.

Фізіологічні характеристики включають в себе такі особливості, як:

- відбитки пальців;
- відбитки пальців, сітківка ока, рогівка;
- геометрія рук і обличчя.

Поведінкові характеристики включають:

- динаміку підпису;
- стиль набору тексту на клавіатурі.

Фізіологічні та поведінкові характеристики включають аналіз мови та розпізнавання мови.

Загалом робота з біометричними даними полягає в наступному. По-перше, створюється і підтримується база даних характеристик потенційного користувача. Для цього отримуються біометричні характеристики користувача, обробляються і результати обробки (так звані біометричні шаблони) вносяться в базу даних. Оригінальні дані, такі як результати сканування пальців або рогівки ока, зазвичай не зберігаються.

Надалі процес збору та обробки повторюється для одночасної ідентифікації та автентифікації користувача, після чого здійснюється пошук у базі даних шаблонів.

Якщо пошук виявився успішним, ідентичність та автентичність користувача вважається встановленою. Для аутентифікації достатньо порівняти користувача з одним біометричним шаблоном, обраним на основі раніше введених даних.

Біометрія зазвичай використовується в поєднанні з іншими засобами автентифікації, такими як смарт-картки. Біометрична автентифікація може також використовуватися для активації смарт-картки. Тоді біометричний шаблон зберігається на тій самій картці.

Біометрія зазнає тих самих загроз, що й інші методи автентифікації. Біометричний шаблон порівнюється з тим, який надходить в точку порівняння, а не з результатом первинної обробки характеристик користувача.

Біометричні методи не більш надійні, ніж бази даних шаблонів. Необхідно враховувати відмінності між використанням біометрії в контрольованому місці і в польових умовах.

Шаблонну базу даних необхідно підтримувати, оскільки біометричні дані людини будуть змінюватися. Найбільша небезпека, однак, полягає в тому, що якщо біометричні дані будуть скомпрометовані, всю систему доведеться суттєво модернізувати.

4.5. Методи визначення рівня інформаційного ризику

Одним з методів визначення рівня інформаційного ризику є аналіз інформаційного ризику. Аналіз інформаційних ризиків – це процес комплексної оцінки безпеки інформаційної системи з використанням кількісних і якісних показників. Одним з основних питань аналізу інформаційних ризиків є оцінка вартості (ціни) ризику. Наразі не існує єдиної методики. Причинами цього є відсутність достатньої кількості статистичних даних про ймовірність реалізації тієї чи іншої загрози та неоднозначність в оцінці вартості інформаційних ресурсів (матеріальних і нематеріальних). У таких ситуаціях поширеними є якісні методи оцінки ризиків, що ґрунтуються на експертних оцінках. Такий підхід ускладнює можливість моделювання ризикової ситуації і не дозволяє говорити про об'єктивність отриманих результатів. Згідно з літературними джерелами виділяють наступні фактори, що впливають на ризик.

1. Міра тяжкості наслідків (яка може бути виміряна у відсотках від вартості ресурсу, якщо вартість ресурсу фіксована). Наприклад, якщо збитки становлять до 10% від вартості ресурсу, наслідки є низького ступеня тяжкості; в діапазоні 11-30% – помірні; 31-80% – тяжкі; 81% і більше – катастрофічні. Трудовитрати, необхідні для ліквідації наслідків інциденту, залежать від вартості одного інциденту та кількості інцидентів протягом періоду оцінки. Трудовитрати на ліквідацію наслідків одного інциденту включають трудовитрати на діагностику, документування, ліквідацію наслідків та звітування про результати. Майнова шкода (упущена вигода). Репутаційні збитки.

2. Оцінка ймовірності реалізації загрози оцінюється за шкалою від 1 до 5 (дуже низька, низька, середня, висока, дуже висока). Ймовірність залежить від ступеня вразливості ресурсу до загрози та ефективності управління ним:

- вразливість процесів, де критична інформація є вхідною або вихідною. Шкала включає низький, середній та високий рівень. Вразливість означає наявність передумов для створення іншої загрози;
- відсоток інцидентів, що призвели до збитків, від загальної кількості інцидентів, спричинених даною загрозою за певний період часу в минулому. Цей показник включає значення дуже низького (0-19%), низького (20-39%), середнього (40-60%), високого (61-80%) та дуже високого (81-100%);
- ефективність врядування оцінюється за шкалою від 1 до 5 відповідно до класифікації зрілості Університету Карнегі-Меллона. Відповідність між

поняттям ефективності управління та зрілістю компанії.

Проблеми інформаційної безпеки при застосуванні вищенаведеної шкали підтверджуються дослідженням PricewaterhouseCoopers, яке ґрунтується на аналізі 21 підприємства та 68 проєктів. Рівень зрілості низькоефективних організацій здебільшого знаходиться між одним та двома рівнями. Рівні зрілості високоефективних організацій – це рівні 3, 4 і 5. Крім того, аналітики PwC виявили, що підвищення рівня зрілості значно покращує результати проєктів (30% компаній покращили результати на 25% і більше).

У всіх цих випадках порогові значення обираються індивідуально для кожного конкретного випадку. Оцінка очікуваних втрат від тієї чи іншої загрози передбачає експертну оцінку та використання шкали, що містить лінгвістичні змінні, яка може бути здійснена за допомогою теорії нечітких множин. Використання методу нечітких множин в оцінці ефективності інвестиційних проєктів є добре відомим.

4.6. Управління ризиками інформаційної безпеки (сімейство стандартів ISO/IEC 27000)

Основою для організації, планування та реалізації практичних дій щодо забезпечення безпеки є аналіз концепції загроз, оцінка характеру реальних і потенційних внутрішніх/зовнішніх небезпек і загроз, критичної ситуації та інших несприятливих факторів. Система реальних і потенційних загроз не є постійною, загрози з'являються і зникають, збільшуються і зменшуються, змінюється їх важливість для безпеки.

Управління ризиками є частиною всіх видів діяльності, пов'язаних з організацією, і включає взаємодію із зацікавленими сторонами. Управління ризиками враховує зовнішній та внутрішній контекст організації, включаючи поведінку людей та культурні фактори.

Друге видання скасовує і замінює технічно переглянуте перше видання (ISO 31000:2009).

Основні зміни порівняно з попереднім виданням такі:

- огляд принципів, які є ключовими критеріями успішного управління ризиками;
- більший акцент на ітеративному характері управління ризиками, зазначаючи, що новий досвід, знання та аналіз можуть призвести до модифікації елементів процесу, дій та засобів контролю на кожному етапі процесу;
- упорядкований зміст з акцентом на підтримку моделей відкритих

систем для задоволення різних потреб і ситуацій.

Рекомендується, щоб контроль безпеки для великих організацій, які використовують інформаційно-комунікаційні технології, базувався на стандарті BS 7799/ISO 17799 ISO/IEC 27001. Сьогодні ISO 17799 широко використовується і відбувається поступовий перехід на стандарти серії 27001. Управління безпекою спрямоване на захист усіх компонентів, які сприяють реалізації організованих бізнес-процесів в компанії (рис. 4.1).

Рекомендується, щоб контроль безпеки для великих організацій, які використовують інформаційно-комунікаційні технології, базувався на стандартах BS 7799/ISO 17799 та ISO/IEC 27001.

Зараз широко використовується стандарт ISO 17799 з поступовим переходом на серію 27001.

Управління безпекою має на меті захистити всі компоненти, які сприяють організованим бізнес-процесам на підприємстві.

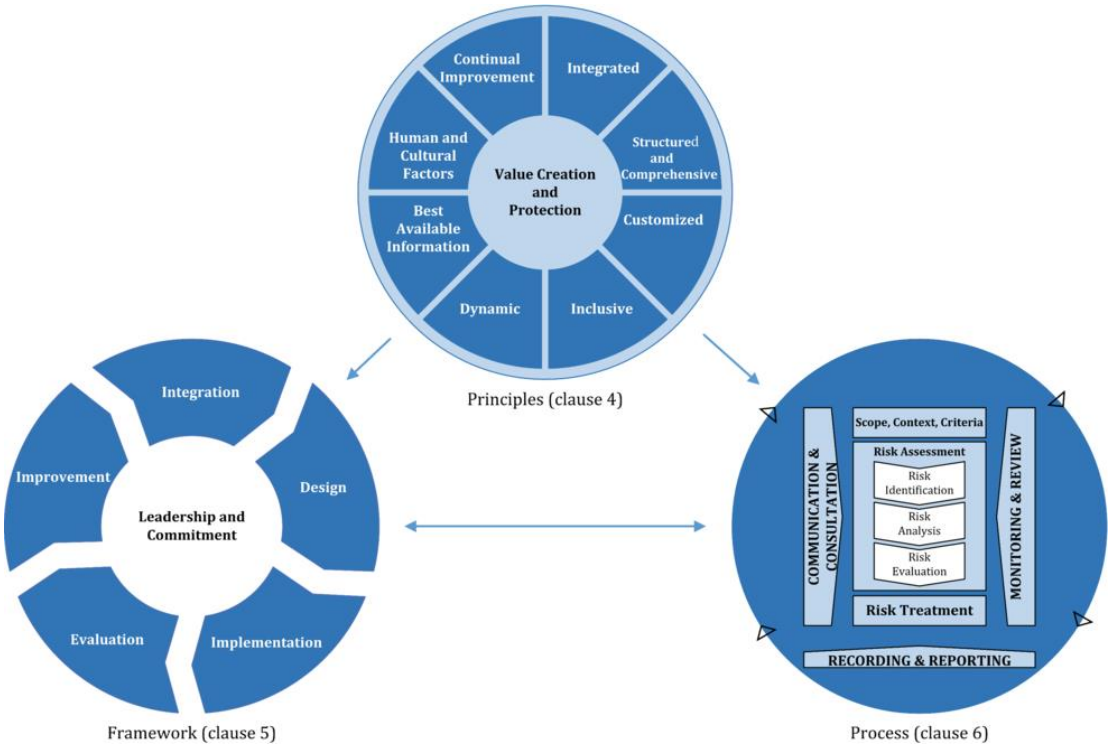


Рис. 4.1. Принципи, структура і процес управління безпекою

Стандарт серії 27001 є моделлю для системи управління інформаційною безпекою (СУІБ). Як і будь-яка сучасна система управління, СУІБ – це набір організаційних заходів і процедур управління, а не технічний стандарт. Стандарт ґрунтується на процесному підході до розробки, впровадження, функціонування, моніторингу, аналізу, підтримки

та вдосконалення СУІБ організації. Він полягає у створенні та використанні системи взаємопов'язаних управлінських процесів у безперервному циклі планування, використання, тестування та поліпшення СУІБ (рис.1, частина "Бізнес-процеси"). Крім того, цей набір стандартів рекомендує перелік програмних та апаратних механізмів захисту інформації, які можуть бути використані на різних етапах бізнес-процесу (рис. 4.3, частина "Технології").

В Україні діють такі стандарти з технічного захисту інформації:

- ДСТУ 3396.0-96 "Захист інформації. Технічний захист інформації. Основні положення". Цей стандарт визначає об'єкти, завдання та організаційні положення щодо забезпечення технічного захисту інформації (ТЗІ) від несанкціонованого доступу до інформації, який може завдати шкоди громадянам, організаціям (юридичним особам) і державі, а також категорії нормативних документів системи ТЗІ.

- ДСТУ 3396.1-96 "Захист інформації. Технічний захист інформації. Порядок виконання робіт". Цей стандарт встановлює вимоги до процедур виконання робіт з технічного захисту інформації.

- ДСТУ 3396.2-96 "Захист інформації. Технічний захист інформації. Терміни та визначення". Встановлює терміни та визначення у сфері технічного захисту інформації.

Найбільш відомим міжнародним стандартом з інформаційної безпеки є британський стандарт BS 7799, розроблений Британським інститутом стандартів (BSI) BS 7799. Складається з двох частин.

Серія стандартів управління інформаційною безпекою ISO/IEC 27000 була розроблена підкомітетом SC 27 технічного комітету ISO/IEC JTC 1.

Система управління інформаційною безпекою (СУІБ) містить вимоги до впровадження та вдосконалення системи управління інформаційною безпекою і базується на моделі "Плануй - Роби - Перевіряй - Дій" (PDCA):

- Створення – ідентифікація активів, управління ризиками;

- Реалізація – етапи впровадження відповідних заходів контролю безпеки;;

- Перевірка – моніторинг та аналіз;

- Act – підтримка та вдосконалення.

Це свідчить про те, що однаково важливо не тільки розробити правила управління та забезпечення безпеки, але й забезпечити циклічність усіх процесів управління безпекою та послідовне проходження всіх процедур через етапи моделі PDCA. Це свідчить про те, що система менеджменту відповідає стандарту ISO 27001 і готова до сертифікації СУІБ.

Відповідність вимогам стандарту ISO/IEC 27001 в першу чергу мінімізує ризик втрати активів компанії/організації і, таким чином, зменшує фінансові втрати.

Стандарт ISO/IEC 27001 спрямований на сертифікацію систем інформаційної безпеки.

Сертифікація системи управління інформаційною безпекою (сертифікація СУІБ) – це ефективне управління бізнес-процесами компанії/організації, інформаційними ризиками і, водночас, доказ того, що компанія є стійкою, розвивається і є надійною. А це призводить до сприятливого ставлення ділових партнерів.

СУІБ, що відповідає стандарту ISO/IEC 27001, є частиною системи менеджменту підприємства.

Сімейство стандартів ISO 27000

Група стандартів включає наступні документи, що стосуються систем управління ІБ:

ISO/IEC 27001 Система управління інформаційною безпекою. Вимоги - Системи управління інформаційною безпекою. Вимоги - Системи управління інформаційною безпекою.

ISO/IEC 27000 Системи управління інформаційною безпекою. Огляд та термінологія - Системи управління інформаційною безпекою. Огляд та термінологія.

ISO/IEC 27003 Системи управління інформаційною безпекою. Настанови - Системи управління інформаційною безпекою. Настанови.

ISO/IEC 27004 Управління інформаційною безпекою. Вимірювання - Вимірювання ефективності систем управління інформаційною безпекою.

ISO/IEC 27006 Requirements for bodies that audit and certify information security management systems - Вимоги до органів, які здійснюють аудит та сертифікацію систем управління інформаційною безпекою.

ISO/IEC 27007 Information security management system audit guidelines (FCD) - Настанови щодо проведення аудитів СУІБ.

Основним механізмом СУІБ є регулярний аналіз ризиків інформаційної безпеки. Аналіз ризиків може базуватися на методах CORAS, CRAMM, Magerit, Mehari, Octave та інших. Він повинен доповнюватися аудиторськими процедурами. Аудити можуть проводитися, наприклад, на основі стандарту CobiT (Control Objectives for Information and related Technology).

Вище керівництво організації також здійснює управління СУІБ, приймаючи рішення на основі результатів аналізу ризиків, внутрішнього аудиту та інших механізмів СУІБ. З точки зору процесів управління,

СУІБ є частиною загальної системи управління організацією та надає додаткові механізми контролю для забезпечення захисту критично важливої інформації. Положення про управління інформаційною безпекою формує позицію керівництва з питань, пов'язаних з політикою безпеки організації, тобто захистом процесів накопичення, зберігання, передачі та знищення інформаційних цінностей, а також дотриманням зобов'язань організації.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які основні загрози інформаційній безпеці виникають у сучасному цифровому середовищі?
2. Які стандарти і нормативні документи регулюють управління інформаційною безпекою?
3. Які підходи існують для аналізу ризиків в управлінні інформаційною безпекою?
4. Які методи шифрування найбільш ефективні для захисту конфіденційної інформації?
5. Як впроваджуються системи багаторівневого захисту інформації і які їхні переваги?
6. Яку роль відіграє управління доступом у захисті інформаційних ресурсів?
7. Які є основні принципи побудови ефективної політики інформаційної безпеки в організації?
8. Як виявлення та протидія атакам (наприклад, фішинг, DDoS) впливають на загальний рівень інформаційної безпеки?
9. Яким чином можна підвищити обізнаність співробітників про ризики та методи захисту інформації?
10. Як оцінюється ефективність впроваджених заходів захисту інформації?

ЛІТЕРАТУРА ЗА РОЗДІЛОМ:

1. Вишня В.Б, Гавриш О.С., Рижков Е.В. Основи інформаційної безпеки : навч. посіб. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2020. 128 с.
2. Бурячок В.Л., Киричок Р.В., Складанний П.М. Основи інформаційної та кібернетичної безпеки: навч. посіб. Київ, 2018. 320 с.
3. Полторак В.П., Савчук О.В. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах. навч. посіб. Київ: КПІ ім. Ігоря Сікорського, 2021. 385с.
4. Полторак В.П. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах: навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с.
5. Носок С.О., Фаль О.М., Ткач В.М. Управління інформаційною безпекою: навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

Розділ 5
ВИКОРИСТАННЯ ВІДКРИТИХ ДЖЕРЕЛ В ІНФОРМАЦІЙНО-АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Сучасні технології та інформаційні ресурси надають національним правоохоронним органам нові можливості для ефективного виконання їхніх завдань. Використання відкритих джерел інформації (Open Source Intelligence – OSINT) стає все більш важливим елементом інформаційно-аналітичної діяльності поліції України.

Різні агенції по-різному дають визначення OSINT, але одне загальноприйняте визначення походить від Довідника НАТО з відкритих джерел розвідки, який визначає OSINT як «*розвідувальну інформацію, яка створюється на основі загальнодоступної інформації та своєчасно збирається, використовується та поширюється належним чином для відповідної аудиторії з метою вирішення конкретної розвідувальної та інформаційної вимоги» [1].*

Протокол Берклі про розслідування цифрових відкритих джерел визначає інформацію з відкритих джерел як *«інформацію, яку будь-який член громадськості може переглядати, купувати або запитувати, не вимагаючи спеціального правового статусу або несанкціонованого доступу. Цифрова інформація з відкритих джерел – це загальнодоступна інформація в цифровому форматі, яку зазвичай отримують з Інтернету» [2].*

OSINT передбачає використання загальнодоступних джерел, таких як газети, телефонні довідники, телебачення, радіопередачі, і, що найважливіше, цифрових джерел, таких як веб-сайти, блоги, форуми та платформи соціальних мереж, для збору інформації, яка може сприяти аналізу розвідданих. Деякі джерела можуть розглядати платні набори даних, які можна отримати через покупку, як інформацію з відкритих джерел, а інші – ні. Але головне, щоб інформація була доступна у відкритих джерелах.

Методи OSINT широко використовуються в кіберрозслідуваннях. Величезна кількість і різноманітність відкритих джерел, особливо в Інтернеті, мають великий обсяг інформації, яку можна зібрати. Від IP-адрес, інформації про веб-сайти та заголовків електронних листів до публікацій у соціальних мережах і онлайнових баз даних дослідники

можуть використовувати OSINT для збору інформації та виявлення моделей діяльності.

Оскільки він покладається на загальнодоступні джерела, інформацію з відкритих джерел можна збирати без попередження суб'єктів розслідування, що робить його ефективним підходом для початкових запитів або коли потрібна обережність. OSINT широко використовується в приватному секторі, а також для збору інформації про ділових партнерів, співробітників або потенційних загроз.

Методи OSINT також є цінними для встановлення контексту в кіберрозслідуваннях. Загальнодоступна інформація може надати передісторію, встановити зв'язки між суб'єктами або розкрити мотиви та поведінку.

5.1. Використання слідчими методів OSINT

Використання методів OSINT може зменшити попит на інші ресурси. Коли цінну інформацію можна отримати з відкритих джерел, немає необхідності вдаватися до більш дорогих, трудомістких або нав'язливих методів. Це може включати операції, які вимагають спеціальних інструментів, спостереження або агентів під прикриттям.

Оперативна безпека (Operations Security – OPSEC) є критично важливим аспектом, який слід враховувати під час проведення OSINT-розслідувань. Процес збору розвідданих залишає за собою сліди, і ця інформація може бути зібрана супротивниками, щоб сформувати ширшу картину, яка скомпрометує розслідування.

У OSINT-розслідуваннях, де слідчі широко використовують онлайн-джерела для збору даних, оперативна безпека має першорядне значення. Будь-яка цифрова діяльність, від перегляду веб-сторінок до онлайн-взаємодій, може відстежуватися. Ці цифрові відбитки можуть виявити особу слідчого або його організацію, характер розслідування та інші конфіденційні деталі, які можуть перешкодити процесу розслідування, скомпрометувати слідчих або навіть поставити під загрозу їхнє життя в екстремальних випадках. Типовим прикладом є підключення до Інтернету з IP-адреси правоохоронного органу під час проведення OSINT-розслідувань. Зловмисник, маючи доступ до журналів веб-сервера, може ідентифікувати IP-адресу та пов'язати її з органом розслідування.

Інформація з відкритих джерел часто оновлюється, іноді в режимі реального часу або майже в режимі реального часу, що дозволяє слідчим

отримувати своєчасні та дієві дані, що є вирішальним у кіберрозслідуваннях. Відкриті джерела часто надають інформацію, яку можна перевірити на кількох платформах або за допомогою підтверджуючих доказів, що підвищує надійність висновків. Якщо ціль має великий цифровий слід, навіть можливо, що більше інформації можна зібрати з відкритих джерел, ніж за допомогою інших методів розслідування.

Використовуючи OSINT-технології, можна обмежити кількість конкретних запитів на інформацію до інших установ або зовнішніх організацій, таких як постачальники онлайн-послуг. Таким чином, запити мають бути зосереджені лише на тих питаннях, на які не можуть відповісти відкриті джерела, підвищуючи загальну ефективність процесу розслідування. Інформація з відкритих джерел, зазвичай, є безкоштовною та широко доступною, що робить її економічно ефективним вибором і полегшує для слідчих збір необхідної інформації без фінансових витрат або складних (міжнародних) правових процедур. Таким чином, слідчі можуть оптимізувати свої ресурси, підвищити швидкість і надійність своїх розслідувань і потенційно виявити критичні фрагменти інформації, які можуть бути недоступні за допомогою інших засобів.

5.1. Юридичні та етичні міркування: OSINT проти NOSINT

Під час роботи з розвідкою відкритих джерел (OSINT) слідчі можуть натрапити на конфіденційну або таємну інформацію, яка незахищена належним чином. Причини їх розголошення можуть бути різними, зокрема випадкові витоки, неправильні конфігурації, несанкціоноване розкриття чи кібератаки.

Чи дозволено дослідникам збирати цю інформацію, часто визначається правовими вказівками, встановленими організацією, або відповідними національними та міжнародними законами. У певних юрисдикціях вони можуть відрізнятися. Дуже важливо знати ці правила та суворо їх дотримуватися, оскільки неналежне поводження з секретною або конфіденційною інформацією або її неправильне використання може призвести до юридичних наслідків, у тому числі до неприйнятності доказів.

Етика – ще один важливий аспект кожного онлайн-розслідування, який стосується того, що є правильним чи неправильним, справедливим чи несправедливим, навіть якщо це законно. Етичні міркування щодо роботи з незахищеною, секретною або конфіденційною інформацією під

час OSINT-роботи можуть бути складними.

Навіть якщо це дозволено законом, неналежне використання закритої інформації може викликати кілька етичних проблем. Слідчі мають поважати конфіденційність і не повинні збирати інформацію з невиправданих причин лише тому, що вони мають до неї доступ. Використання такої інформації може порушити право на конфіденційність, і вона не може використовуватися як доказ у кримінальному провадженні.

Використання неналежним чином захищеної таємної інформації може завдати шкоди окремим особам, організаціям, а іноді навіть націям, особливо якщо це стосується національної безпеки чи інших чутливих сфер.

Коли дослідники стикаються з неналежним чином захищеною або секретною інформацією, вони повинні діяти обережно або повідомити про це керівництво своєї організації та дозволити їм прийняти рішення про відповідний курс дій. Слідчі не повинні використовувати або поширювати таку інформацію без належного дозволу.

Розслідувачі повинні стежити як за правовими, так і етичними принципами, коли мають справу з секретною або конфіденційною інформацією, яку вони знаходять під час роботи OSINT. У той час, як юридичні вказівки пропонують "чи можу я?", етичні міркування відповідають на питання "чи повинен я?". Обидва аспекти є важливими для забезпечення відповідальної та шанобливої поведінки в роботі OSINT [1].

1. Професійні принципи, які встановлені протоколом Берклі, є критично важливими для забезпечення якості розслідувань із відкритих джерел. Ці принципи підвищують довіру, надійність і підзвітність розслідувань.

2. Працівник, який використовує OSINT для методів збору та аналізу інформації, зобов’язаний дотримуватися таких принципів:

- Слідчі повинні забезпечити підзвітність шляхом належного документування, ведення записів і нагляду. Прозорість методів, що застосовуються, має вирішальне значення для підзвітності, тому слідчі змушені вести записи про свою діяльність, коли це можливо. Етапи розслідування, починаючи від виявлення відповідного матеріалу до аналізу та звітності, слід послідовно документувати. Ті, хто бере участь у зборі онлайн-інформації, повинні бути готові до того, що їхні методи збору інформації стануть явними та, можливо, свідчити у суді. Документування може бути ручним або автоматизованим за допомогою програмного забезпечення, якщо воно є ретельним і послідовним. Слідчі

повинні реєструвати будь-які інструменти чи програмне забезпечення, які вони використовують у своїй роботі.

- Слідчі мусять мати відповідну підготовку та технічні навички для своєї діяльності. Вони повинні проводити розслідування в професійній та етичній манері онлайн, віддаючи належне учасникам, коли це безпечно, і повідомляючи точні дані Важливо залишатися гнучким, йти в ногу з розробками, знати та застосовувати нові технології.
- Особисті, культурні та структурні упередження можуть вплинути на роботу; тому слідчі повинні вжити заходів для забезпечення об'єктивності. Вони зобов’язані підходити до своїх розслідувань неупереджено, розробляючи та перевіряючи численні гіпотези, не віддаючи перевагу жодній теорії. Онлайн-розслідування вимагають особливої уваги до об’єктивності через те, як структурована та представлена інформація в Інтернеті. Такі фактори, як веб-переглядачі, пошукові системи та пошукові терміни, можуть призвести до різних результатів, навіть якщо використовується той самий запит. Внутрішні упередження в архітектурі Інтернету та алгоритмах пошуку можуть поставити під загрозу об’єктивність. На результати пошуку можуть впливати такі технічні аспекти, як пристрій, місцезнаходження та історія користувача. Щоб протистояти цим упередженням, дослідники повинні використовувати різноманітні методології, включаючи численні пошукові запити в різних системах і браузерах.
- Вирішальними аспектами будь-якого розслідування є дотримання відповідних законів, вимога до слідчих мати базове розуміння відповідних норм. Це включає усвідомлення законів про захист даних і права на конфіденційність, яке гарантується міжнародними законами про права людини. Хоча інформація може бути загальнодоступною, це не скасовує конфіденційності під час її збирання та використання. Слідчі повинні оцінити наслідки для конфіденційності, враховуючи розумні очікування особи щодо конфіденційності в різних цифрових просторах.

5.2. Додаткові дозволи і заходи безпеки через підвищені проблеми конфіденційності

Слідчі повинні знати, що в деяких юрисдикціях послідовний онлайн-моніторинг або систематичний збір даних може вимагати додаткових дозволів і заходів безпеки через підвищені проблеми конфіденційності.

1. Оперативна безпека

Володіння елементарною обізнаністю щодо операційної безпеки, щоб зменшити цифровий слід і пам'ятати про потенційні ризики, є неминучим. Організації, які займаються розслідуваннями з відкритим кодом, повинні надати слідчим навчання з питань оперативної безпеки. Це допомагає їм зрозуміти ризики, з якими вони можуть зіткнутися, і три основні аспекти інформаційної безпеки: конфіденційність, цілісність і доступність.

2. ***Збереження анонімності***

Слідчі повинні дотримуватися певних основних принципів, які можуть значно підвищити безпеку та ефективність OSINT-розслідувань. Кожне дослідження відрізняється за своєю природою, хоча загалом можна застосовувати наступні принципи:

- **Чистий аркуш:** слідчі повинні починати розслідування з чистого аркуша, що означає свіжий, безпечний і безкомпромісний стан. Це може включати використання спеціального автономного пристрою зі щойно встановленою операційною системою, віртуальну машину, повернуту до початкового знімка, або новий профіль браузера. Це мінімізує ризик перенесення будь-яких артефактів, файлів cookie або зловмисного програмного забезпечення з попередніх розслідувань, які можуть скомпрометувати поточне розслідування.
- **Лише основні дії.** Виконання лише тих дій, які необхідні для розслідування, має вирішальне значення. Це зменшує ймовірність залишення непотрібних цифрових слідів, які можуть викликати підозру. Активні OSINT-методи слід використовувати в крайньому випадку, якщо всі пасивні методи не дали результатів і немає можливості зібрати інформацію будь-якими іншими способами.
- **Відсутність взаємодії:** слідчим слід уникати взаємодії з ціллю або онлайн-сервісами, якими керує ціль, якщо це не є абсолютно необхідним для розслідування. Взаємодія з ціллю може сповістити її про розслідування або, можливо, піддати слідчого ризику. Слідчі повинні дотримуватися пасивних методів збору інформації і де це можливо.

- **Використання легального/безкоштовного/ з відкритим вихідним кодом і оновленого програмного забезпечення.** Слідчим належить використовувати лише легальні, безкоштовні або відкриті програмні засоби, які були протестовані до розслідування. Ці інструменти слід регулярно оновлювати. Використання піратського або застарілого програмного забезпечення може наражати слідчих на юридичні ризики та вразливі місця в безпеці.
- **Окремі сценарії/робочі процеси.** Дослідники повинні ізолювати різні дослідження або робочі процеси один від одного, щоб запобігти перехресному забрудненню даних і цифрових слідів. Для кожного дослідження слід використовувати віртуальні машини з відновленим початковим станом і з чистими профілями браузера та захищеними з'єднаннями VPN. Слідчим ніколи не потрібно змішувати особистий/професійний веб-трафік із слідчим трафіком.

5.3. Підходи до створення середовища розслідування для онлайн-розвідки

1. Підготовка досліджуваного середовища

Як уже обговорювалося, збереження онлайн-анонімності має вирішальне значення в OSINT-розслідуваннях для захисту особи слідчого та цілісності розслідування. Перед проведенням будь-якого збору розвідувальної інформації необхідно добре підготувати середовище для проведення розслідувань. Існує кілька підходів до створення такого середовища:

- **Виділений комп'ютер OSINT. Це** окремий фізичний комп'ютер, який використовується лише для роботи OSINT. Це може допомогти ізолювати розслідування від особистої або пов'язаної з діяльністю слідчих, зменшуючи ризик змішування цифрових слідів. Спеціальний комп'ютер має використовувати безпечне оновлене програмне забезпечення та в ідеалі під'єднуватися до Інтернету через безпечне анонімне з'єднання, наприклад VPN.
- **Віртуальна машина (VM) –** це програмна емуляція комп'ютерної системи, що працює в основній операційній системі дослідників. Використання віртуальної машини для роботи OSINT може забезпечити контрольоване ізольоване середовище, яке можна легко повернути до чистого стану (або знімка). Віртуальні машини також можна налаштувати з різними параметрами безпеки та конфіденційності для збереження анонімності. Віртуальна машина може використовувати

окреме VPN-з'єднання від хост-комп'ютера або запускати інші операційні системи, наприклад Linux.

- **Віртуальна машина на виділеному комп'ютері –** це комбінація двох вищезазначених варіантів. Він передбачає запуск віртуальної машини на спеціальному комп'ютері OSINT. Це дає слідчим додатковий рівень ізоляції та контролю, дозволяючи підтримувати окремі середовища для різних розслідувань, а також фізично відокремлювати OSINT-діяльність від інших дій.
- **Віддалений хост (VPS). В**іртуальний приватний сервер (VPS) – це віртуальна машина, яка надається службою хостингу. Розслідувачі можуть дистанційно підключатися до VPS і використовувати його для операцій OSINT. Завдяки цьому розслідування повністю відключається від локальних комп'ютерів, додаючи ще один рівень анонімності. Використання VPS все ще вимагає довіри до постачальника хостингу щодо конфіденційності та безпеки даних, що пересилаються.

Усі ці варіанти мають свої переваги та недоліки щодо вартості, зручності, безпеки та технічної складності. Найкращий вибір залежить від специфіки розслідування, технічного досвіду слідчого та наявних ресурсів.

2. Безпека фізичного обладнання

Фізичне обладнання, яке використовується для OSINT-розслідувань, має бути постійно захищеним як для захисту цілісності розслідування, так і для захисту від потенційних порушень, які можуть призвести до розкриття конфіденційних даних. Під час використання автономного комп'ютера, де не застосовуються організаційні налаштування безпеки, дослідники повинні переконатися, що пристрій захищений та його безпечно використовувати.

Деякі аспекти захисту фізичного пристрою, який використовується для цілей OSINT, включають:

- **Захист паролем. У**сі пристрої та системи, які використовуються для OSINT, мають бути захищені паролем. Це включає комп'ютери, мобільні пристрої та будь-яке програмне забезпечення чи облікові записи в Інтернеті, які використовуються для розслідування. Дослідникам треба використовувати надійні унікальні паролі для кожної системи та розглянути можливість використання менеджера паролів для безпечного зберігання та керування ними.
- **Шифрування повного диска. Б**ажано увімкнути шифрування повного диска на пристроях. Це шифрує всі дані на жорсткому диску пристрою, тому їх неможливо прочитати без ключа шифрування. Це особливо важливо для автономних OSINT або інших портативних

пристроїв, які можуть бути втрачені або викрадені.

- **Багатофакторна автентифікація.** Дослідники зобов'язані використовувати багатофакторну автентифікацію (MFA) для своїх пристроїв і облікових записів в Інтернеті. MFA вимагає більше одного метода автентифікації для перевірки особи користувача, наприклад пароль і тимчасовий код, надісланий на його телефон. Це забезпечує додатковий рівень безпеки на випадок зламу пароля, хоча для цього потрібен додатковий пристрій, який буде легко доступним, коли з'явиться запит.
- **Окрема зашифрована система зберігання. С**лідчі повинні зберігати дані, пов'язані з розслідуванням, окремо від інших даних (в ідеалі – в зашифрованій системі зберігання). Це може бути зашифрований жорсткий диск або портативна служба зберігання. Це допомагає організовувати дані розслідування та водночас захищає їх у разі зламу пристрою.
- **Без особистого спорядження.** Слідчим слід суворо уникати використання особистого спорядження для OSINT-роботи. Використання окремого обладнання для розслідування знижує ризик перехресного зараження цифрових слідів і допомагає підтримувати чітку межу між особистим життям слідчого та розслідуванням. Це також може допомогти захистити особисті дані слідчих у разі зламу обладнання, яке використовується для розслідування.

Слідчі повинні невідворотно дотримуватися процедур безпеки, встановлених їх організацією, і суворих стандартів безпеки під час використання пристроїв для онлайн-розслідувань. Це може гарантувати, що розслідування залишається конфіденційним, а середовище для розслідування – завжди безпечним.

3. Налаштування віртуальної машини

Налаштування віртуальної машини є простим процесом за допомогою інструментів віртуалізації, таких як VirtualBox. Після налаштування віртуальна машина може забезпечити безпечне та ізольоване (або ізольоване) середовище для OSINT-досліджень.

Щоб налаштувати віртуальну машину з використанням Windows 10 як операційної системи, дослідникам належить виконати такі дії:

1. **Завантажте необхідне програмне забезпечення та ОС**. По-перше, слідчі повинні мати копію VirtualBox, встановлену на своєму комп'ютері. VirtualBox можна завантажити з офіційного сайту. Щоб інсталювати операційну систему, слідчим знадобиться ISO-файл конкретної системи (для цього посібника Windows 10), який можна завантажити з офіційного веб-сайту Microsoft.

2. **Створіть нову віртуальну машину.** Дослідники повинні відкрити VirtualBox і натиснути кнопку «Нова». У діалоговому вікні, що з'явиться, потрібно буде вибрати ім'я для віртуальної машини, тип операційної системи, що встановлюється (Microsoft Windows), і версію (Windows 10).

3. **Призначте розмір пам'яті.** На цьому етапі дослідники повинні додати необхідний обсяг оперативної пам'яті для віртуальної машини. Це значною мірою залежить від доступних системних ресурсів, але 4 ГБ має бути мінімумом для Windows 10, хоча рекомендується 8 ГБ.

4. **Створіть віртуальний жорсткий диск.** VirtualBox запропонує дослідникам створити віртуальний жорсткий диск. Вони повинні вибрати «Створити віртуальний жорсткий диск зараз» і натиснути «Створити». Для типу віртуального жорсткого диска слід вибрати «VDI (VirtualBox Disk Image)».

5. **Розподіл пам'яті на фізичному жорсткому диску.** Дослідники мають вибрати між «Динамічним розподілом» або «Фіксованим розміром» для зберігання. Динамічний розподіл економить місце на фізичному жорсткому диску, але може сповільнити продуктивність, тоді як фіксований розмір може підвищити продуктивність за рахунок збільшення обсягу фізичної пам'яті.

6. **Розташування та розмір файлу.** На цьому етапі дослідники мусять визначити розмір віртуального жорсткого диска. Розмір залежить від вимог до ОС і додатків, які дослідник планує встановити, але для Windows 10 рекомендується мати принаймні 50 ГБ. Слідчі повинні вибрати місце для збереження файлів віртуальної машини або залишити його за замовчуванням, а потім натиснути «Створити".

7. **Встановіть операційну систему.** Створивши віртуальну машину, слідчі можуть уточнити її параметри (наприклад, додати віртуальний оптичний диск) або вибрати її в диспетчері VirtualBox і натиснути «Пуск». У вікні, що відкриється, дослідники повинні перейти до місця розташування ISO-файлу Windows 10, вибрати його та натиснути «Пуск». Віртуальна машина завантажиться з файлу ISO та почне процес встановлення Windows 10, як це було б на фізичному комп'ютері.

8. **Налаштування Windows**. Дослідники повинні слідувати підказкам щодо встановлення Windows 10, наприклад вибрати регіон і мову, прийняти умови ліцензії та налаштувати обліковий запис користувача. Вибираючи розкладку клавіатури та регіональні налаштування, дослідники повинні пам'ятати, що вони також мають відображати профіль розслідування, а не справжнє фізичне розташування

чи компонування апаратного забезпечення. Після завершення налаштування дослідники зможуть завантажитися в Windows 10 і почати використовувати її так само, як і «звичайний» комп'ютер. Після встановлення необхідних компонентів дослідники повинні створити знімок віртуальної машини. Для нового розслідування слідчі повинні завжди повертатися до цього початкового знімка.

Необхідно постійно оновлювати програмне забезпечення віртуальної машини та ОС Windows для забезпечення безпеки та продуктивності віртуального середовища.

4. Приховування підключення до мережі

Віртуальна приватна мережа (VPN) – це технологія, яка використовується для створення безпечного зашифрованого з'єднання між комп'ютером і комп'ютерною мережею, розташованою в іншому місці в Інтернеті. З точки зору OSINT-розслідувань це має дві основні переваги: воно приховує IP-адресу комп'ютера слідчого, що значно ускладнює відстеження веб-сайтів або інших онлайн-сервісів їхнього розташування; і він шифрує дані на вихідному комп'ютері, тобто навіть якщо хтось перехопить інтернет-трафік, він не зможе розшифрувати зв'язок.

При проведенні OSINT-розслідувань використання VPN є надзвичайно важливим. Слідчі часто мають справу з конфіденційною інформацією або службами, якими керують об'єкти інтересів, і їм може знадобитися приховувати свою діяльність. Завдяки маскуванню IP-адреси та шифруванню онлайн-трафіка VPN може забезпечити важливий рівень анонімності та безпеки, захищаючи слідчих від цифрового стеження та кіберзагроз. Однак під час доступу до контенту, що залежить від регіону, дослідники повинні підключатися до серверів VPN з IP-адресою, що відповідає бажаному географічному розташуванню.

Найпоширеніші доступні типи VPN:

- **VPN, реалізовані в браузері.** Зазвичай це служби VPN, інтегровані у веб-браузер. Вони захищають лише дані, які надсилаються та отримуються в цьому конкретному браузері, і не захищають інший Інтернет-трафік на пристрої. Opera має вбудований VPN, а користувачі Chrome і Firefox можуть використовувати розширення VPN для браузера.
- **VPN-клієнти.** VPN-клієнти – це автономні програми, встановлені на пристрої. Вони шифрують усі дані, надіслані та отримані пристроєм, незалежно від того, яка програма використовується. Це забезпечує більш комплексний рівень безпеки порівняно з VPN, реалізованим у браузері. Приклади включають такі служби, як NordVPN, ExpressVPN і ProtonVPN.

- **Сервери VPN.** Розслідувачі можуть використовувати сервери VPN, які можуть бути виділеними або віртуальними серверами. Підключаючись до сервера VPN, пристрій фактично отримує доступ до Інтернету з розташування цього сервера. Це може бути корисним для обходу географічних обмежень щодо вмісту або додавання додаткового рівня заплутування до онлайн-дій. Налаштування VPN-сервера потребує певних технічних знань, хоча таким чином дослідникові не доведеться покладатися на стороннього постачальника.

Вибираючи VPN для роботи OSINT, важливо враховувати такі фактори, як політика конфіденційності постачальника, чи зберігає він журнали активності, чи пропонує захист від витоку DNS, міцність шифрування та репутацію постачальника щодо безпеки.

5.3.1. Безпека браузера

Захист браузера, який дослідники використовують для доступу до веб-вмісту, є ключовим аспектом захисту їх онлайн-активності від порушень безпеки. Це може включати використання зашифрованого зв'язку, захищених браузерів або розширень, керування файлами cookie браузера тощо.

Під час перегляду онлайн-вмісту програмне забезпечення інтернет-браузера залишає за собою унікальний слід інформації, відомий як відбиток пальця браузера. Цей відбиток пальця можна використовувати для відстеження онлайн-дій, навіть якщо слідчі використовують приватний перегляд або режим анонімного перегляду. Відбиток веб-переглядача зазвичай містить такі дані, як тип і версія браузера, операційна система, налаштування мови та регіону, роздільна здатність екрана, системні шрифти та плагіни. Ці дані часто використовуються веб-сайтами для ідентифікації та відстеження користувачів.

Файли cookie – це невеликі файли, які зберігаються браузером і дозволяють веб-сайтам запам'ятовувати інформацію про сеанс перегляду. Вони можуть зберігати облікові дані для входу, ідентифікатори сеансів, персоналізувати роботу користувачів в Інтернеті та навіть відстежувати дії користувачів на сайті. Однак їх також можна використовувати для більш інвазивних цілей, таких як відстеження онлайн-дій на різних веб-сайтах для цільової реклами.

WebRTC (веб-зв'язок у реальному часі) – це технологія, яка забезпечує відео- та голосовий зв'язок безпосередньо у веб-переглядачі без необхідності будь-яких плагінів чи програмного забезпечення. WebRTC потенційно може виявити фактичну IP-адресу, навіть якщо використовується VPN, що може серйозно зашкодити конфіденційності.

Щоб підвищити анонімність браузера, дослідникам необхідно виконувати такі дії:

- Регулярно очищайте файли cookie або налаштовуйте браузер на автоматичне виконання.
- Використовуйте приватний перегляд або режим анонімного перегляду, який не зберігає історію веб-перегляду.
- Вимкніть WebRTC, якщо він не використовується. Зазвичай це можна зробити в налаштуваннях браузера або за допомогою розширення браузера.
- Використовуйте VPN, щоб приховати IP-адресу.
- Використовуйте контейнери сеансів, які створюють ізольований сеанс браузера для кожної вкладки браузера та обмежують міжсайтове відстеження, надаючи кожній вкладці власний окремий набір файлів cookie (наприклад, контейнери кількох облікових записів або тимчасові контейнери).

Блокувальники реклами можуть блокувати рекламу та трекери, підвищуючи конфіденційність в Інтернеті, але водночас видаляючи вміст, який може зацікавити слідчих. Розслідуючи зловмисний вміст у захищеному середовищі, дослідники повинні розглянути питання про відключення блокувальників реклами, щоб отримати повний огляд служби, що досліджується.

Хоча ці інструменти можуть долучити додаткові рівні захисту та ускладнити веб-сайтам відстеження дій, дослідники повинні пам’ятати, що навіть із цими запобіжними заходами досягти абсолютної анонімності в Інтернеті складно. Однак ці кроки можуть значно зменшити цифровий слід і ускладнити веб-сайтам і третім особам відстеження активності в Інтернеті.

5.3.2. Цифровий слід

Цифровий слід – це слід, залишений особою або організацією в цифровому середовищі під час виконання певних дій. Він представляє широкий спектр даних, який може включати відвідування веб-сайтів, електронні листи, витік інформації, публікації в соціальних мережах і онлайн-транзакції. Кожна дія в цифровому середовищі залишає за собою слід, який може призвести до людини. Чим більший цифровий слід, тим більше інформації можна зібрати.

Оскільки використання онлайн-сервісів продовжує зростати, розмір і складність цифрових слідів користувачів ще більше розширюються. Люди використовують Інтернет майже для всіх аспектів свого життя, таких як спілкування, покупки, банкінг, спілкування,

навчання та робота. Ці взаємодії створюють такі дані, як мітки часу, геолокації та інші деталі, які зібрані воєдино, складають онлайн-профілі користувачів, як розповідь про їхню поведінку. Навіть просте відвідування веб-сайту може залишити IP-адресу разом із слідом браузера, який у певних ситуаціях може дати цінну інформацію.

Дії, які містить цифровий слід, можуть бути взаємопов'язані. Прикладом цього може бути пошуковий запит у веб-переглядачі, який може привести до відвідування веб-сайту, що може призвести до онлайн-покупки. Кожна з цих дій є точкою в цифровому сліді, але вони пов'язані з онлайн-діяльністю окремого користувача та можуть відстежуватися адміністраторами веб-сайтів за допомогою методів відстеження браузера.

1. Інформаційні категорії

Інформацію можна розділити на різні групи залежно від рівня обробки та достовірності. Розуміння цих категорій є важливим для ефективної роботи OSINT, оскільки вони визначають, як слід обробляти, інтерпретувати та застосовувати дані.

Ці категорії інформації:

- **Дані з відкритих джерел**. Це необроблені, загальні дані, які є у вільному доступі та доступні для громадськості. Можуть включати будь-що: від вмісту веб-сайту, публікацій у соціальних мережах, статей новин, публікацій у блогах, публічних записів до наборів даних із різних онлайн-платформ. Незважаючи на те, що ці дані спроможні бути цінними, вони часто можуть бути великими та різноманітними, що створює труднощі при вилученні конкретних даних без додаткової обробки.
- **Інформація з відкритих джерел** – це дані, які вже пройшли певний рівень обробки або фільтрації, щоб зробити їх більш сприйнятливими або релевантними. Обробка може включати фільтрацію, упорядкування, сортування або категоризацію даних. Навіть якщо вона обробляється, інформація з відкритих джерел ще не пристосована для задоволення конкретних вимог розвідки.
- **Аналіз отриманої інформації** часто передбачає інтерпретацію, перевірку та агрегування інформації для розуміння моделей, тенденцій, взаємозв'язків і наслідків.
- **Перевірена розвідувальна інформація з відкритих джерел (згідно з НАТО)** – це найвищий рівень інформації з відкритих джерел, яка представляє дані, підтверджені джерелом OSINT або надійним джерелом. Перевірка має вирішальне значення для забезпечення надійності та точності розвідувальних даних. Це часто передбачає

перехресну перевірку даних в інших джерелах, перевірку достовірності джерела або використання інших методів для підтвердження автентичності інформації.

У процесі збору розвідувальних даних дослідники переходять від відкритих джерел даних до підтверджених відкритих розвідувальних даних, і інформація стає більш уточненою, надійною та цінною для прийняття рішень або дій. Важливо також пам'ятати, що кожен крок цього процесу вимагає досвіду, спеціальних методів і чіткого розуміння етичних і правових принципів роботи OSINT.

5.3.3. Електронні докази з відкритих джерел

Електронні докази з відкритих джерел (е-докази) стосуються інформації, зібраної із загальнодоступних цифрових джерел, яка має доказову цінність у правовому контексті, часто стосовно кримінального провадження. Це може включати дані з веб-сайтів, платформ соціальних медіа, онлайнових баз даних, форумів, блогів та інших цифрових платформ, відкритих для громадськості.

Вкрай важливо відрізняти інформацію від доказів. Не вся інформація кваліфікується як доказ, який може бути використаний у кримінальному провадженні, але всі докази містять інформацію. Ключова відмінність полягає в юридичній допустимості та доказовій силі даних.

Інформація з відкритих джерел може бути використана як електронний доказ, якщо вона:

- **Отримана законним шляхом.** Під час збору даних важливо дотримуватися всіх відповідних законів і нормативних актів, зокрема поважати права на конфіденційність, права інтелектуальної власності та умови угод про надання послуг (якщо це можливо).
- **Має доказову силу**. Інформація має відповідати справі, що розглядається, і мати доказову силу. Повинна бути здатною довести або спростувати факт у кримінальному провадженні.
- **Може бути перевірена.** Походження та цілісність даних завжди мають бути перевірені. Це передбачає документування процесу збору, збереження та аналізу, щоб продемонструвати, що дані не були підроблені.
- **Прийнятна в суді.** У різних юрисдикціях діють різні правила щодо того, що вважається допустимим доказом. Це може залежати від кількох факторів, зокрема джерела інформації, методу збору, надійності та актуальності даних тощо.

5.4. Етичні та правові наслідки під час збору та обробки електронних доказів із відкритим кодом

Проводячи OSINT-розслідування, важливо пам'ятати про вимоги до даних, щоб кваліфікувати їх як електронні докази. Навіть якщо інформація, виявлена під час розслідування, може здатися важливою чи значущою, вона може бути корисною в правовому контексті лише в тому випадку, якщо вона задовольняє вищеперелічені умови. Слідчі повинні завжди пам'ятати про етичні та правові наслідки під час збору та обробки електронних доказів із відкритим кодом.

1. Отримання інформації

Техніки отримання інформації варіюються від ручних до повністю автоматизованих, кожна з яких має свої унікальні переваги та міркування. Ручне отримання вимагає зусиль людини та займає більше часу, тоді як автоматизовані інструменти можуть бути дорогими. У певних сценаріях кожен метод отримання даних має свої переваги та недоліки.

- **Отримання вручну**. Цей метод передбачає ручний пошук і перегляд онлайн- і офлайн-джерел для збору інформації. Це може включати пошук у профілях соціальних мереж, публічних записах, блогах, форумах або будь-яких інших платформах з відкритим кодом. Хоча ручне отримання може зайняти багато часу та вимагати більше робочої сили, воно забезпечує високий рівень людського контролю та точності. Дослідник може інтуїтивно слідувати підказкам, застосовувати людське судження для оцінки відповідності та надійності та адаптувати стратегію пошуку в міру відкриття нової інформації.
- **Напівавтоматичний збір. Н**апівавтоматичні методи використовують сценарії або спеціалізовані інструменти для автоматизації певних аспектів процесу збору інформації. Наприклад, сценарій (наприклад, букмарклет – «закладка») можна використовувати для збирання даних із веб-сайту або автоматичного пошуку за певними ключовими словами на кількох платформах. Ці інструменти можуть підвищити ефективність, дозволяючи слідчим збирати великі обсяги даних швидше, ніж вручну. Однак ці методи все ще вимагають певної участі людини для встановлення параметрів, контролю за процесом та інтерпретації результатів.
- **Автоматичне отримання.** Повністю автоматичне отримання залежить від передових програмних програм або служб, розроблених спеціально для цілей OSINT, які пропонують треті сторони. Ці

інструменти можуть відстежувати визначені джерела, фільтрувати та аналізувати дані на основі попередньо визначених критеріїв і навіть надавати сповіщення, коли виконуються певні умови. Вони можуть швидко обробляти велику кількість даних, виявляючи закономірності та зв'язки, які дослідники можуть пропустити. Однак вони також потребують ретельного налаштування та контролю, щоб уникнути таких проблем, як перевантаження даних, помилкові спрацьовування або порушення конфіденційності чи умов угоди про надання послуг.

Кожен метод може мати свої переваги в комплексній стратегії OSINT-розслідування, і вони часто використовуються в комбінації. Найкращий підхід залежить від таких факторів, як характер і обсяг розслідування, наявні ресурси та конкретні юридичні та етичні міркування.

5.5. Класифікація OSINT-розслідування

1. OSINT-розслідування

OSINT-розслідування можна класифікувати залежно від мети та методології збору інформації. Кожен тип має унікальну спрямованість і методологію.

OSINT-розслідування можуть бути такі:

- **Моніторинг OSINT**. Передбачає підтримання регулярного спостереження за ціллю, якою може бути особа, група, організація або навіть певна тема. Мета полягає в тому, щоб стежити за діяльністю об'єкта, розвитком або змінами з часом. Це може включати моніторинг дописів у соціальних мережах, публічних оголошень або онлайн-дій для збору поточної інформації. Цей тип OSINT зазвичай використовується правоохоронними органами, коли важливо бути в курсі потенційних загроз (наприклад, у контексті публічних демонстрацій, спортивних заходів тощо).
- **Локалізація OSINT.** Цей підхід зосереджений на визначенні того, хто є об'єктом інтересу, та отриманні уявлення про його місцезнаходження, діяльність, зв'язки та інші контекстуальні деталі. Мета полягає в тому, щоб ідентифікувати, знайти та зрозуміти предмет у деталях. Це може включати збір інформації з онлайн-профілів, публікацій із геотегами, IP-адрес або будь-яких інших загальнодоступних даних, які можуть допомогти точно визначити місцезнаходження суб'єкта чи контекст.
- **Цільовий OSINT**. Він передбачає більш глибоке,

цілеспрямоване дослідження конкретного предмета інтересу. Мета полягає в тому, щоб зібрати якомога більше інформації про конкретну ціль, яка вже була ідентифікована, включаючи її поведінку, приналежність, моделі, мережі та будь-які інші відповідні деталі. Це може передбачати глибоке дослідження онлайн-присутності об'єкта на кількох платформах, аналіз його зв'язків і діяльності, а також використання спеціальних інструментів або методів для збору цінної інформації.

Хоча ці категорії забезпечують корисну структуру, на практиці складна OSINT-операція може включати всі вищезазначені типи збору розвідувальних даних, залежно від конкретних цілей і вимог розслідування.

2. Методи OSINT

Методи OSINT можна розділити на три основні категорії залежно від того, чи існує будь-яка взаємодія з об'єктом або джерелом інформації:

- **Пасивні методи OSINT.** У цьому підході слідчі збирають інформацію без безпосередньої взаємодії з ціллю або будь-яким чином змінюючи джерело. Це може включати такі дії, як перегляд публічних записів, читання публікацій у блогах, аналіз каналів соціальних мереж або моніторинг статей новин. Перевагою цього методу є те, що він навряд чи попередить ціль або викличе будь-яку підозру, оскільки слідчий просто спостерігає за легкодоступною інформацією. Однак отримана інформація може бути обмеженою та залежати від того, що ціль вирішить поділитися публічно. Слідчі також повинні мати на увазі, що доступ до певного вмісту може стати активним OSINT, коли ціль має доступ до функцій керування досліджуваним сервісом (наприклад, журнали доступу до веб-сервера).
- **Напівпасивні методи OSINT** передбачають певний рівень взаємодії з джерелом, але таким чином, що нагадує типову поведінку користувача та не викликає підозр. Наприклад, слідчий може створити профіль у соціальних мережах, щоб стежити за діяльністю об'єкта, використовувати пошукову систему для вивчення теми або приєднатися до онлайн-форуму для перегляду публікацій і обговорень. Хоча цей метод може давати більш детальну та своєчасну інформацію, він також несе в собі більший ризик виявлення, оскільки передбачає більш помітну діяльність.
- **Активні OSINT-методи** передбачають пряму та часто приховану взаємодію з метою збору більш детальної або конкретної інформації. Це може включати такі методи, як надсилання запиту «друзі об'єкта в соціальних мережах», участь в онлайн-розмові або

використання приводу для отримання інформації. Ці методи можуть надати цінну інформацію, недоступну за допомогою пасивних або напівпасивних методів. Однак вони також несуть найвищий ризик виявлення та можуть мати юридичні та етичні наслідки.

Перш ніж використовувати методи OSINT, слідчі зобов'язані врахувати ці фактори та вибрати найбільш відповідний метод на основі характеру розслідування, потенційних ризиків, а також правових і етичних принципів, застосовних до їхньої роботи.

3. Цикл *інтелекту*

Цикл розвідки – це процес, який використовується аналітиками розвідки для розуміння та надання необхідної інформації тим, хто запитує. Цикл інтелекту складається з п'яти фаз (рис. 5.1):

1. **Планування.** Це початковий етап, на якому визначаються вимоги до інтелекту. Окреслюється мета або розвідувальне питання, а також конкретні типи розвідувальних даних, які потрібно зібрати. Цей етап також передбачає розподіл ресурсів і проведення оцінки ризиків. Етап планування гарантує, що процес збору розвідувальної інформації є цілеспрямованим, надійно забезпеченим ресурсами та проводиться в межах прийнятного рівня ризику.

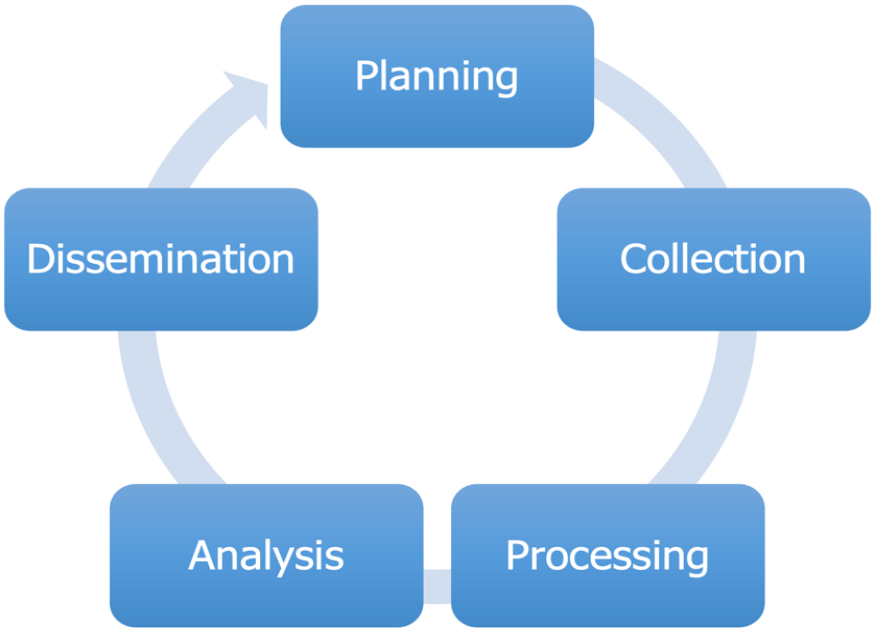


Рисунок 5.1 Цикл розвідки

2. **Збір.** Цей етап передбачає отримання даних з різних джерел, вручну або автоматично, відповідно до плану збору розвідувальних даних. Визначається релевантність доступних джерел, розподіляються

обов’язки та вибираються пристрої або програмне забезпечення для використання. На цьому етапі необхідна документація для запису процесу збору даних.

3. **Обробка.** На цьому етапі зібрані дані проходять ряд обробок. Фільтрація виконується для відсіювання нерелевантних або ненадійних даних, зосереджуючись на високоякісних, своєчасних і дієвих даних. Інші процеси можуть включати переклад, дешифрування та інтерпретацію даних. Оцінка достовірності, надійності та дійсності даних має вирішальне значення для забезпечення їх достовірності, послідовності та точності.

4. **Аналіз.** Цей етап передбачає інтеграцію, оцінку та аналіз усіх доступних даних та інформації. Когнітивні та перцептивні упередження, такі як дзеркальне відображення (припущення, що ціль поводиться як дослідник), фіксація цілі (дотримання однієї гіпотези) або використання потенційно неправильних аналогій, є одними з кількох когнітивних пасток, яких слід уникати. Для мінімізації цих пасток використовуються методи структурованого аналізу [1].

5. **Розповсюдження.** На завершальному етапі розвідувальний продукт передається споживачам у формі вичерпних, лаконічних звітів, у яких підсумовуються оброблені розвідувальні дані. Ці звіти повинні відповідати на всі розвідувальні запитання, висвітлювати найбільш релевантні висновки та можуть приймати різні форми залежно від вимог, встановлених організацією або запитувачем. Після розповсюдження перша фаза може бути розпочата знову, перезапускаючи цикл.

Перш ніж почати розслідування відкритого коду, важливо створити план дослідження. Цей план має містити загальну стратегію розслідування та конкретні завдання для онлайн-розслідування. Якщо онлайн-дослідження є частиною більшого розслідування, яке також включає традиційні методи, такі як розмова зі свідками чи збір речових доказів, надзвичайно важливо поєднати онлайн-план із основною стратегією розслідування. Хоча увага зазвичай зосереджена на етапах збору, обробки та аналізу, дуже важливо провести чітку межу між документацією та звітністю. Належна документація забезпечує підзвітність і прозорість, але звіт не повинен містити подробиць усіх дій для збереження конфіденційності. Цей баланс забезпечує всебічне розуміння, підтримуючи безпеку процесу розслідування.

Основна мета циклу розвідки полягає в тому, щоб відповісти на питання розвідки, що потенційно може призвести до появи додаткових питань розвідки. У міру повторного запуску циклу мета залишається незмінною, хоча увага переключається на нове питання інтелекту.

5.6. Методологічні принципи

Слідчі повинні дотримуватися чітких методологічних принципів під час проведення аналізу розвідувальних даних і переходу між фазами циклу розвідувальних даних.

Забезпечення точності розслідувань є як методологічним, так і етичним принципом, який передбачає довіру виключно до надійних джерел. Дослідники з відкритим кодом повинні надавати пріоритет правдивості та точності, особливо під час представлення висновків, і визнати обмеження у зборі розвідувальної інформації. Точність можна додатково підвищити, дослідивши численні гіпотези та залучивши експертну оцінку для пом'якшення потенційних упереджень. У висновках слід уникати перебільшень, а використання чіткої, об'єктивної, заснованої на фактах мови є важливим для підтримки об'єктивності розслідування.

Принцип мінімізації даних встановлює, що цифрову інформацію слід збирати та обробляти лише тоді, якщо це виправдано для чіткої мети, необхідно для досягнення цієї мети та пропорційно для її досягнення. Під час розслідувань онлайн-контент слід збирати лише у випадку, коли він має відношення до конкретного запиту. Застосування цього принципу запобігає надмірному збору, який спричинює різні проблеми, особливо вразливість безпеки, якщо слідчі не знають їхньої інформації. Проблеми щодо конфіденційності та захисту даних можуть виникнути, якщо автоматизовані процеси не дискримінують інформацію.

З іншого боку, принцип збереження має на меті запобігти недостатньому збору, гарантуючи, що цінні докази не будуть втрачені. Постачальники онлайн-контенту можуть видаляти вміст, який порушує їхні умови, хоча це може бути потенційно корисним для слідчих. Без своєчасних запитів на збереження чи дій слідчих, наприклад належного документування, така інформація може зникнути. Користувачі також можуть видаляти або змінювати свій вміст, здійснюючи колись загальнодоступні дані недоступними. Інтернет-інформація може бути легко деконтекстуалізована, втрачена, стерта або пошкоджена. Щоб зберегти цифровий матеріал для майбутньої звітності, збереження є досить важливим.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ

1. Які основні типи відкритих джерел інформації використовуються в діяльності Національної поліції?
2. Які методи аналізу інформації з відкритих джерел є найбільш ефективними для правоохоронних органів?
3. Як відкриті джерела допомагають у виявленні кримінальних зв’язків та групових правопорушень?
4. Які ризики виникають при використанні інформації з відкритих джерел у кримінальних розслідуваннях?
5. Які технологічні інструменти використовуються для збору та обробки даних із соціальних мереж?
6. Які принципи забезпечення конфіденційності та безпеки при роботі з відкритими джерелами?
7. Як оцінити достовірність інформації з відкритих джерел у контексті правоохоронної діяльності?
8. Які юридичні аспекти пов'язані з використанням даних з відкритих джерел у слідчих діях?
9. Які є приклади успішного використання інформації з відкритих джерел для розкриття злочинів?
10. Як автоматизація процесів обробки даних із відкритих джерел впливає на ефективність аналітичної роботи поліції?

ЛІТЕРАТУРА ЗА РОЗДІЛОМ:

1. Akhgar, B., Bayerl, P. S., Sampson, F. (2016): Open Source Intelligence Investigation From Strategy to Implementation, Spinger.
2. Bazzell, M. (2023). OSINT Techniques: Resources for Uncovering Online Information. CreateSpace Independent Publishing Platform.
3. Borges, D. (2021). Adversarial Tradecraft in Cybersecurity: Offense versus defense in real-time computer conflict. Packt.
4. Hassan, N., Hijazi, R. (2018). Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence. Apress
5. Schaurer, F., & Störger, J. (2013). The evolution of open source intelligence (OSINT). *Comput Hum Behav*, *19*, 53-56.
6. Tayebi, M., Glasser, U., Skillicorn, D. (2020). Open Source Intelligence and Cyber Crime: Social Media Analytics. Springer
7. Wells, D., & Gibson, H. (2017). OSINT from a UK perspective: Considerations from the law enforcement and military domains. *Proceedings Estonian Academy of Security Sciences, 16: From Research to Security Union*, *16*, 84-113.
8. UC Berkeley School of Law. (2022). Berkeley Protocol on Digital Open Source Investigations. United Nations Human Rights Office of the High Commissioner.
9. US Government. (2009). A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Retrieved from: https://www.cia.gov/static/955180a45afe3f5013772c313b16face/Tradecraft-Primer-apr09.pdf.

Розділ 6
ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ІНФОРМАЦІЙНО-АНАЛІТИЧНІЙ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

На сучасному етапі розвитку суспільних відносин та науково-технічного прогресу правоохоронні органи в цілому та органи й підрозділи Національної поліції зокрема в рамках окресленого правового поля мають можливість використовувати в процесі інформаційно-аналітичної діяльності можливості штучного інтелекту (далі – ШІ) задля вирішення своїх функціональних завдань.

Спектр підрозділів Національної поліції при цьому достатньо розгорнутий – від кримінального аналізу до превенції. І якщо діяльність перших вже достатньо висвітлена у вітчизняних та закордонних спеціалізованих джерелах, то діяльність підрозділів блоку превентивної діяльності та оперативних підрозділів набуває первинного досвіду використання у своїх сегментах можливостей ШІ.

Саме на прикладі останніх ми і пропонуємо розглянути як сам ШІ з його історико-теоретичними аспектами, так і прикладні позиції його потенційного використання у діяльності окремих служб Національної поліції.

Одне із базових завдань ШІ у правоохоронній сфері – збір (пошук) та обробка різноманітної інформації про осіб, які становлять превентивний або слідчо-оперативний інтерес та відповідні факти протиправної діяльності.

Одним із доступних джерел про людину є соціальні мережі. Правоохоронні органи можуть використовувати значні обсяги даних з соціальних мереж для збору необхідної інформації. Однак для конкретного правопорушення потрібна певна кількість інформації, тому пошук має бути спрямований на виявлення саме тих даних, які мають значення для справи, відкидаючи непотрібну інформацію, яка може уповільнити процес. Головним завданням розробників програмного забезпечення є створення інструментів, які дозволяють правоохоронцям ефективно використовувати дані з соціальних мереж.

6.1. Штучний інтелект: поняття та історія виникнення

Термін “Штучний інтелект” пройшов через різні етапи розвитку, отримуючи нові визначення. В загальному ШІ можна описати як набір методів, що дозволяють комп’ютерам імітувати людське мислення.

У сучасному світі штучний інтелект виступає як ключовий елемент у розвитку технологій, впливаючи на багато аспектів нашого життя. ШІ охоплює широкий спектр технологій та методик, спрямованих на створення систем, які можуть відтворювати людські когнітивні процеси, такі як навчання, мислення та взаємодія з навколишнім середовищем.

ШІ базується на таких фундаментальних концепціях:

Машинне навчання (ML) – розробка алгоритмів, здатних навчатися та адаптуватися для виконання завдань без прямого програмування.

Глибоке навчання (DL) – використання багатошарових нейронних мереж для виявлення складних закономірностей у даних.

Нейронні мережі – математичні моделі, що імітують структуру нейронів біологічного мозку для вирішення завдань.

Обробка природних мов (NLP) – автоматичне розуміння, генерація та переклад мовних даних.

Когнітивні системи – моделювання людського мислення для покращення виконання завдань.

Розпізнавання образів – виявлення повторюваних моделей у даних для застосувань, зокрема, розпізнавання облич.

Ці елементи визначають можливості та обмеження ШІ, а також напрями його застосування та розвитку. ШІ вже застосовується у багатьох сферах, включаючи обробку мови, розпізнавання образів, автоматизацію рішень та робототехніку. І дозволяє створювати системи, які аналізують дані швидше та точніше, ніж людина, і постійно вдосконалюються.

Вивчаючи ШІ, можна стверджувати, що він є одним з багатообіцяючих технологічних напрямів, який вже вплинув на хід цивілізації та продовжує відкривати нові можливості та виклики для людства.

Штучний інтелект має багатовимірну історію, яка включає в себе ключові моменти та досягнення, що вплинули на його сучасний стан. Ця галузь розвивалася у згоді з прогресом у сфері комп’ютерних наук, але також має свої унікальні віхи.

Зародження ШІ відбулося у середині XX-го століття з теоретичних робіт та експериментів вчених на кшталт Алана Тьюрінга, які запитували, чи можуть машини "думати". Тест Тьюрінга став першим значним випробуванням для ШІ, і він досі використовується як міркування здатності програм імітувати людську поведінку [9].

Таким чином, ШІ зародився у 50-х роках XX ст., коли вчені почали розробляти машини, здатні виконувати завдання, які раніше вважались виключно людською прерогативою. Одним з перших значних досягнень стала шахова програма, яка перемогла чемпіона світу.

З того часу ШІ стрімко розвивався і зараз використовується у багатьох сферах. У 1956-1974 роках програми ШІ, які розв'язували математичні задачі та вчилися мовам, викликали всесвітнє захоплення.

У 1980-х роках "експертні системи" стали одним з основних напрямів ШІ, а Японія значно інвестувала у розвиток цієї галузі.

Світовий інтерес до ШІ зріс наприкінці XX століття завдяки розвитку обчислювальних технологій і доступності значних даних, що призвело до проривів у машинному навчанні та глибокому навчанні. Це дозволило створити продукти зі здатністю розпізнавати мову, аналізувати зображення, керувати транспортом та перемагати в інтелектуальних іграх.

До 2011 року ШІ досяг важливих цілей, зокрема завдяки збільшенню обчислювальної потужності та спеціалізації на конкретних завданнях.

Технологія глибокого навчання, започаткована у 2011 році, дозволила комп'ютерам здійснювати складні висновки та прогнози, використовуючи великі масиви даних. Ця технологія продовжує відігравати роль у багатьох областях.

Після 2000 року ШІ, з огляду на його ефективність, відносну новизну та універсальність, продовжує розвиватися і, без сумніву, знаходитиме застосування у багатьох сферах людської діяльності в майбутньому, в тому числі і у сфері діяльності правоохоронних органів.

Сучасний розвиток ШІ включає не лише технічні аспекти, але й етичні та соціальні наслідки. Наприклад, Міністерство оборони США в 2020 році прийняло етичні принципи для ШІ, що відображає зростання соціальної відповідальності [10].

В Україні інтерес до ШІ та його розвиток почалися ще в радянські часи із розробки інтелектуальних систем. Після здобуття незалежності ця сфера отримала значний розвиток завдяки внеску українських науковців, які працюють над машинним навчанням, нейронними мережами та аналізом даних. Історія ШІ в Україні відображає як історичне коріння,

так і сучасні тенденції. Україна зміцнила свої позиції в ШІ, що підтверджується зростанням досліджень та участі в міжнародних проєктах. В Україні наука і технологія розвивалися відповідно до світових тенденцій, але також адаптувалися до місцевих умов. Дослідження в галузі сприяли розумінню потенціалу та обмежень ШІ.

Вивчення історії штучного інтелекту (ШІ) виявляє, що з моменту його зародження виникали побоювання щодо його впливу на людську діяльність та її результати. З часом ці занепокоєння тільки поглибилися, оскільки стало зрозуміло, що ШІ може призводити до ризиків. Видатні особистості у сфері технологій закликають до негайного встановлення правил для безпечного впровадження ШІ у різні сфери. Наприклад, у березні 2023 року Ілон Маск висловився за призупинення досліджень у певних аспектах ШІ, вказуючи на його потенційний вплив на соціальні та економічні структури суспільства [11]. Це підкреслює значення інтеграції ШІ у системи правоохоронної діяльності, яка може значно посилити його можливості, здійснюючи тему регулювання ШІ ще більш актуальною. При впровадженні ШІ у важливі сфери, необхідно запобігти будь-якій можливості, щоби не завдати шкоди суспільству, навіть якщо вона буде мінімальною, оскільки з розвитком ШІ ризики для інформаційного простору можуть лише зростати.

6.2. Технології, які застосовані у соціальних мережах

Соціальні мережі є втіленням ідей та цілей їх творців. Функціональність цих платформ відображає стратегічні напрями, які задані їх власниками та розробниками, часто з метою монетизації. Таким чином, аналізуючи можливості соціальних мереж, слід враховувати інтереси їх творців.

Штучний інтелект є ключовою технологією для аналізу поведінки користувачів. ШІ виявляє поведінкові шаблони та пропонує контент, який, ймовірно, зацікавить користувача. Згідно з Марціном Фронкевичем, алгоритми ШІ можуть аналізувати поведінку, вподобання та інтереси користувачів, надаючи персоналізований контент, що підвищує залученість та задоволеність користувачів. ШІ дозволяє створювати детальний портрет інтересів користувача, виходячи з його дій у соціальній мережі.

Facebook (Додаток 1) аналізує комунікацію між користувачами, пропонуючи контент на основі інтересів їхнього соціального кола. Це дозволяє виявити, з ким користувач взаємодіє та які відносини він мав

у минулому. Цей підхід є ефективним для пошуку інформації в рамках оперативно-розшукової діяльності, особливо коли доступна інформація про соціальне середовище аналізованого користувача.

TikTok (Додаток 1) базується на аналізі взаємодії користувача з контентом через інтерактивні елементи, такі як коментарі, лайки, збереження, час перегляду та кількість переглядів. Це дозволяє створювати детальний профіль інтересів користувача, враховуючи його несвідомі переваги.

Instagram (Додаток 1) комбінує різні підходи, адаптуючись до суспільних настроїв та актуальних трендів, використовуючи різноманітні формати контенту, такі як reels та stories, для залучення користувачів.

Використання ШІ в соціальних мережах може значно підвищити ефективність оперативно-розшукової діяльності, оскільки алгоритми відображають не лише зовнішню інформацію про користувача, а й його глибинні інтереси та думки.

Історія розвитку технологій у суспільстві завжди була спрямована на автоматизацію праці. У сучасному світі, де технології розвиваються стрімко, створення штучного інтелекту стало кульмінацією цього процесу, як “автоматизація автоматизації”. Використання застарілих методів у порівнянні з можливостями ШІ не є достаньо перспективним.

Соціальні мережі відіграють головну роль у виявленні підозрюваних у кримінальних розслідуваннях, але процес пошуку цих осіб вимагає значних зусиль. Використання ШІ у пошуковій та інформаційно-аналітичній діяльності може спростити цей процес, досліджуючи дії користувачів у соціальних мережах і формуючи список потенційних підозрюваних. ШІ може імітувати людське мислення, а соціальні мережі ефективно відображають думки людей, тому комбінація цих двох факторів може дозволити ШІ відтворювати процеси мислення людини через соціальні мережі.

Однак існують перешкоди для інтеграції ШІ у соціальні мережі, зокрема обмеження, встановлені їх власниками. Співпраця з власниками соціальних мереж може бути складною, і якщо пряме вирішення цієї проблеми неможливе, необхідно знайти інші способи впливу на дії користувачів для інтеграції ШІ. Одним з таких способів може бути використання процесів на платформах, де функціонують соціальні мережі, оскільки вони є середовищем для всіх програмних процесів.

Інтеграція у пристрій користувача, включаючи використання

“зомбі-вірусів” для віддаленого контролю, не є новою для оперативно-розшукових підрозділів [8]. Комбінація таких технологій з ШІ може забезпечити автономність у зборі даних.

Анонімність у сучасному світі ІТ стала складнішою. Тому спеціалісти працюють над створенням умов для забезпечення анонімності у соціальних мережах через шифрування. ШІ може аналізувати закономірності та алгоритми, що у змозі допомогти у розшифровці інформації.

ШІ також може аналізувати візуальні елементи та контекст, що відкриває можливості для доступу до даних користувачів. Оперативно-розшукові підрозділи можуть використовувати ШІ для виявлення підозрюваних, навіть якщо інформація про них не була явно сформована.

Створення єдиного реєстру дій користувачів соціальних мереж та його аналіз з допомогою ШІ може сприяти розкриттю складних злочинів, включаючи ті, що відображаються в “ефекті метелика”, де дії одного користувача впливають на дії багатьох інших. Таким чином, ШІ у соціальних мережах може стати потужним інструментом для оперативно-розшукової діяльності як дієвий інструмент інформаційно-аналітичної діяльності.

6.3. Правова основа використання штучного інтелекту та інформації, отриманої за допомогою соціальних мереж, в оперативно-розшуковій діяльності

Сучасний розвиток суспільства вимагає швидкого реагування від правоохоронних органів. Важливо, щоб дії поліції були засновані на законодавстві. Існує виклик у правовому регулюванні використання даних з соціальних мереж та штучного інтелекту в оперативно-розшуковій діяльності. Тому необхідно проаналізувати національне законодавство при опрацюванні соціальних мереж, а також національне та міжнародне законодавство при використанні штучного інтелекту.

6.3.1. Особливості вітчизняного законодавства про соціальні мережі

З розвитком інформатизації в Україні було прийнято закони для регулювання інформаційних відносин. Ці закони включають Конституцію України та інші важливі акти. Є потреба визначити

ключові правові норми для учасників інформаційних відносин, особливо для запобігання злочинам. Проте сучасне законодавство часто є нечітким і неузгодженим, що призводить до різного тлумачення норм.

У контексті цієї теми ми аналізуємо положення Конституції України та законів, що стосуються Національної поліції та оперативно-розшукової діяльності. Конституція вимагає від правоохоронних органів забезпечувати національну безпеку та боротися зі злочинністю. Закон України "Про оперативно-розшукову діяльність" не визначає використання соціальних мереж, але дозволяє поліції збирати дані для розслідувань. Таким чином, використання соціальних мереж відповідає законодавству України і допомагає поліції виконувати свої завдання.

ЗУ "Про Національну поліцію" визначає загальні напрями роботи, але не дає конкретних вказівок щодо соціальних мереж. Закон "Про оперативно-розшукову діяльність" також не має чітких правил для використання соціальних мереж, але містить положення, які дозволяють таку діяльність. Зокрема, стаття 6 вказує на можливість збору інформації для розслідувань. Закон "Про інформацію" визначає, що персональні дані можуть збиратися без згоди особи лише в певних випадках, але коли інформація стає масовою, поліція може її збирати. Масова інформація – це дані, що поширюються серед необмеженого кола осіб.

Вищезгадана стаття 6 визначає основи для здійснення оперативно-розшукових дій, які включають перевірку інформації, отриманої законним шляхом, щодо:

- підготовки кримінальних злочинів;
- осіб, що планують злочини;
- осіб, які уникають правосуддя або виконання покарання;
- зниклих безвісти;
- діяльності, що підриває державну безпеку України;
- загрози життю та майну, пов'язаних із службовою діяльністю.

Закон України "Про інформацію" визначає персональні дані як інформацію про ідентифіковану особу. Збір, зберігання, використання та розповсюдження такої інформації без згоди особи дозволяється лише за умов, визначених законом, і в інтересах національної безпеки, економічного благополуччя та захисту прав людини. Однак, коли особиста інформація стає частиною соціальної мережі, вона перетворюється на масову інформацію, доступну широкому колу користувачів.

Стаття 7 Закону “Про оперативно-розшукову діяльність” зобов’язує оперативні підрозділи:

вживати заходів для попередження та розкриття злочинів;

збирати інформацію про протиправну діяльність;

таємно фіксувати докази злочинів;

використовувати технічні засоби для збору інформації;

створювати конспіративні підприємства та інформаційні системи.

Ці положення вказують на можливість використання соціальних мереж для збору інформації, але не встановлюють конкретних орієнтирів. Вони дозволяють збирати інформацію, яка має оперативний інтерес, включаючи встановлення місцезнаходження користувачів та доступ до інформації, закритої для широкого кола осіб. Законодавство дозволяє використовувати новітні технічні засоби без необхідності частого оновлення закону, але вимагає судового рішення для збору інформації, яка не є публічно доступною. З іншого боку, дії, що не обмежують права громадян, можуть здійснюватися без судового дозволу. Закон також передбачає, що певні заходи можуть проводитися лише в рамках оперативно-розшукової справи певної категорії.

Стаття 11 встановлює рамки для співпраці у сфері оперативно-розшукових дій. Частина 1 цієї статті має обов’язковий характер і вимагає від державних органів, підприємств, установ та організацій всіх форм власності надавати підтримку оперативним підрозділам у виконанні їх завдань.

Закон “Про організаційно-правові основи боротьби з організованою злочинністю” є ключовим документом, що регулює використання соціальних мереж у оперативно-розшуковій діяльності. Стаття 15 цього закону дозволяє застосування спеціальних технічних засобів у певних випадках. Зокрема, спецпідрозділи мають право з дозволу прокурора використовувати ці технічні засоби для:

моніторингу, запису та документування дій осіб, підозрюваних у злочинній діяльності;

фіксації фактів телефонних розмов, листування без порушення конфіденційності;

забезпечення особистої безпеки співробітників та учасників кримінального процесу.

В інших випадках спецпідрозділи використовують технічні засоби згідно із Законом “Про оперативно-розшукову діяльність”.

Інформація, отримана з використанням технічних засобів, може

служити доказом у суді.

Ця стаття надає право оперативним підрозділам документувати злочинну діяльність не тільки через телефонні розмови, а й за допомогою інших технічних засобів, включаючи соціальні мережі та штучний інтелект.

Аналізуючи вказані нормативні акти, можна зробити висновок, що українське законодавство має певний фундамент у сфері використання інформації з соціальних мереж для оперативно-розшукових цілей. При цьому закони та підзаконні акти приймалися в різний час і часто мали невизначені або некоректні терміни, що призводило до неоднозначного тлумачення та застосування. Так, термін "соціальна мережа" взагалі відсутній у нормативно-правових актах, що регулюють ці відносини. Особиста інформація користувачів соціальних мереж прямо не вважається конфіденційною, що дозволяє її використання для розкриття злочинів та пошуку зниклих осіб.

Хоча законодавець не передбачив прямої можливості використання інформації з соціальних мереж, особлива конструкція норм дозволяє це робити. Оперативно-розшукові заходи з використанням соціальних мереж можливі як у рамках оперативно-розшукової справи, так і без неї.

Щодо штучного інтелекту, то ця технологія ще не має чіткого правового регулювання, але в Україні вже зроблені перші кроки для його розвитку. У 2020 році була прийнята Концепція розвитку штучного інтелекту, яка визначає основні спрямування його розвитку в країні.

6.3. Міжнародний досвід використання штучного інтелекту та інформації, отриманої за допомогою соціальних мереж, в оперативно-розшуковій діяльності правоохоронними органами

Робота правоохоронних органів ефективно виконується завдяки застосуванню новітніх технологій та методів, що дозволяють оперативно виявляти злочини, особливо в умовах поширення інформаційних технологій.

Як і в Україні, міжнародні правоохоронні органи активно використовують соціальні мережі для моніторингу, що сприяє попередженню та розкриттю злочинів, вчинених як онлайн, так і за допомогою традиційних методів.

Поліція Великобританії використовувала соціальні мережі для

ідентифікації учасників заворушень у Лондоні ще у 2011 році. Тоді громадськість допомогла впізнати осіб на фотографіях, що призвело до ідентифікації понад сотню правопорушників.

Італійська поліція на постійній основі використовує соціальні мережі для слідкування за членами організованої злочинності, зокрема через моніторинг особистих сторінок та аналіз переписки. Facebook співпрацює з правоохоронцями, надаючи необхідну інформацію.

Успіх боротьби з кіберзлочинністю залежить від кваліфікації персоналу. Міністерство внутрішніх справ Великобританії включило в програму навчання поліцейських курс, присвячений збору інформації з соціальних мереж.

Поліція Великобританії визнала значення соціальних мереж у розкритті злочинів, навчаючи молодих детективів збирати інформацію з цифрових пристроїв та соціальних мереж. Це особливо корисно при розслідуванні шантажу та домашнього насильства.

Поліція графства Великий Манчестер використовує Twitter для спілкування з громадянами, публікуючи важливі повідомлення та орієнтування на осіб, що перебувають у розшуку.

Поліція Нової Зеландії затримала грабіжника завдяки підтримці користувачів Facebook, які допомогли ідентифікувати злочинця за опублікованими фотографіями.

Інтерпол використовує соціальні мережі для розшуку осіб, що перебувають у міжнародному розшуку, і планує активно вести розшук злочинців через Інтернет, розміщуючи відео- та фотоматеріали на популярних платформах.

Основні напрями використання соціальних мереж поліцією включають:

отримання оперативної інформації про готові та вчинені злочини;

розшук зниклих осіб та осіб, що уникають правосуддя;

встановлення контакту з особами, що становлять оперативний інтерес.

Правове регулювання використання штучного інтелекту включає нормативні акти, що визначають правила збору та обробки даних, захисту персональних даних та вимоги до використання штучного інтелекту. Загальний регламент про захист персональних даних (GDPR) в ЄС встановлює стандарти захисту приватності, а Європейський парламент працює над створенням правової основи для штучного інтелекту.

У діяльності Національної поліції України використання соціальних мереж стає все більш актуальним для отримання

оперативно-значущої інформації, особливо для розшуку злочинців та зниклих осіб. Підрозділи кримінального аналізу та карного розшуку аналізують дані з соціальних мереж для виявлення інформації, що може сприяти розкриттю злочинів.

6.4 Напрями використання інформації, отриманої за допомогою використання штучного інтелекту, для аналізу соціальних мереж в практичній діяльності Національної поліції України

Оперативні підрозділи Національної поліції України все частіше вдаються до використання інтернет-ресурсів, зокрема таких соціальних мереж, як Instagram, Facebook, TikTok, для отримання важливої оперативної інформації. Аналіз та обробка даних, що циркулюють у цих мережах, стають ключовими для виявлення злочинів, що готуються, та пошуку злочинців і зниклих безвісти осіб [7].

Соціальні мережі можна порівняти з автоматизованими інформаційними системами, які вже використовуються в МВС України. Вони мають певні особливості:

інформація надходить автоматично, без участі поліцейських;

дані в соціальних мережах постійно оновлюються, маючи динамічний характер.

Переваги соціальних мереж як джерела інформації включають:

економію на розробці спеціалізованих баз даних;

вільний доступ до різноманітних інформаційних ресурсів;

доступність інформації;

постійне оновлення та розвиток баз даних;

простота використання завдяки інтуїтивно зрозумілому інтерфейсу;

можливість обробки великих обсягів даних;

цілеспрямований пошук інформації;

наявність усталених систем обліку інформації.

Однак інформаційні системи поліції потребують регулярного технічного обслуговування, що вимагає значних матеріальних витрат.

Основним напрямом використання соціальних мереж є розшук злочинців та зниклих осіб. Ефективність пошуку залежить від наявності попередньої інформації про особу та її активності в інтернеті. Успішний пошук може вимагати створення профілів на сайтах, де ведеться пошук, та використання спеціальних методів для встановлення місцезнаходження особи.

Соціальні мережі також можуть використовувати для безпосереднього контакту з особою та виявлення її зв’язків, що вимагає розробки нових тактик та методик проведення оперативно-розшукових заходів.

Наукова спільнота ще не розробила повноцінної тактики та методики для такого типу діяльності, хоча деякі автори вказують на можливість встановлення контакту з особою, діяльність якої документується.

Завершуючи, слід зазначити, що соціальні мережі стали важливою онлайн-платформою для спілкування та обміну інформацією, що має значення для оперативних підрозділів. Вони допомагають у документуванні злочинної діяльності та вимагають подальших досліджень для розвитку ефективних методів роботи в цій сфері.

Таким чином, використання ШІ для аналізу даних, особливо великих масивів даних соціальних мереж, є одним з найбільш перспективних напрямів інтеграції сучасних технологій в оперативно-розшукову діяльність. ШІ може автономно обробляти інформацію соціальних мереж, забезпечуючи підтримку багатьох напрямів ОРД.

Направленістями використання соціальних мереж у процесі здійснення ОРД можуть бути:

- розробка ШІ-агента для аналізу активності користувачів соціальних мереж;
- створення єдиного реєстру, який зберігатиме всі дані про користувачів соціальних мереж та їх взаємодії;
- використання ШІ для доступу до зашифрованих даних;
- активне впровадження ШІ у використання соціальних мереж в ОРД.

Цей напрям пошуку інформації є обнадійливим, оскільки правоохоронні органи багатьох країн вже активно використовують соціальні мережі для моніторингу та розкриття злочинів.

За цих обставин обов’язковим залишається дотримання принципу законності, який забезпечує баланс між використанням ШІ у ОРД та захистом прав людини, включаючи етичне використання ШІ, прозорість прийняття рішень та встановлення контролю за діяльністю ШІ.

6.5. Перспективи використання штучного інтелекту при здійсненні відеоспостереження в рамках превентивної діяльності

Правоохоронні органи повинні адаптуватися до технологічних змін, щоб ефективно реагувати на нові форми злочинності. Тому системи відеоспостереження, які є одними з найбільш ефективних інструментів для виявлення та розкриття правопорушень, а також здійснення

превентивної функції були інтегровані у діяльність правоохоронних органів. Завдяки можливостям нейромереж ці системи тепер не тільки фіксують порушення, а й аналізують зібрані дані, що дозволяє глибше розуміти різноманітні ситуації.

У часи, коли штучний інтелект активно розвивається, правоохоронці мають можливість використовувати цю технологію у практичних цілях. Наразі ШІ вже забезпечує автономність багатьох процесів, які раніше залежали від людської участі, або менш ефективних технологій. Станом на 2024 рік ШІ перевершує людські можливості у багатьох областях, підтверджуючи свою перевагу над традиційними методами. Фіксація умовного моменту перевершення можливостей ШІ над людськими можливостям наведена на рис. 6.1.

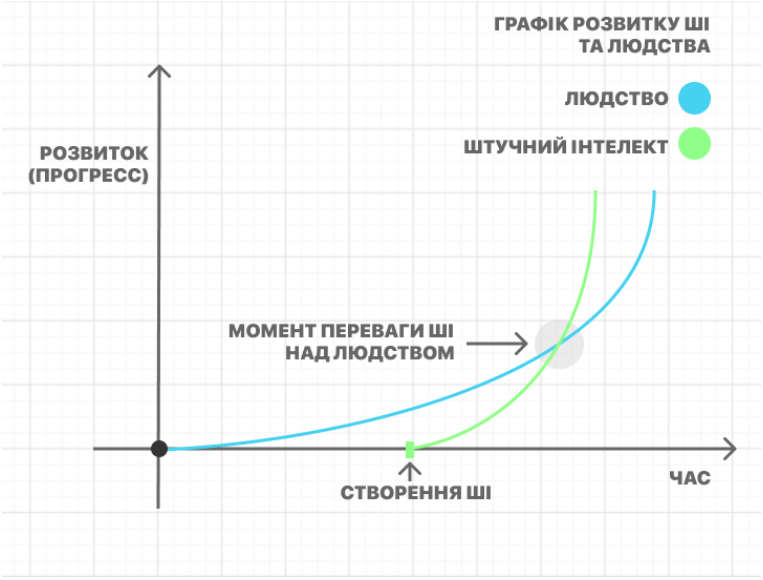


Рис. 6.1. Фіксація умовного моменту перевершення можливостей ШІ над людськими можливостями

Інтеграція ШІ у правоохоронну діяльність не обмежилася лише системами відеоспостереження. Це також включає роботу ситуаційних центрів, інформаційної підсистеми “Гарпун” інформаційного порталу Національної поліції та автоматизованих систем відеофіксації. ШІ сприяє автоматизації багатьох процесів, які раніше виконували працівники відповідних підрозділів. Основною перевагою використання ШІ у системах відеоспостереження є здатність обробляти великі обсяги даних та виявляти закономірності, що раніше були недоступні.

6.6. «Штучний інтелект-агент» як найбільш перспективна система організації відеоспостереження з використанням штучного інтелекту: поняття, передумови створення та процес реалізації

Система відеоспостереження – це комплекс заходів та технологій, які забезпечують візуальне спостереження, запис, аналіз та архівацію відеооб'єктів чи процесів, як у режимі реального часу, так і для подальшого використання. Вона включає в себе різноманітне обладнання та програмне забезпечення, що застосовуються як у приватному секторі, так і в галузях державного управління, національної безпеки та правопорядку. Структура системи може бути як простою, наприклад, однокамерною системою для моніторингу невеликої зони, так і складною, як у випадку мережевих систем з сотнями камер, пов'язаних з центральним контрольним центром. Основні елементи включають відеокамери, засоби зберігання, сервери, програмне забезпечення для керування відео та монітори для перегляду. Різноманітність камер дозволяє налаштувати систему для задоволення специфічних потреб – від базових аналогових до передових цифрових IP-камер з функціями обертання, зуму та автоматичного слідкування. Завдяки новітнім технологіям, таким як розпізнавання облич та відеоаналітика, відеоспостереження стає ще більш ефективним, збільшуючи можливості автоматизації безпекових процедур.

Загалом відеоспостереження є важливим інструментом як у сфері безпеки та контролю, так і у сфері превентивної діяльності, який своєю чергою продовжує розвиватися завдяки постійному технологічному прогресу. Водночас воно має знаходити баланс між забезпеченням безпеки та повагою до прав і свобод особистості.

ШІ-агент – це інтелектуальна система, що використовується в інформаційних системах для аналізу дій об'єктів та пов'язаних з ними факторів, базуючись на Blockchain технології. Вона відповідає таким принципам: детальний аналіз активності об'єктів та їх контексту; створення інтелектуальних суб'єктів; часткова самостійність; забезпечення таємниці та цілісності інформації.

ШІ-агент може функціонувати на електронних пристроях користувачів, які є предметом його аналізу, і взаємодіяти з Blockchain базами даних. Кожна особа може мати персонального ШІ-агента на своєму пристрої для здійснення кримінально-правової або адміністративної діяльності.

Система, яка гарантує точність, конфіденційність, цілісність

інформації та її децентралізацію, є ключовою для забезпечення інформаційної безпеки. Дотримання цих принципів у сферах з високими вимогами до безпеки даних є критичним для здобуття довіри громадян до обробки їхніх персональних даних.

Використання нейромереж для аналізу значних даних відкриває нові перспективи для розуміння поведінкових патернів, що може сприяти глибшому інсайту в соціальні процеси. Такий аналіз може бути корисним для правоохоронних органів та покращення життя громадян через інтеграцію інноваційних рішень. Це створює можливості для розвитку безпечнішого та ефективнішого суспільства, де технології підвищують якість життя та оптимізують управлінські процеси.

Інтеграція штучного інтелекту (ШІ) у системи відеонагляду має відповідати сучасним тенденціям розвитку цієї технології, яка є однією з найбільш перспективних у сучасному світі. Необхідність такої інтеграції обумовлена значним впливом систем відеонагляду на ефективність правоохоронних органів, тому будь-які зміни в системі повинні базуватися на актуальних і регульованих підходах, щоб уникнути потенційних ризиків. Розвиток ШІ відбувається паралельно з дискусіями про його безпеку в суспільстві. Основними критеріями успіху систем ШІ є їх ефективність та безпека.

Встановлення цих критеріїв як цілей дозволяє успішно інтегрувати ШІ у різні сфери, включаючи діяльність правоохоронних органів для забезпечення безпеки на дорогах. Врахування критерію безпеки ШІ допомагає виявляти та усувати ризики, формуючи безпечне середовище для ШІ.

Видатні дослідники в галузі ШІ вказують на непередбачуваність поведінки ШІ як на причину багатьох проблем, споріднених з його безпечним застосуванням. Це пов’язано з нездатністю людини обробити всі дані, які може опрацювати ШІ, що ускладнює повне розуміння мотивації ШІ. Таким чином, одним з чільних завдань при інтеграції ШІ є визначення та прогнозування його мотивації, щоб запобігти діям ШІ, які можуть призвести до непередбачуваних суспільних ризиків.

Основна проблема, що стоїть перед штучним інтелектом (ШІ), полягає у розбіжності між його мотивацією та мотивацією суспільства, особливо в контексті труднощів із прогнозуванням та контролем мотивації ШІ. Широкомасштабне впровадження ШІ може відповідати загальним суспільним очікуванням, але непередбачуваність залишається проблемою, особливо в централізованих системах нейромереж. Ця невідповідність, навіть з урахуванням потенціалу ШІ, може становити загрозу для суспільства. Тому важливо розробити систему, яка б

мінімізувала ризики, пов’язані з розбіжностями між мотивацією ШІ та суспільства.

Децентралізація технології ШІ може сприяти врахуванню всіх аспектів суспільної мотивації, оскільки достатня кількість окремих ШІ-суб’єктів може аналізувати індивідуальні випадки мотивації. Цей підхід відповідає закону діалектики Гегеля, де якісні зміни переходять у кількісні. Однак у цьому контексті “якісні” аспекти не страждають, оскільки варіативність мотивації одного суб’єкта недостатньо значуща для застосування екстраполяції. На відміну від централізованого ШІ, який екстраполює дані, децентралізовані суб’єкти обробляють менші обсяги даних, але здійснюють це більш повно і точно. Екстраполяція умовиводів централізованого ШІ, на відміну від моделі ШІ-агент, наведена на рис. 6.2.

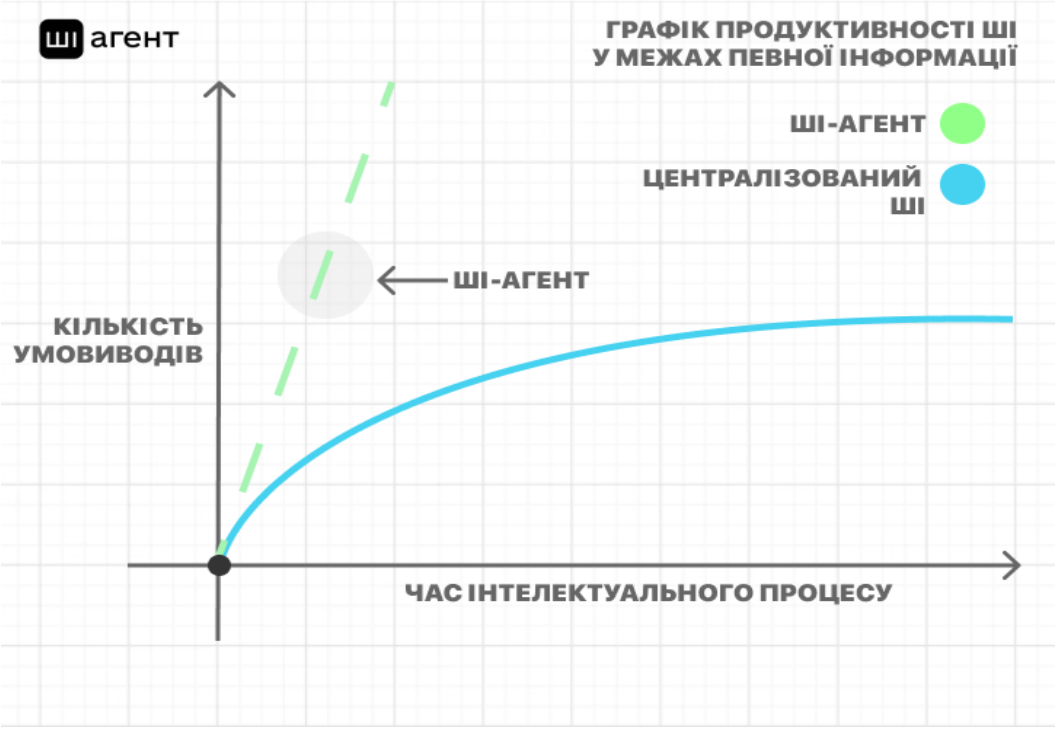


Рис. 6.2. Екстраполяція умовиводів централізованого ШІ, на відміну від моделі ШІ-агент

Децентралізація штучного інтелекту (ШІ) сприяє впровадженню принципу плюралізму, який є основою для створення екосистеми ШІ, де кожен агент враховує мотивацію інших, знижуючи ризики невідповідностей між ними. У такій системі відома мотивація кожного агента дозволяє уникнути непередбачуваності їхніх дій. На відміну від централізованих систем, де прогнозування поведінки ШІ ускладнене, розгалуження на автономні суб’єкти полегшує цей процес, сприяючи

відповідності мотивації ШІ суспільним цілям. Принцип передбачення базується на діяльності ШІ, яка повинна відображати мотивацію суспільства, особливо коли ШІ створюється для досягнення конкретних цілей. Це досягається через аналіз людських дій та їх відтворення у поведінці ШІ. Таким чином, формується система, де ШІ-агенти відтворюють мотивацію людей, враховуючи інтереси всіх суб'єктів суспільства та забезпечуючи глибший аналіз даних. Використання технології blockchain у системах відеоспостереження з ШІ забезпечує безпеку даних, неможливість їх зміни без згоди всіх учасників мережі, та стійкість до втручань. Blockchain також підвищує продуктивність ШІ, оптимізує обробку даних, забезпечує прозорість та децентралізацію, продукуючи роботу ШІ більш об'єктивною та надійною. ШІ-агенти, що працюють на принципі самоконтролю, усувають корупцію та зловживання владою, відображаючи принципи суспільної волі, закладені в основі їх навчання, як, наприклад, принципи Конституції України. Таке поєднання blockchain та ШІ відкриває нові можливості для забезпечення безпеки та довіри в цифровому світі.

Міністерство цифрової трансформації України (Мінцифри) активно працює над стратегією регулювання штучного інтелекту в країні, використовуючи підхід "bottom-up" для співпраці з концепцією ШІ-агента. Уряд підтримує цю ініціативу, що сприяє розвитку правової бази та залученню громадськості до дискусій. Такий підхід дозволяє враховувати різні точки зору та інтереси при формуванні стратегій використання ШІ.

Технічні аспекти системи ШІ передбачають обмеження інформації, що використовується, до даних, які безпосередньо стосуються діяльності людей, включаючи транспортні засоби. Це забезпечується за допомогою методів ідентифікації та аналізу, які обмежуються лише необхідними даними, підвищуючи ефективність системи ШІ.

Встановлення технології на пристрої користувачів відповідає двом основним вимогам: технічній можливості підтримки системи та забезпеченню прозорості для користувачів, які можуть безпосередньо спостерігати за результатами діяльності системи. Це включає складність створення хмарних технологій для аналізу публічної безпеки та необхідність використання потужних комп'ютерів для обробки великої кількості даних. Розподіл процесів аналізу між пристроями користувачів дозволяє збалансувати навантаження та забезпечити прозорість обробки даних. Основні формати фіксації системи відеоспостереження з використанням ШІ наведені на рис. 6.3.

Рис. 6.3. Основні формати фіксації системи відеоспостереження з використанням ШІ

Система ШІ-агента сприяє створенню безпечного середовища для систем відеоспостереження, що є ключовим для їх довгострокового розвитку та ефективності. Ефективне використання технологій ШІ виступає як важливий фактор, який з часом може стати фундаментальним у формуванні різноманітних систем, не обмежуючись лише відеоспостереженням. Інтеграція ШІ у діяльність правоохоронних органів забезпечує відповідність високим стандартам безпеки та ефективності, що є необхідним для успішного впровадження інтегрованих технологій ШІ.

6.7. Реалізація системи «Штучний інтелект-агент»

ШІ-агент втілюється у систему, що інтегрується з інструментами збору даних, blockchain базою та пристроями користувачів із вбудованими нейромережами. Основна вимога до засобів збору даних полягає у сумісності форматів даних для аналізу моделлю ШІ. Blockchain база слугує для зберігання даних, необхідних державним органам, та

передачі їх на пристрої користувачів. Після імпортування даних до бази відбувається ідентифікація або реєстрація об'єктів. ШІ-агент на пристрої користувача аналізує дані, запитуючи інформацію з blockchain бази та обробляючи її за допомогою нейромережі. Результати аналізу потім зберігаються у новому блоці blockchain бази. Технологія, розроблена спільно з компанією evergreens, вже застосовується у бізнесі та є кроком до впровадження ШІ-агента у правоохоронній сфері.

Пристрої користувачів, на яких встановлено ШІ-агента, повинні відповідати технічним вимогам та забезпечувати безперервну роботу агента. Аналіз даних ШІ-агентом не повинен перевантажувати пристрій, а його діяльність має контролюватися антивірусами та системами виявлення збоїв.

У разі втрати зв'язку між ШІ-агентом та базою даних відповідальність може покладатися на користувача пристрою з встановленим агентом. Це забезпечує відповідальність за збереження зв'язку та інтегритет даних, що є важливим для ефективності системи. У разі навмисного порушення зв'язку ситуація може розглядатися як правопорушення, але якщо втрата зв'язку сталася без умислу, необхідно надати час для відновлення роботи ШІ-агента. Це запобігає можливості обходу системи нагляду зловмисниками. Процес діяльності ШІ-агента наведено на рис. 6.4.

Рис. 6.4 Процес діяльності ШІ-агента

Процес функціонування:

1) Інформація про публічні місця фіксується та імпортується з систем відеоспостереження у Blockchain базу даних, проходячи через процес ідентифікації.

2) Дані зберігаються у Blockchain базі даних.

3) Конкретні дані (ідентифіковані) експортуються із Blockchain бази даних за запитом ШІ-агента на технічний пристрій із встановленим ШІ-агентом.

4) ШІ-агент аналізує дані за допомогою нейромережі, фіксуючи певні об’єкти, обставини та закономірності із наданої інформації.

5) Результати аналізу експортуються у Blockchain базу даних у вигляді створення нового блоку.

6.8. Правова регламентація використання «штучного інтелекту-агента» у забезпеченні відеофіксації

В епоху широкого впровадження цифрових технологій, зокрема в сфері діяльності Міністерства внутрішніх справ України, було розроблено низку законодавчих актів, які закладають основу для інтеграції технологій штучного інтелекту (ШІ) в системи відеоспостереження. Ці правові рамки ґрунтуються на ряді нормативних документів, включаючи Закон України “Про захист персональних даних” та рішення Кабінету Міністрів, які регулюють функціонування систем фіксації порушень і єдиної інформаційної системи МВС.

Зареєстрований у 2024 році законопроєкт про створення єдиної системи відеомоніторингу в публічних місцях має на меті встановлення уніфікованої та ефективної мережі спостереження для підвищення громадської безпеки [14]. Пропонується встановлення відеокамер у ключових і чималих публічних просторах для покращення реагування на злочини та підвищення безпеки громадян. За цих обставин забезпечується захист особистих даних відповідно до українського законодавства та стандартів ЄС.

Заступник міністра внутрішніх справ підкреслив, що існуюча система відеонагляду потребує уніфікації стандартів для підвищення її ефективності. Законопроєкт також передбачає вдосконалення системи ідентифікації осіб з метою забезпечення балансу між безпекою та приватністю.

Цей законопроєкт є кроком до створення більш ефективного механізму для забезпечення громадської безпеки, одночасно

наголошуючи на важливості захисту особистих даних. Він відкриває шлях для технологічних інновацій та зміцнення правової бази для захисту даних, сприяючи інтеграції ШІ в системи відеоспостереження для ефективного виявлення та реагування на злочинні дії.

Законопроєкт має потенціал значно підвищити ефективність роботи правоохоронних органів, зокрема в сфері безпеки дорожнього руху, завдяки широкому впровадженню відеонагляду. Він також зосереджує увагу на захисті особистих даних та приватності, передбачаючи розвиток правових норм та введення контрольних механізмів для забезпечення дотримання стандартів. Система ШІ-агент буде відповідати принципам прозорості та конфіденційності, забезпечуючи цілісність даних. Основні критерії системи ШІ-агент у межах інформаційної безпеки наведено на рис. 6.5.

Рис. 6.5 Основні критерії системи ШІ-агент
у межах інформаційної безпеки

Цей законопроєкт про відеомоніторинг у публічних місцях відображає прагнення України до впровадження передових технологій та відповідності сучасним правовим стандартам, з акцентом на важливість збереження балансу між безпекою та особистими правами громадян. Технології, такі як “штучний інтелект-агент” та системи відеоспостереження, знаходяться в центрі юридичних дебатів в Україні, де обговорюються їх доцільність, етичність та законодавче регулювання. Правові основи для їх використання розглядаються в контексті існуючих законів, директив ЄС та міжнародного досвіду [15].

Закон України “Про захист персональних даних” встановлює юридичні рамки для обробки даних, зібраних через відеоспостереження та ШІ, вимагаючи, щоб така обробка була законною, справедливою та прозорою та мала законну підставу або згоду особи.

Україна у відповідь на швидкий розвиток цифрових технологій прагне адаптувати своє законодавство, знаходячи баланс між підтримкою інновацій та захистом прав громадян. Це вимагає спільних зусиль уряду, законодавців, громадськості та експертів.

Правові основи використання ШІ у відеоспостереженні є ключовими для забезпечення законності та прозорості. Важливо, щоб використання ШІ відповідало законодавству та поважало приватність та права громадян, що сприятиме розвитку систем відеоспостереження на благо суспільства, забезпечуючи безпеку та дотримання прав людини.

6.9. Міжнародні правові акти у сфері використання «штучного інтелект-агента» та систем відеоспостереження

Міжнародні нормативні акти є першочерговими у визначенні універсальних стандартів для регулювання використання технологій штучного інтелекту та систем відеоспостереження, особливо з огляду на їх стрімкий розвиток та потенційний вплив на права людини та етику. Зростаюча потреба у міжнародному регулюванні вимагає уваги до основоположних документів, які встановлюють керівні принципи для “штучного інтелект-агента” та систем відеонагляду.

GDPR, як основний регуляторний документ ЄС, визначає правила збору та обробки персональних даних, підкреслюючи важливість прозорості та конфіденційності. Він вимагає, щоб системи, такі як “ШІ-агент з blockchain базою даних”, відповідали цим принципам [16].

Конвенція 108, як один з перших міжнародних документів про захист даних, акцентує на необхідності захисту прав людини у контексті автоматичної обробки даних, встановлюючи стандарти прозорості та безпеки даних.

AI Act 2024 року, прийнятий ЄС, є піонерським документом, який встановлює комплексні правила для ШІ, враховуючи різні рівні ризику. Цей акт підкреслює необхідність прозорості, справедливості, відповідальності та захисту даних у роботі з ШІ, вимагаючи від компаній забезпечення зрозумілості своїх систем [17].

Завдяки цим міжнародним правовим актам формується глобальний підхід до регулювання ШІ та відеоспостереження, що сприяє

відповідальному розвитку технологій з повагою до прав людини. Водночас існують виклики, пов'язані з практичним застосуванням цих принципів та їх дотриманням, що вимагає балансу між інноваціями, етикою, безпекою та приватністю. Концепція "ШІ-агент з blockchain базою даних" може відповідати цим викликам, створюючи безпечне середовище для інтеграції ШІ, зокрема у сферу відеоспостереження.

Таким чином, концепція "ШІ-агент з blockchain базою даних" відображає ключові принципи інформаційної безпеки, які є важливими для забезпечення безпеки дорожнього руху. Система підтримує цілісність, точність, конфіденційність інформації та децентралізацію, що є критичними для захисту інформації. Цілісність забезпечує незмінність даних, точність гарантує їх вірогідність, а конфіденційність захищає особисту інформацію. Децентралізація допомагає вирішувати проблеми корупції та зловживання владою.

В Україні вже створено правову основу для інтеграції ШІ в системи відеоспостереження, що використовуються для забезпечення заходів превенції та інших функцій служб Національної поліції. Впровадження публічного ШІ-агента може поліпшити фіксацію та аналіз правопорушень у суспільних місцях, надаючи співробітникам органів та підрозділів якісні дані для розслідувань. У процесі здійснення інформаційно-аналітичної діяльності ШІ може обробляти великі обсяги даних, недоступні для людської обробки. А це сприятиме розвитку нових технологій та методів у діяльності органів та підрозділів Національної поліції України, зменшуючи ризики правопорушень та уникнення відповідальності.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які основні сфери застосування штучного інтелекту (ШІ) у діяльності Національної поліції?
2. Як ШІ може допомогти в автоматизації процесу аналізу великих обсягів даних для розслідування злочинів?
3. Які методи машинного навчання можуть використовуватись для прогнозування злочинної активності?
4. Які етичні питання виникають при застосуванні ШІ у правоохоронній діяльності?
5. Як забезпечити конфіденційність та захист персональних даних у системах з використанням ШІ?
6. Які є приклади успішного застосування ШІ для забезпечення громадської безпеки в інших країнах?
7. Які ризики та виклики можуть виникати при застосуванні ШІ у слідчих діях?

8. Як можна використовувати обробку природної мови для аналізу відкритих джерел та соціальних мереж?

9. Які ресурси та підготовка потрібні для ефективного впровадження ШІ в інформаційно-аналітичну діяльність поліції?

10. Яким чином алгоритми ШІ можуть підтримувати процеси прийняття рішень на основі зібраної інформації?

ЛІТЕРАТУРА ЗА РОЗДІЛОМ:

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, N 30, ст. 141) URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

2. Закон України "Про Національну поліцію" (Відомості Верховної Ради (ВВР), 2015, № 40-41, ст.379) URL: https://zakon.rada.gov.ua/laws/show/580-19#Text

3. Закон України "Про оперативно-розшукову діяльність" (Відомості Верховної Ради України (ВВР), 1992, № 22, ст. 303) URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text

4. Закон України "Про інформацію" (Відомості Верховної Ради України (ВВР), 1992, N 48, ст.650) URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

5. Закон України "Про доступ до публічної інформації" (Відомості Верховної Ради України (ВВР), 2011, N 32, ст.314) URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

6. Закон України "Про організаційно-правові основи боротьби з організованою злочинністю" (Відомості Верховної Ради України (ВВР), 1993, № 35, ст.358) URL: https://zakon.rada.gov.ua/laws/show/3341-12#Text

7. Бочковий О.В., Звонок Є.О. Віртуальні соціальні мережі як джерела оперативно значимої інформації для підрозділів карного розшуку МВС України \ збірник матеріалів конференції. Х. 2010 р. – С. 58-62.

8. Зомбі-вірус [Електронний ресурс]. – Режим доступу до статті "Зомбі-вірус" URL: https://uk.wikipedia.org/wiki/%D0%97%D0%BE%D0%BC%D0%B1%D1%96_(%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0)

9. Рижков Е.В. Протидія кіберзлочинам в період воєнного стану в Україні / Е.В. Рижков // Науковий вісник Дніпроп. держ. ун-т внутр. справ URL: https://visnik.dduvs.in.ua/wp-content/uploads/2023/04/S1/NV_DDUVS_spec_1_2022-55-60.pdf

10. Кабінет Міністрів України. Розпорядження від 2 грудня 2020 р. № 1556-р Про схвалення Концепції розвитку штучного інтелекту в Україні. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text

11. Ілон Маск і група експертів закликали призупинити роботу над ШІ через ризики для суспільства [Електронний ресурс] URL:

https://forbes.ua/news/ilon-mask-zaklikav-prizupiniti-robotu-nad-shi-cherez-riziki-dlya-suspilstva-29032023-12714

12. Еволюція штучного інтелекту (ШІ): Визначні моменти в історії та застосування [Електронний ресурс] URL: https://cases.media/en/article/evolyuciya-shtuchnogo-intelektu-shi-viznachni-momenti-v-istoriyi-ta-zastosuvannya

13. Впровадження технологій штучного інтелекту у забезпечення національної безпеки та обороноздатності України: проблеми та перспективи повоєнного періоду [Електронний ресурс] URL: https://coordynata.com.ua/vprovadzenna-tehnologij-stucnogo-intelektu-u-zabezpecenna-nacionalnoi-bezpeki-ta-oboronozdatnosti-ukraini-problemi-ta-perspektivi-povoennogo-periodu

14. Проєкт Закону Країни Про єдину систему відеомоніторингу стану публічної безпеки. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=77597

15. Регламент (ЄС) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб щодо обробки персональних даних і про вільний рух таких даних, а також про скасування Директиви 95/46/ЄС [Електронний ресурс] URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

16. Конвенція про захист осіб щодо автоматизованої обробки персональних даних (ETS № 108) [Електронний ресурс] URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

17. Європарламент ухвалив перший у світі закон про штучний інтелект [Електронний ресурс] URL: https://cedem.org.ua/news/eu-zakon-pro-shtuchnyi-intelekt/

РОЗДІЛ 7. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ ОБЛИЧЧЯ НА ВІДЕО- ТА ФОТОЗОБРАЖЕННЯХ

Проблема встановлення осіб, які вчинили злочини як кримінального, так і адміністративного характеру, є важливою складовою діяльності правоохоронних органів. Починаючи з початку війни, правоохоронці Національної поліції та прокуратури зіткнулися з розслідуванням нових видів злочинів, які раніше не були типовими. Одним з таких завдань є ідентифікація осіб, які вчиняли злочинні дії чи видали накази на вчинення злочинів. Ця проблема особливо актуальна в контексті воєнних злочинів проти цивільного населення, які часто вчинялися відносно осіб, які підлягали катуванням та покаранням за будь-яку, навіть уявлену, нелояльність до окупантів. Ці злочини можуть бути вчинені як російськими військовими, так і колаборантами з України, і вимагають ідентифікації в рамках кримінальних проваджень.

Залишається актуальним і питання ідентифікації колаборантів на тимчасово окупованих територіях, які співпрацюють з окупаційною владою. Деякі з них можуть бути завербовані російськими спецслужбами та здійснювати підривну діяльність, намагаючись проникнути на територію України як нелегальними, так і законними шляхами. Таким чином, ідентифікація таких осіб стає надзвичайно важливою для національної безпеки. Під час досудового розслідування правоохоронні органи можуть мати фото- або відеоматеріали, на яких зображені підозрювані особи. Проте перевірка цих зображень за допомогою відомчих баз даних може бути ефективною лише щодо громадян України, які мали правопорушення раніше.

У зв'язку з цим іноді потрібно використовувати відкриті джерела для ідентифікації підозрюваних. Проте існуючі методи, такі як "OSINT-технології", не завжди призводять до позитивних результатів у встановленні осіб. Тому в даному дослідженні ми спробуємо розглянути механізми та методи ідентифікації осіб за їх обличчями, а також існуючі програмно-інформаційні системи, які допомагають у цьому процесі.

7.1. Особливості технології розпізнавання обличчя

Сьогодні однією з актуальних проблем є розпізнавання облич осіб на фото та відео. Цікавим є сам процес виконання відеоспостереження. Сучасні камери для ефективного відеоспостереження можуть забезпечувати високоякісне зображення у будь-який час доби та мати широкий кут огляду з відповідними основними параметрами. Відеоспостереження спрямоване на ідентифікацію осіб за обличчям для створення баз даних спостереження.

Важливо відрізняти процес виявлення та розпізнавання облич. Під час виявлення збираються фото- та відеозаписи, отримані від камер відеоспостереження, і проводиться їх обробка за допомогою спеціального програмного забезпечення. Виявлення особи становить основу для подальшого аналізу інформації. Під час розпізнавання відбувається аналіз для порівняння характерних особливостей особи. Фото та відеозаписи містять інформацію про дату та час зйомки, що полегшує відбір даних для подальшого використання.

Існують два основні методи розпізнавання обличчя: у статичному та динамічному потоках. Камери відеоспостереження Dahua використовують ці методи для ідентифікації осіб. Інформація з камер передається на сервер, де вона декодується, класифікується та додається до бази даних. Програма класифікує обличчя за різними категоріями, такими як стать, вік, особливі прикмети та одяг.

Сучасні системи використовують спеціальні алгоритми для розпізнавання та ідентифікації об'єктів спостереження, що дозволяє швидко знайти необхідну інформацію. Спостереження може відбуватись в офісах, школах, банках, магазинах, на вулицях та в інших місцях. Отримані дані дозволяють ефективно аналізувати та приймати рішення в реальному часі.

7.2. Сфери застосування систем відеоспостереження

Системи відеоспостереження, які можуть ідентифікувати особу на основі аналізу обличчя та інших біометричних параметрів, широко використовуються у сфері громадської безпеки. Криміналісти застосовують автоматизовані системи біометричної ідентифікації (ABIS) для порівняння різних типів біометрії. Головними користувачами таких систем є органи правопорядку, які використовують їх для боротьби зі злочинністю та тероризмом.

Використання систем розпізнавання облич має для поліції великі переваги у виявленні та запобіганні злочинам. Ці системи також застосовуються під час видачі документів для ідентифікації особи, а також у поєднанні з іншими біометричними технологіями, наприклад, відбитками пальців.

Отримані зображення облич через системи відеоспостереження можуть використовуватись при прикордонних перевірках для порівняння з власником біометричного паспорта (рис. 7.1). Це спрощує процес перетину кордону та забезпечує безпеку прикордонних перевірок.

Ще одним застосуванням камер розпізнавання обличчя є їх використання на безпілотних літальних апаратах для масових заходів на великій площі. Системи безпілотників можуть ідентифікувати об'єкти спостереження на висоті до 100 метрів.

Системи відеоспостереження з розпізнаванням облич також знаходять застосування у сфері національної безпеки, де вони допомагають у пошуку зниклих чи викрадених осіб, виявленні злочинців та наданні інформації для розслідування злочинів (рис. 7.2):

Рис. 7.1. Ідентифікація осіб при перетині кордону

Рис. 7.2. Камери зовнішнього відеоспостереження

Ці системи дозволяють поліцейським швидко знаходити та ідентифікувати осіб, яких необхідно розшукати, використовуючи їх фотографії у відповідних системах. Сучасні технології дозволяють здійснювати відеоаналітику для пошуку зниклих осіб та виявлення їх можливого місцеперебування.

Системи відеоспостереження проводять аналіз фотографій в базах даних та швидко знаходять збіги з відсотком точності від 70% до 90%. Розпізнавання обличчя може відбуватись не лише за самим обличчям, але й за очима, одягом та манерами поведінки.

Застосування сучасних систем відеоспостереження допомагає покращити безпеку та швидко реагувати на потенційні загрози у різних сферах – від громадського транспорту до великих заходів на відкритих майданчиках.

7.3. Технологія комп’ютерного зору

Комп’ютерний зір – це технологія, що створює комп'ютерні засоби для проведення, виявлення, спостереження та класифікації об'єктів. Використання штучного інтелекту для аналізу та розпізнавання об'єктів є перспективним напрямом наукових досліджень.

Однією з найпопулярніших проблем у цьому спрямуванні є розпізнавання облич. Світовими лідерами в цій галузі є технологія Face ID від Apple, яка використовується у соціальних мережах для розпізнавання осіб на фотографіях. Крім того, Facebook розробив алгоритм, який засвідчив ефективність розпізнавання облич у 93% випадків.

Для розпізнавання облич були створені бібліотеки та API, такі як OpenCV та dlib, які широко використовуються в проєктах з розпізнавання.

7.4. Технології розпізнавання облич

Розпізнавання облич за допомогою сервісів, таких як Facebook DeepFace та Apple Face ID, відображає різні підходи та характеристики.

Система Facebook DeepFace розроблена спеціально для соціальної мережі Facebook. Вона вражає ефективністю розпізнавання облич на рівні близько 97,25%, що є досить вражаючим показником. Її перевагами є велика кількість доступних даних для пошуку та розпізнавання облич.

Однак система вимагає значних апаратних ресурсів та адаптована лише під використання у межах Facebook, що може обмежувати її застосування в інших сценаріях.

З іншого боку, система Apple Face ID спрямована на авторизацію власника телефону і використовує унікальне апаратне забезпечення для покращення ефективності розпізнавання. Вона володіє високою ефективністю, можливістю розпізнавання облич при різних умовах освітлення та має додатковий шар захисту від недостовірної інформації. Проте для користування цією системою потрібне спеціальне апаратне забезпечення, і вона доступна лише на пристроях від Apple.

Отже, обидва сервіси мають свої переваги та недоліки, і вибір між ними може залежати від конкретних потреб і вимог користувача.

Сервіс Microsoft Face API є потужним інструментом для побудови систем розпізнавання облич з широким спектром функцій, включаючи пошук, ідентифікацію, групування, знаходження подібних облич та визначення характеристик, таких як вік, стать та емоційний стан. Особливістю є те, що ця система надає доступ стороннім розробникам через API, що сприяє розробці різноманітних додатків на основі цієї технології. Висока ефективність розпізнавання та можливість використання серверів Microsoft для операцій пошуку є її перевагами.

З іншого боку, сервіс має свої недоліки, зокрема, відсутність можливості додаткових налаштувань та залежність розробки від стороннього API, що може обмежувати гнучкість та контроль над системою.

Система Aware Nexa|Face пропонує комплексний підхід до ідентифікації та автентифікації особи у складі біометричної системи. Вона включає в себе різноманітні модулі, такі як розпізнавання відбитків пальців, сітківки ока, голосу та тексту. Ця система має високу ефективність розпізнавання та захищеність, а також можливість підключення додаткових модулів для посилення функціональності. Однак комплексність та висока вартість можуть бути серйозними недоліками цієї системи.

Система розпізнавання облич Samsung Face Recognition розроблена для використання в флагманських моделях S серії і є зручним засобом підтвердження особи без потреби у додатковому апаратному забезпеченні, як у випадку з Apple Face ID. Додаткові захисні шари, такі як Secure Folder і система Knox, забезпечують високий рівень безпеки важливих даних користувача, а також захист від несанкціонованого доступу.

Однією з унікальних особливостей системи Samsung Face Recognition є можливість розпізнавання зіниці ока, що додає додатковий

рівень аутентифікації. Однак серед недоліків можна відзначити можливість недостовірного розпізнавання, особливо при поганому освітленні, а також обмеження в технології, яка може використовуватися лише в продукції Samsung.

7.5. Сфери використання CV

Застосовування технологій комп'ютерного зору (CV) має широкий спектр використань у різних сферах суспільного життя. Ось деякі з них:

1. **Виробництво**. CV використовується у великому та малому виробництві для автоматизації та контролю якості. Промислові роботизовані системи вживаються для автоматизації збору, обробки та упаковки продукції, а також для контролю якості виробництва (рис. 7.3).

2. **Транспорт**. CV застосовується для розробки систем автономного керування автомобілями. Наприклад, компанія Tesla впровадила систему автопілота, яка дозволяє автомобілю керувати без участі водія на основі аналізу відео- та сенсорних даних (рис. 7.4).

Рис. 7.3. Камери відеоспостереження на виробництві


Рис. 7.4. Відеоспостереження в транспорті

3. **Шопінг**. Введення розумних та автономних супермаркетів, які не потребують касирів, є інноваційною технологією, що впроваджується компанією Amazon. CV використовується для виявлення товарів в кошику покупця та автоматичного нарахування вартості без необхідності перебувати в черзі (рис. 7.5).


Рис. 7.5. Відеоспостереження в торговельних центрах

4. Медицина. CV застосовується для аналізу медичних зображень, таких як рентгенівські знімки та томографія. Системи CV допомагають у автоматизації аналізу результатів досліджень, надають базові приписи та рекомендації щодо лікування на основі обробки цих зображень (рис. 7.6).

Рис. 7.6. Відеоспостереження в медицині

Системи взаємодії, організації інформації та безпеки використовують технології комп'ютерного зору для різноманітних завдань.

5. Системи взаємодії. Технології комп'ютерного зору використовуються для розуміння жестів людини, виявлення її емоцій та іншої візуальної інформації. Наприклад, відеоспостереження в банках може застосовуватися для виявлення підозрілих дій або реакцій клієнтів.

6. Системи організації інформації. Технології CV застосовуються для індексації баз даних зображень, відслідковування та автоматизації доступу до об'єктів на цих зображеннях. Це допомагає у швидкому та ефективному пошуку та обробці великої кількості візуальної інформації.

7. Безпека. Системи розпізнавання облич, такі як Face ID та Nexa|Face, використовуються для забезпечення безпеки, а також відеоспостереження застосовується в широкому спектрі ситуацій, включаючи поліційні підрозділи. У таких умовах технології CV допомагають у пошуку, виявленні та розкритті різних злочинів та порушень правопорядку.

Технології комп'ютерного зору мають важливе значення для забезпечення безпеки в Україні, особливо в умовах воєнного конфлікту. Підрозділи Національної поліції використовують різноманітні системи відеоспостереження та системи розпізнавання облич для виявлення злочинців, здійснення пошуку та затримання осіб, які порушують правопорядок (рис 7.8).

У таких ситуаціях технології комп'ютерного зору можуть допомогти в знаходженні осіб, яких розшукують, виявленні та розкритті різних злочинів, включаючи крадіжки, терористичні акти та воєнні злочини. Завдяки використанню цих технологій поліція може ефективніше реагувати на загрози безпеці та забезпечувати захист громадян і території країни.

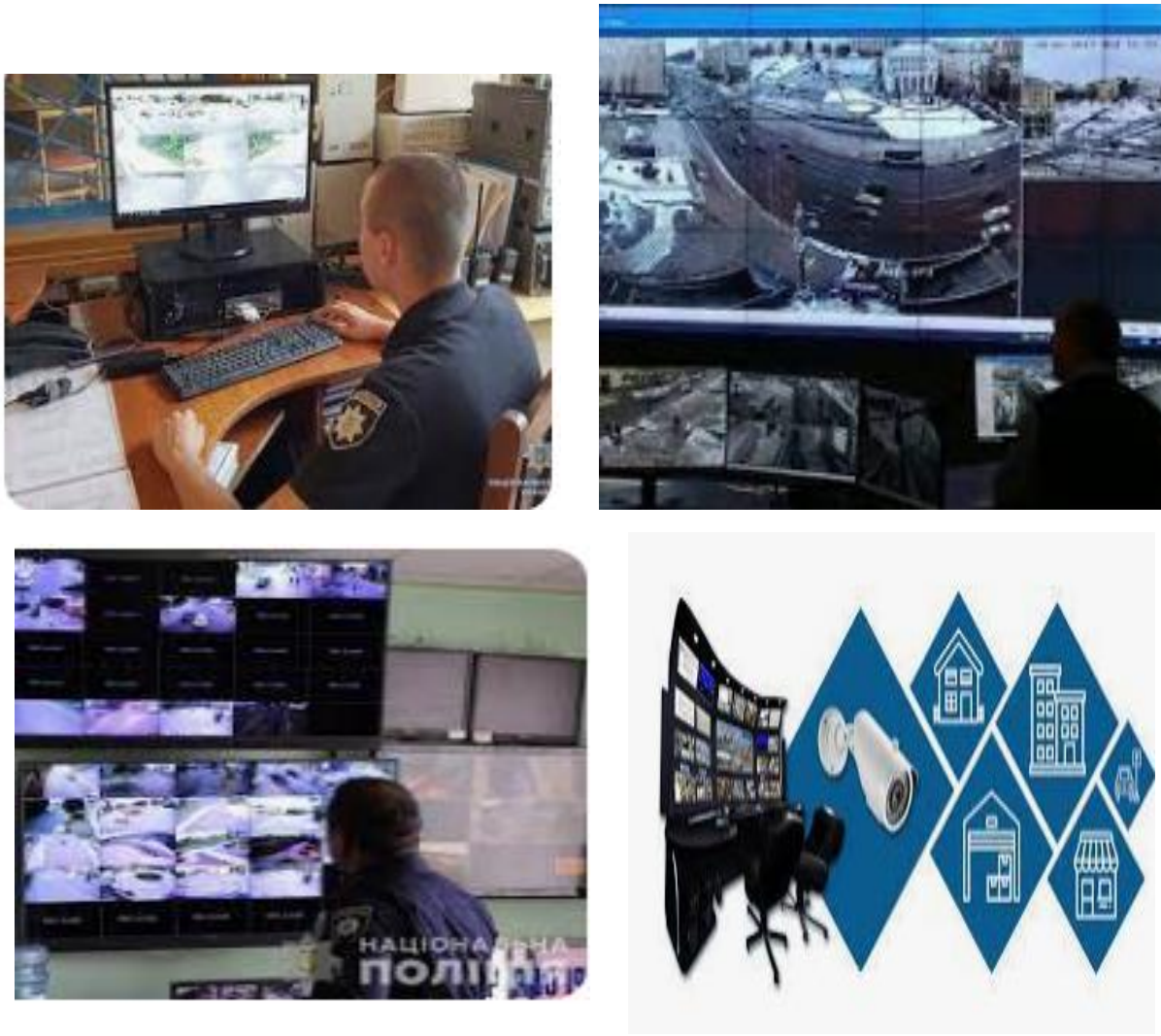


Рис. 7.8. Відеоспостереження в підрозділах Національної поліції

7.6. Методи автоматичного розпізнавання осіб

Методи автоматичного розпізнавання осіб використовуються в різних сферах, включаючи охоронні системи, верифікацію осіб, криміналістичну експертизу та інші. Ці методи включають такі напрями досліджень:

1. Нейрофізіологічні моделі. Вони базуються на дослідженнях нервової системи людини, аби розуміти, як мозок сприймає та розпізнає

обличчя. Ці моделі спираються на психофізіологічні аспекти сприйняття обличчя людиною.

2. Інформаційно-процесуальні моделі. Вони орієнтовані на теорії обробки інформації, які досліджують, як системи сприймають та обробляють візуальну інформацію, включаючи обличчя.

3. Комп'ютерні моделі розпізнавання. Ці моделі використовують алгоритми та технології комп'ютерного зору для автоматичного розпізнавання обличчя на зображеннях або відео.

4. Нейропсихологічні моделі. Вони поєднують аспекти нейрофізіології та психології для розуміння процесу сприйняття та розпізнавання облич.

Розпізнавання осіб відіграє важливу роль у сфері комп'ютерного зору вже з самого початку його розвитку. Розробка автоматизованих систем розпізнавання облич людей є однією з основних задач у цій галузі. Багато компаній витратили значні зусилля на створення таких систем, які можуть ефективно впізнавати обличчя в графічних файлах та відеопотоках.

Наприклад, компанії ImageWare, Imagis, Epic Solutions, Spillman, Miros, Vissage Technology, Visionics та Smith & Wesson розробляли різноманітні системи розпізнавання облич людей. Ці системи використовують різні методи та алгоритми для автоматичного пошуку та розпізнавання облич у графічних файлах та відеопотоках.

Технології розпізнавання облич дозволяють здійснювати різноманітні застосування, включаючи безпеку, відеоспостереження, криміналістичну експертизу, а також вирішення завдань у сферах бізнесу та медицини. Ці технології продовжують активно розвиватися і стають все більш доступними та ефективними завдяки постійним дослідженням і розвитку комп'ютерного зору.

7.7. Система розпізнавання осіб в Face recognition

Системи розпізнавання осіб, такі, що використовують технологію Face recognition, можуть здійснювати різноманітні функції, які стають все більш популярними і необхідними у різних сферах. Зокрема, таких:

1. **Підтвердження і визначення особистості студентів під час написання іспитів онлайн**. Це може забезпечити безпеку тестування та запобігти шахрайству.

2. **Розпізнавання людей в громадських місцях, які знаходяться в "чорному списку"**. Це може бути корисним у забороні входу певним

особам на публічні території або в обмежених зонах.

3. **Оплата різних товарів**. Системи розпізнавання можуть використовуватися для автоматичної оплати, наприклад, через розпізнання обличчя клієнта.

4. **Збереження місця в черзі в парках розваг**. Відомо, що в деяких парках тематичних розваг можна зберегти своє місце в черзі за допомогою систем розпізнавання осіб.

5. **Розблокування телефонів**. Це може бути одним із методів аутентифікації для розблокування смартфонів або планшетів.

У правоохоронній сфері системи розпізнавання осіб мають особливе значення для пошуку та ідентифікації злочинців, а також для забезпечення безпеки та запобігання злочинам. Урядові організації також використовують ці системи для зменшення рівня шахрайства на виборах та забезпечення загальної безпеки громадян (рис. 7.9).

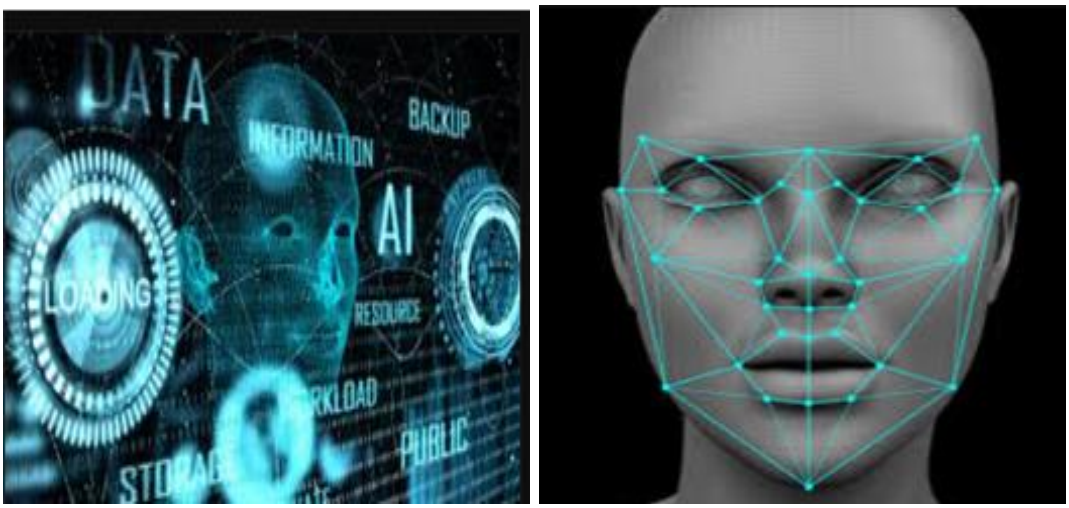


Рис. 7.9. Технологія розпізнавання обличчя

Використання систем розпізнавання осіб у різних галузях, таких як банківський сектор та авіаційна промисловість, демонструє їх широкий потенціал і різноманітні можливості.

Ідентифікація осіб у громадських місцях може проводитися з використанням 3D-зображень для створення тривимірної моделі обличчя. Цей підхід дає можливість отримати більш точне уявлення про форму обличчя та його особливості, ніж при використанні звичайних 2D-зображень.

Процес використання 3D-зображень для ідентифікації осіб може включати такі кроки:

1. **Формування тривимірної моделі обличчя**. Спеціальні системи або пристрої сканують обличчя особи з різних кутів, щоб

створити тривимірну модель об'єкта.

2. **Визначення контрольних точок**. На основі отриманої тривимірної моделі система аналізує особливості обличчя та визначає контрольні точки, такі як положення очей, носа, рота тощо.

3. **Порівняння з базою даних**. Отримані контрольні точки порівнюються з відомими образами облич, що зберігаються в базі даних. Якщо виявляється відповідність, то ідентифікація вважається успішною.

Цей метод ідентифікації може бути корисним в ситуаціях, де потрібна висока точність ідентифікації, а також в умовах, коли стандартні 2D-зображення можуть бути недостатньо ефективними, наприклад, при поганих умовах освітлення або при зміні позиції обличчя.

7.8. Метод Face recognition – математичне обґрунтування

Методи розпізнавання облич, такі як "Face recognition", базуються на різних алгоритмах та математичних моделях для виявлення та класифікації осіб на зображеннях. Ось деякі з методів, які часто використовуються:

1. **Метод каскаду Хаара (Haar Cascade Method)**. Цей метод застосовується для виділення основних компонентів обличчя, таких як очі, ніс, губи і т.д., на зображеннях. Він використовує попередньо створені шаблони для виявлення цих основних компонентів. Якщо область на зображенні відповідає одному з шаблонів, вона відзначається і розміщується в окрему папку.

2. **Метод Віоли-Джонса (Viola-Jones Method)**. Цей метод також відомий як каскад Хаара. Він використовує ковзне вікно для пошуку облич в різних масштабах на зображенні. Кожен регіон на зображенні порівнюється з шаблонами, і якщо знаходиться відповідність, то обличчя виявляється.

3. **Алгоритм градієнтного бустінгу (Gradient Boosting Algorithm)**. Цей алгоритм використовується для обробки ознак обличчя, виявлених за допомогою каскаду Хаара. Він дозволяє покращити якість класифікації, використовуючи послідовний підхід, де кожна нова модель у композиції виправляє помилки попередніх.

4. **Вирішальні дерева (Decision Trees)**. Цей метод використовується для класифікації осіб на основі ознак обличчя. Кожне вирішальне дерево будується автоматично, шляхом вибору таких предикатів, які найкраще розділяють класи.

Методи найшвидшого бустінгу та каскаду Хаара використовуються

разом для побудови моделі розпізнавання облич, що забезпечує високу якість класифікації та робить систему більш ефективною.

Ці методи допомагають системі розпізнавання облич ефективно працювати з відеопотоками та фотографіями, виявляючи та класифікуючи обличчя з високою точністю.

7.9. Використання засобів розпізнавання облич підрозділами Національної поліції

Розвиток технологій біометричної ідентифікації облич відкриває широкі можливості для застосування в різних галузях, включаючи безпеку, маркетинг, медицину та інші. Приблизно до 2030 року цей сектор може досягти значної вартості на світовому ринку, що свідчить про його важливість та широкі перспективи розвитку.

Компанія Amazon активно використовує свою розробку Amazon Rekognition для розпізнавання облич у різних сферах, включаючи урядові установи, поліцію, приватні компанії та міграційні служби. Ця технологія дозволяє проводити аналіз зображень та відео, шукає обличчя, розпізнає фото знаменитостей та логотипи брендів (рис. 7.10). Китайська компанія Hanwang впровадила новаторську технологію розпізнавання облич, яка може ідентифікувати людину навіть у медичній масці. Це важливий крок у забезпеченні безпеки та ефективному контролі входу в будівлі.

Використання систем розпізнавання облич, таких як Blue Wolf та Clearview AI, в сфері безпеки та військових операціях має значний потенціал, але водночас викликає істотні етичні та правові питання.

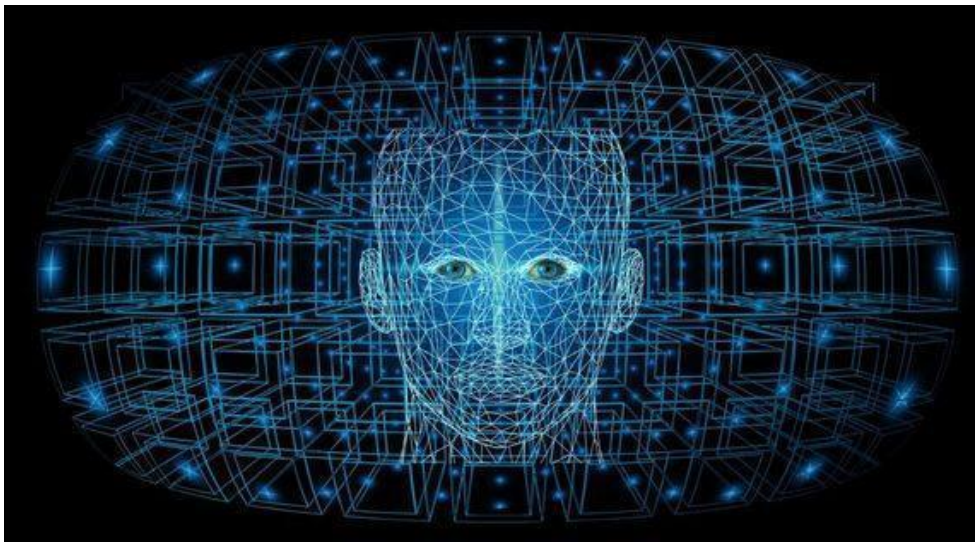


Рис. 7.10. Технологія розпізнавання обличчя

Blue Wolf, як система розпізнавання облич, використовується військами Ізраїлю для ідентифікації палестинців. Після збереження фотографій у базі даних система порівнює їх з іншими зображеннями, щоб визначити особу. Однак це може викликати застереження з точки зору приватності та прав людини, особливо у воєнний час.

Clearview AI також використовується в Україні для ідентифікації воєнних злочинців та виявлення ворогів на блокпостах. Ця система має велику базу даних з фотографіями, що дозволяє швидко розпізнавати осіб. Проте використання таких систем у воєнних операціях може породжувати питання про точність та захист приватності.

Хоча розробники Clearview AI планують співпрацювати з українським Міністерством цифрової трансформації для будівництва цифрової інфраструктури, важливо ретельно вивчити всі аспекти їхньої роботи, зокрема забезпечити відповідність законодавству та правам людини.

7.10. Використання МВС технологій для розпізнавання облич під час іспитів на водійські права

Використання технологій розпізнавання облич МВС для проведення іспитів на отримання водійських прав має спростити та удосконалити процес видачі прав. Завдяки цьому програмному забезпеченню, яке розпізнає обличчя, можна забезпечити точну ідентифікацію кандидатів під час складання іспитів.

Інтеграція такої технології в національну автоматизовану інформаційну систему МВС дозволить урядовим установам ефективно використовувати інформаційні ресурси та забезпечити безпеку та конфіденційність даних.

Попереднє фото кандидатів під час іспиту може стати частиною процедури перевірки їхньої особистості та відповідності вимогам законодавства. Однак важливо забезпечити захист особистої інформації та визначити чіткі правила зберігання та використання цих даних (рис. 7.11).

Рис. 7.11. Розпізнавання обличчя за кермом авто

Крім того, важливо враховувати можливі етичні та правові аспекти використання таких технологій, зокрема забезпечити дотримання прав та свобод громадян, а також уникнути можливих помилок та неточностей у роботі системи.

7.11. Камери з розпізнавання облич на вулицях міст в Україні

Впровадження систем відеоспостереження з функцією розпізнавання облич в містах України, зокрема на Київщині, виявилося дієвим інструментом для підвищення рівня безпеки та зменшення злочинності. За допомогою таких камер поліція може швидше реагувати на правопорушення, розшукувати зниклих осіб та розкривати злочини (рис. 7.12).

Рис. 7.12. Відеоспостереження на вулицях міст України

Технологія розпізнавання облич дозволяє ідентифікувати осіб навіть у складних умовах, таких як погане освітлення або частково закрите обличчя. Це значно полегшує роботу правоохоронців у виявленні та розслідуванні правопорушень.

Підрозділи Національної поліції мають можливість не лише використовувати дані з камер для розшуку правопорушників, але й для запобігання злочинам. Це важливий крок у напрямі підвищення ефективності правоохоронних органів та забезпечення безпеки громадян.

Залучення працівників ситуаційних центрів та підрозділів кримінального аналізу ГУНП в областях до роботи з камерами розпізнавання осіб підвищує можливості використання цієї технології у розкритті злочинів та реагуванні на екстрені ситуації.

7.12. Застосування тепловізора для біометричної ідентифікації людини

Біометричні системи для контролю доступу складаються з апаратних та програмних компонентів. Апаратні засоби включають в себе біометричні сканери і термінали, які фіксують біометричні параметри, такі як відбитки пальців, райдужну оболонку очей або малюнок вен на долоні. Ці параметри перетворюються на цифрові моделі, які потім можуть бути оброблені програмним забезпеченням.

Програмні засоби виконують обробку отриманих даних,

співвідносять їх з базою даних та формують рішення щодо ідентифікації осіб. У комерційних системах ідентифікатори зазвичай зберігаються у вигляді цифрових моделей, що забезпечує високий рівень конфіденційності.

Для роботи біометричних систем контролю доступу використовуються пристрої контролю доступу, такі як рідери або сканери. Вони зчитують інформацію, а потім аналізують її та порівнюють з інформацією про особу, яка була занесена до системи раніше. Якщо дані збігаються, відбувається аутентифікація особи, і якщо вона має відповідні права доступу, то пристрій надає доступ.

Найбільш поширеною біометричною характеристикою для ідентифікації є відбитки пальців, але в деяких високоризикових місцях використовується сканування сітківки ока або технологія розпізнавання обличчя.

Технологія розпізнавання облич дійсно працює за принципом, схожим на роботу людського мозку. При перегляді зображення ми спочатку визначаємо особливості обличчя, звертаючи увагу на різні риси, такі як очі, ніс, рот тощо, і потім обробляємо ці дані у своїй свідомості. Аналогічно і технологія розпізнавання облич шукає особливі риси на зображенні і виділяє їх, щоб ідентифікувати особу.

Для досягнення цієї мети використовуються різні алгоритми, включаючи аналіз схожості пропорцій, виявлення контурів обличчя та порівняння їх зі збереженими шаблонами, а також використання нейронних мереж для виділення симетрії та інших ознак. Ці алгоритми дозволяють системі ефективно розпізнавати обличчя на зображеннях і відео.

Технологія розпізнавання облич має широкий спектр застосувань у різних сферах діяльності, включаючи безпеку, криміналістику, банківські послуги, маркетинг, рекламу та багато іншого. Вона дозволяє вирішувати різноманітні завдання, такі як пошук підозрілих осіб, верифікація особистостей, контроль доступу та ідентифікація осіб на зображеннях.

Застосування технології розпізнавання облич в різних сферах є актуальним і широко використовується у різних країнах світу. Відмінність у рівні доступу до цих технологій, а також управління та регулювання їх використання може варіюватися в залежності від законодавства кожної конкретної країни.

Головний недолік технології розпізнавання облич – це погіршення якості розпізнавання при погіршенні освітленості або зміні положення голови і ракурсу.

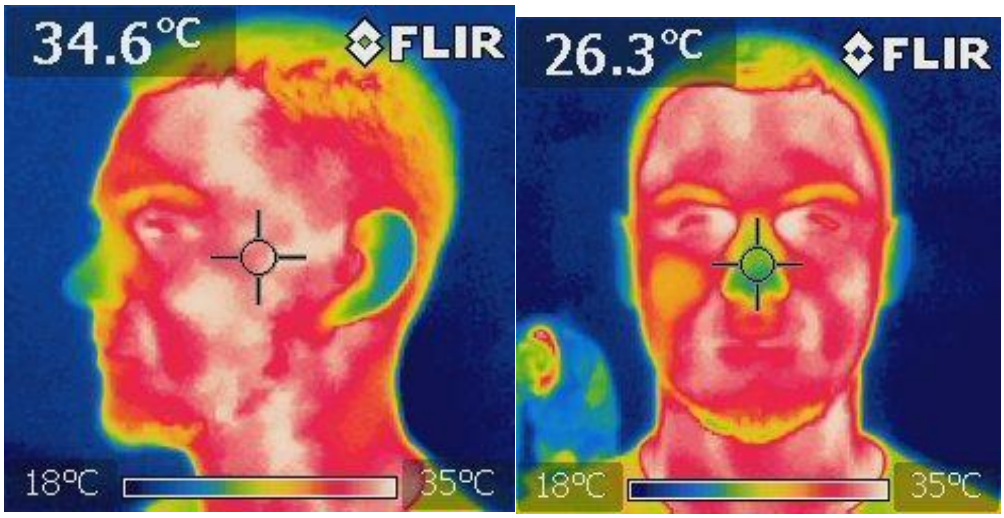
Використання тепловізійних камер для розпізнавання облич є перспективним напрямом, який дозволяє уникнути деяких недоліків, що існують при використанні звичайних відеокамер.

Основна конкурентна перевага тепловізійних камер полягає в їхній ефективності при будь-яких погодних умовах. Вони можуть знаходити мету навіть тоді, коли вона схована за густим листям дерев.

Для реалізації розпізнавання облич з використанням тепловізійних камер застосовуються різні методи. Наприклад, генерація тривимірної поверхні особи може відбуватися за допомогою інструменту 3D Basel Face Model (BFM) з використанням даних зображень тепловізійної камери. Цей метод дозволяє ефективно створювати тривимірні обличчя за допомогою вектора, який використовується для генерації облич (рис. 7.13).

Технологія розпізнавання облич з використанням тепловізійних камер може вирішувати такі завдання, як розпізнавання облич в повній темряві або в умовах недостатнього освітлення, а також розпізнавання облич з макіяжем, різними зачісками, бородою, капелюхом або окулярами. Крім того, вона дозволяє розпізнавати навіть близнюків.

У різних країнах світу ведеться розробка двох основних напрямів використання тепловізійних камер для розпізнавання облич: ідентифікація за заздалегідь створеним термограмам ідентифікованих осіб, а також ідентифікація за зображеннями, отриманими з тепловізійних камер, з використанням бази даних двовимірних зображень і глибоких нейронних мереж.



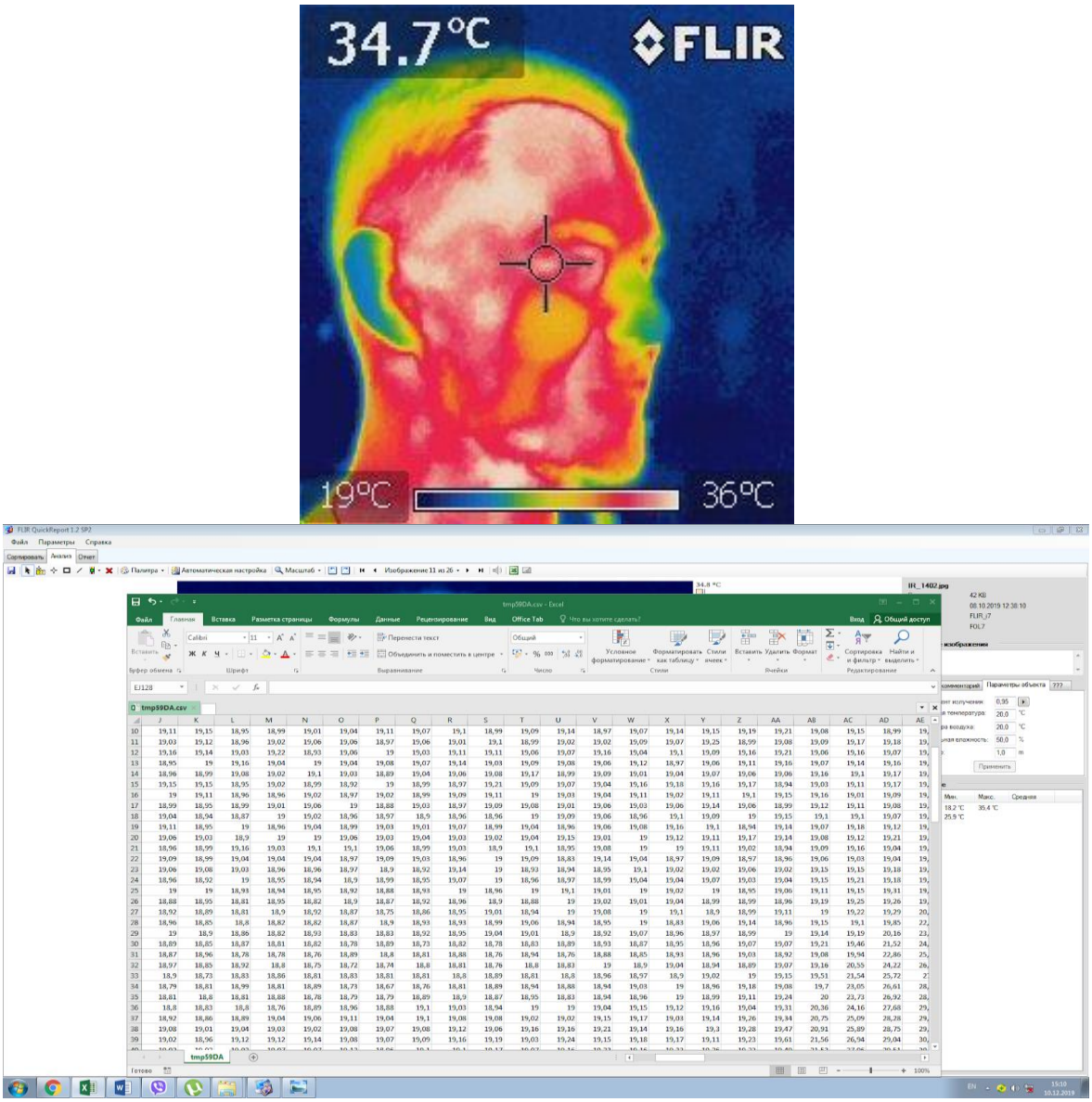


Рис. 7.13. Тепловізійні камери для ідентифікації облич

7.13. Пошуково-ідентифікаційна система Clearview AI

Clearview AI є впливовою системою пошуку та ідентифікації осіб, що працює на основі розпізнавання облич. Вона призначена для використання правоохоронними органами як у боротьбі зі злочинністю, так і в профілактичній діяльності. Система Clearview AI містить базу даних з більш ніж 30 мільярдів фотозображень, які були зібрані з відкритих джерел, таких як соціальні мережі, інформаційні сайти, кримінальні бази даних та інші ресурси. Розробники використовують потужні алгоритми штучного інтелекту для розпізнавання облич, що дозволяє системі ефективно та швидко ідентифікувати осіб, порівнюючи

їх зображення з великим обсягом фото та відео. Це дозволяє Clearview AI не лише ідентифікувати конкретних осіб, а й виявляти зачіпки, ідеї та зв'язки. Інформація, зібрана за допомогою цієї системи, допомагає правоохоронним органам отримувати доказову базу під час розслідування злочинів та ідентифікувати не лише підозрюваних, а й жертв. Clearview AI також пропонує рішення для правоохоронних органів, такі як генерація зачіпок для швидкого розслідування злочинів, співпраця з іншими установами, ефективний пошук навіть через низьку якість зображень та доступ до великої бази даних загальнодоступних зображень (рис. 7.14).

З початком війни в Україні розпорядники пошукової платформи Clearview AI надали можливість безкоштовного використання своєї системи силовим відомствам країни. Міністерство оборони України почало використовувати технологію розпізнавання облич Clearview AI для ідентифікації російських нападників, боротьби з дезінформацією та встановлення осіб, що загинули.

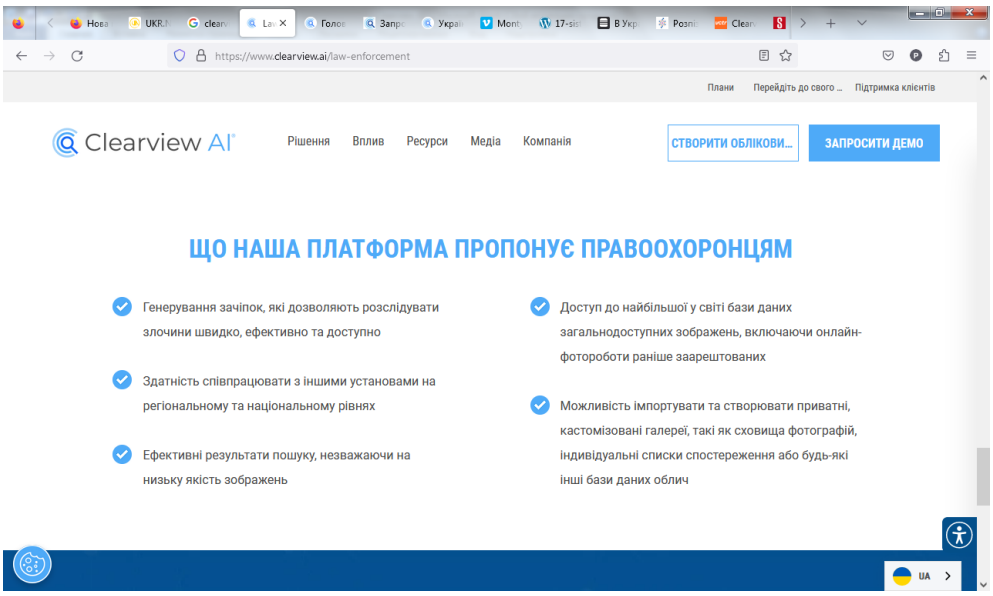


Рис. 7.14. Можливості Clearview AI для правоохоронців

Особливою привабливістю цієї системи є доступ до більш ніж 2 мільярдів фото та відео з російської соцмережі "ВКонтакте", що дозволяє ефективно використовувати її на контрольно-пропускних пунктах для виявлення осіб, які активно спілкуються у російських соціальних мережах та можуть мати зв'язок з ФСБ, колаборантами та пропагандистами "русского мира". Крім того, Clearview AI допомагає в ідентифікації загиблих громадян України та військовослужбовців

збройних сил, яких знайдено на звільнених від окупантів територіях, завдяки ефективному розпізнаванню облич, навіть у разі пошкодження.

На веб-сайті Clearview AI є окремий розділ, присвячений їхній діяльності в Україні та результатам допомоги правоохоронним органам країни (рис. 7.15).

Більше ніж сім відомств України та понад 1000 військовослужбовців активно користувалися платформою Clearview AI, здійснивши понад 160 000 пошуків.

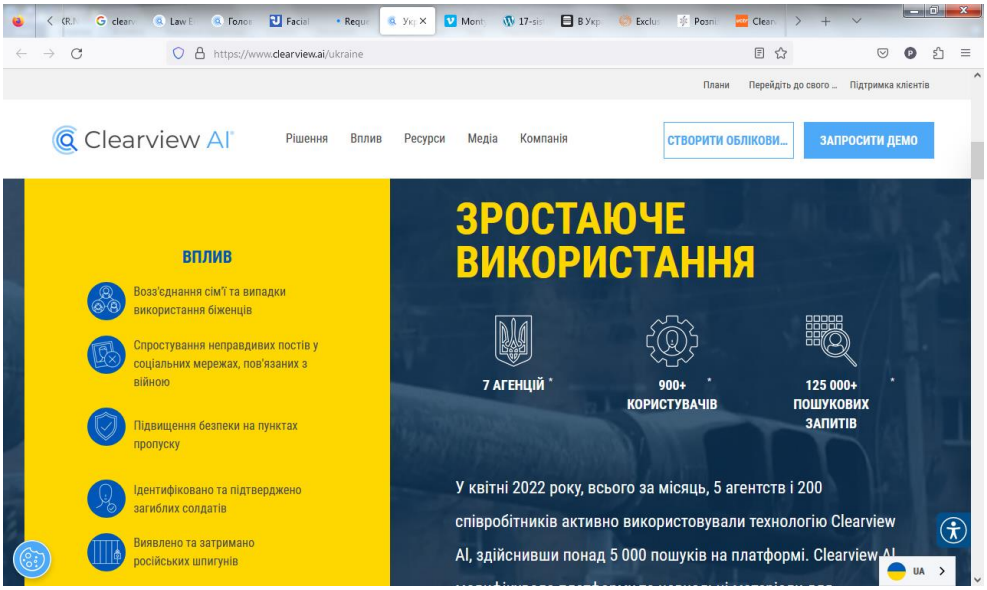


Рис. 7.15. Розділ веб-сайту Clearview AI, присвячений допомозі Україні

За допомогою цієї системи прикордонникам вдалося ідентифікувати понад 10 тисяч осіб, серед яких були полонені громадяни України, особи, причетні до незаконного перевезення дітей з тимчасово окупованих територій до Російської Федерації, військовослужбовці Російської Федерації, російські пропагандисти, які підтримують окупаційні війська та беруть участь в інформаційній війні проти України, колаборанціоністи та зрадники України, а також особи, причетні до кримінальних та адміністративних правопорушень.

Сайт пропонує встановити демоверсію інформаційно-пошукової системи зі штучним інтелектом Clearview AI лише правоохоронним органам (рис. 7.16).

Пошукова платформа Clearview AI здобула лідерські позиції серед систем ідентифікації осіб за їх обличчям з відкритих джерел. Її успіх зумовлений широкою базою даних зображень з різноманітних джерел у мережі Інтернет та потужним алгоритмом розпізнавання, що надає цінну інформацію правоохоронним органам.

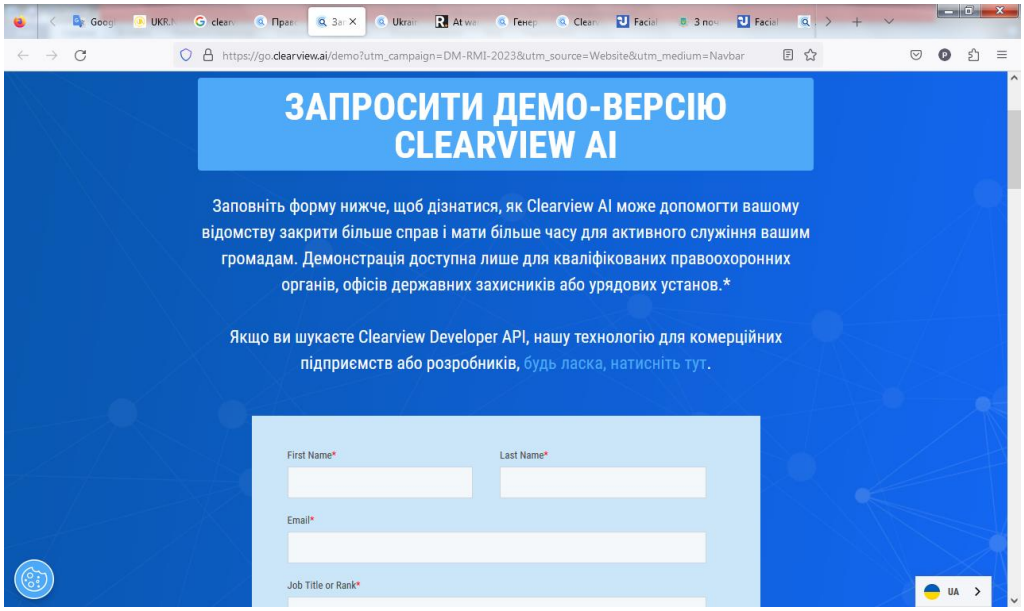


Рис. 7.16. Форма запиту для встановлення демоверсії Clearview AI

Проте компанія Clearview AI стикається з серйозними юридичними проблемами у багатьох країнах. Практично у всіх демократичних державах світу законодавство захищає конфіденційність особистих даних та інформації громадян. Суди у багатьох країнах, включаючи країни Європи, Канаду та Австралію, визнали базу даних фотозображень Clearview незаконною, і судові рішення зобов'язують керівництво Clearview видалити фотографії своїх громадян. Деякі країни, такі як Італія та Великобританія, наклали штрафи на компанію Clearview AI в багатомільйонних розмірах за порушення законодавства.

7.14. Пошукова система PimEyes

PimEyes – це пошукова платформа, спрямована на пошук осіб за їх фотозображеннями. Унікальність алгоритму полягає в тому, що він розпізнає обличчя на фотографії на початковому етапі, що відрізняє систему PimEyes від інших пошукових сервісів. Наприклад, значна кількість інших систем, таких як Google Images, шукають ідентичні фотографії в Інтернеті (рис. 7.17).

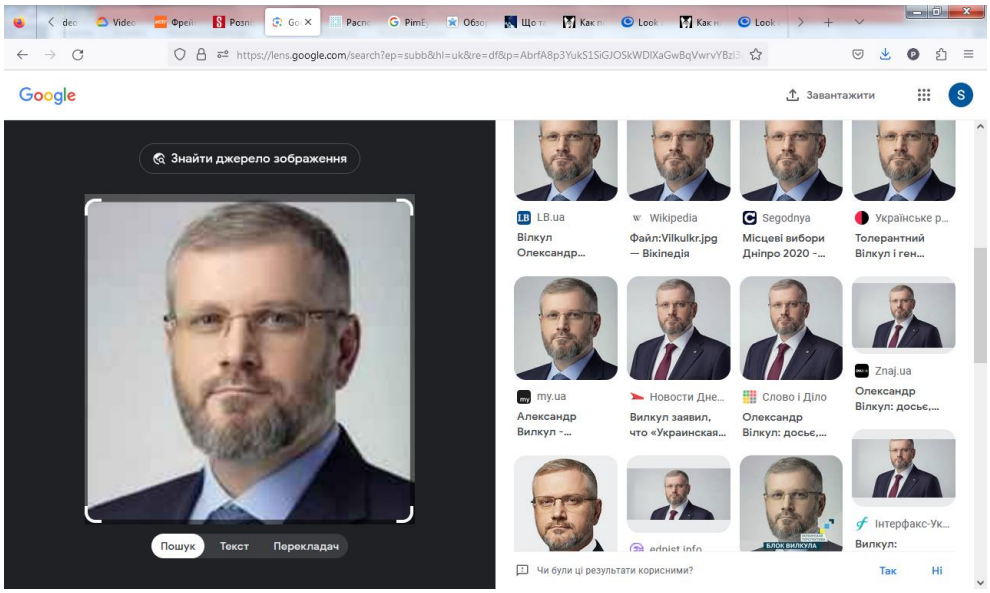


Рис. 7.17. Приклад пошуку за фотозображенням за допомогою оболонки Google-зображення

Платформа PimEyes використовує можливості вбудованого штучного інтелекту, щоб спочатку розпізнати обличчя людини на вхідному зображенні, а потім шукати це обличчя на інших фотографіях, що доступні в мережі Інтернет. Для використання PimEyes не потрібна реєстрація, але користувачі не можуть переглядати зображення повністю або отримувати посилання на сайт, де вони були знайдені. Також не доступні сповіщення про нові фотографії в мережі.

Платформа PimEyes була розроблена у Польщі у 2017 році Лукашем Ковальчиком і Денисом Татіною. У 2022 році її придбав громадянин Грузії Гобронідзе, який в 2023 році заблокував доступ до PimEyes для осіб, що проживають у Росії, на знак солідарності з Україною.

Це платна послуга, яка має різні тарифні плани, найбільш доступний – Open Plus за $30 на місяць. Є обмеження на кількість запитів на день, які становлять 25 навіть у платному плані.

Якісний результат пошуку фотозображення повинен відповідати певним вимогам, таким як формат файлу, розмір та якість фотографії. Навіть за наявності цих вимог результати пошуку є дуже точними.

Також слід зазначити, що пошукова оболонка не зможе знайти фотографії, якщо вони знаходяться на сайтах, що закриті для індексації, таких як Facebook.

Платформа PimEyes має безкоштовну версію, яка дозволяє проводити обмежену кількість пошуків без реєстрації на веб-сайті (рис. 7.18).

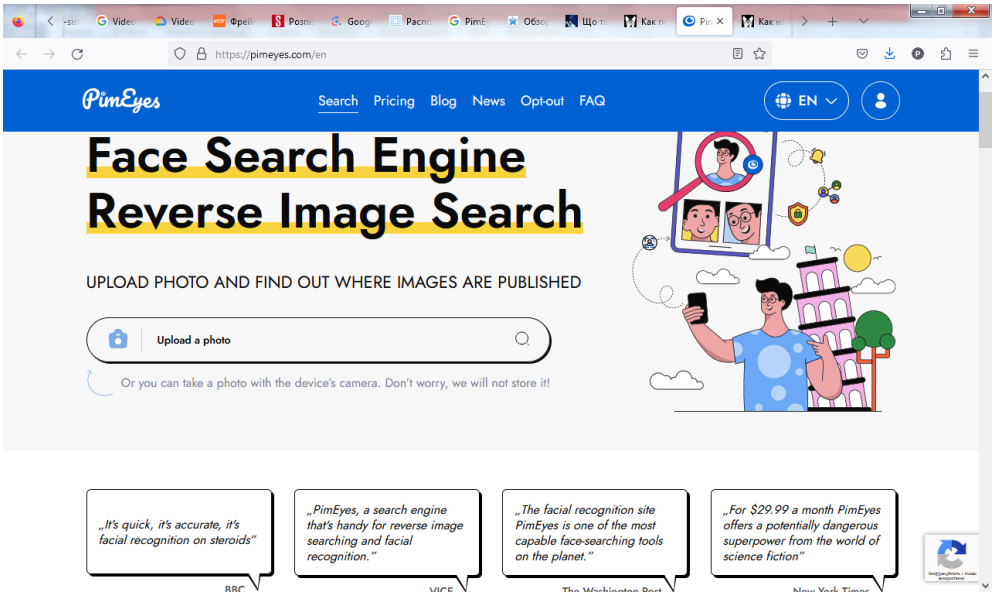


Рис. 7.18. Загальний вигляд веб-сайту пошукової оболонки PimEyes

На веб-сайті пошукової оболонки PimEyes для пошуку за фотозображенням ви натискаєте кнопку "Upload a photo", що відкриває вікно для вибору зображення, яке збережено на вашому пристрої. Опісля цього вибираєте потрібне фото, яке ви хочете використати для пошуку (рис. 7.19).

Наприклад, для пошуку фото колаборантки Євгенії Більченко виберіть фото, яке ви знайшли через пошукову систему Google. Введіть ім'я "Євгенія Більченко" у пошуковий рядок, а потім оберіть відповідне фото (рис. 7.20).

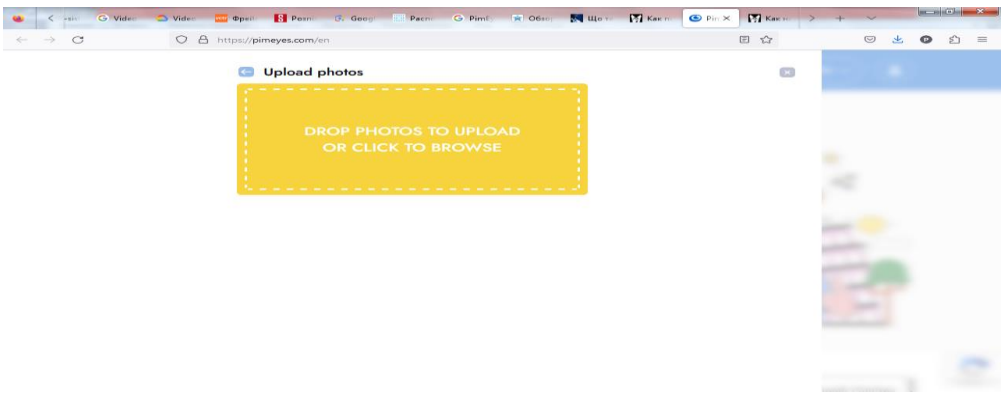


Рис. 7.19. Вікно вибору фото для введення
у пошукову оболонку PimEyes

Після вибору фото, завантаженого до PimEyes, система проведе пошук та надасть вам результати, які включають зображення, де знайдено аналогічне або схоже обличчя.

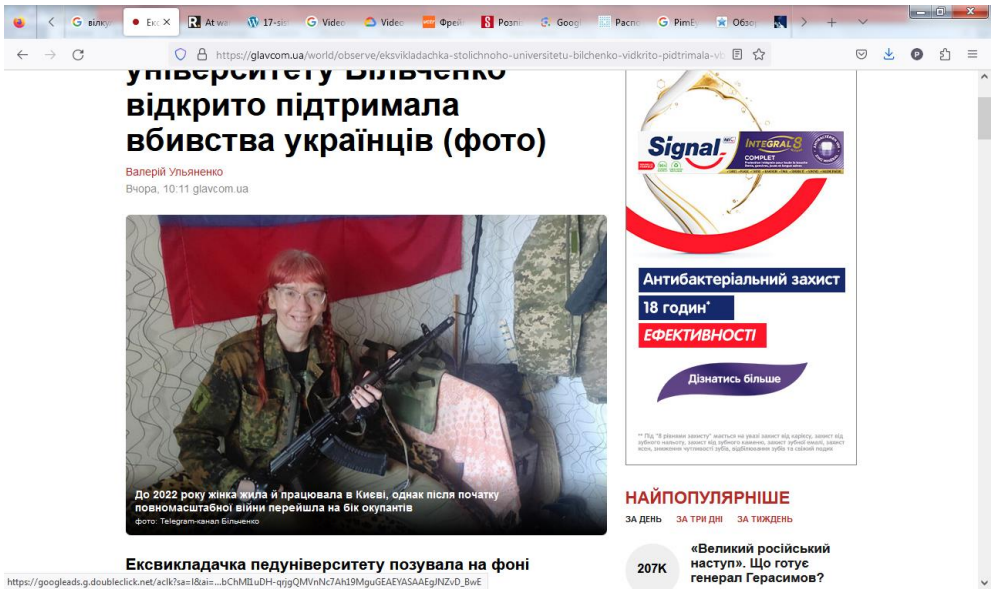


Рис. 7.20. Фотозображення колаборантки Євгенії Більченко

Вибране фото зберігається на вашому комп'ютері, а потім завантажується у програму PimEyes. Система обробляє це фотозображення і виділяє обличчя особи для пошуку (рис. 7.21).

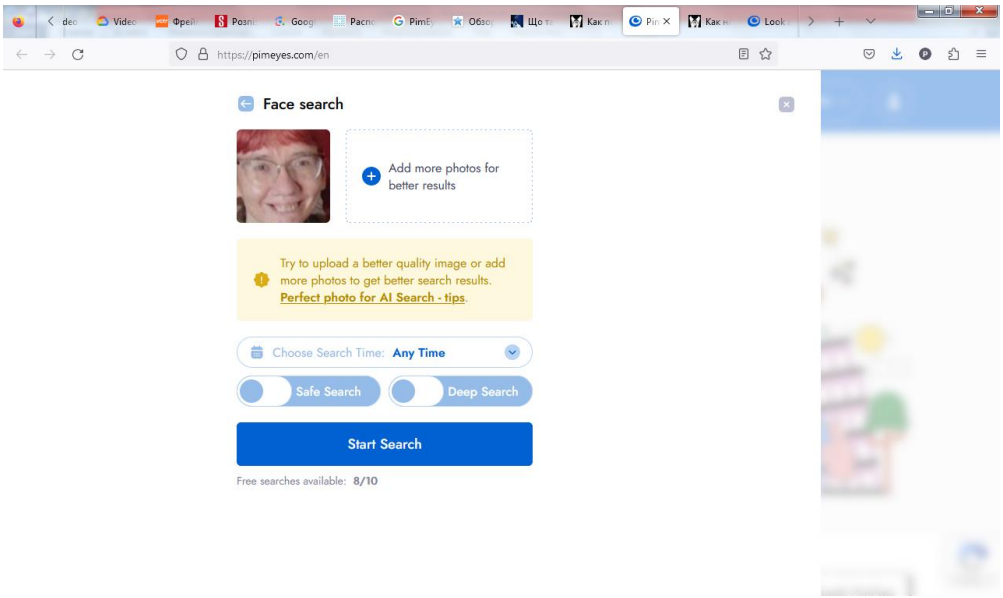


Рис. 7.21. Сканування обличчя особи

Після цього натискаєте кнопку "Start Search", щоб запустити пошук. Після завершення пошуку PimEyes показує результати, знайдені на відкритих платформах Інтернету (рис. 7.22). У вашому випадку система знайшла 251 зображення, що містять аналогічне або схоже обличчя Євгенії Більченко.

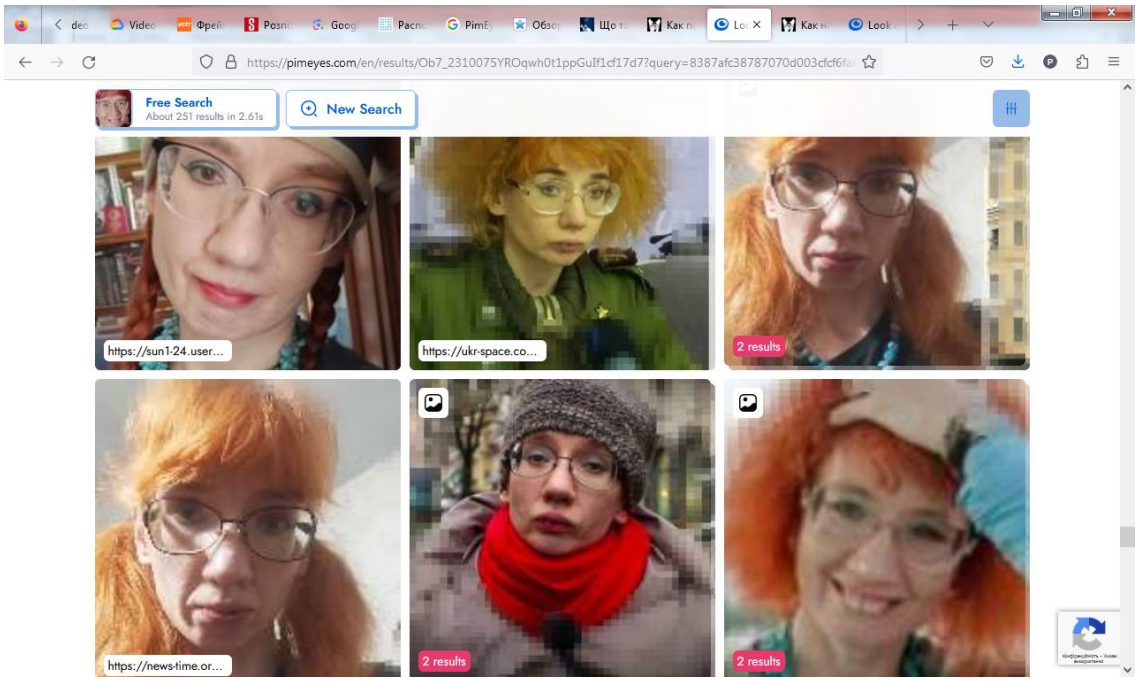


Рис. 7.22. Результати пошуку по фото Євгенії Більченко

Хоча результат вважається чудовим, доступ до знайдених джерел фотозображень при безкоштовному доступі може бути обмеженим. Це може стати однією з проблем, з якими стикається компанія PimEyes. Наприклад, Німеччина розпочала розслідування щодо можливих порушень європейського закону про конфіденційність щодо PimEyes.

Варто зазначити, що керівництво компанії вважає, що їхній алгоритм дії схожий на цифровий картковий каталог. Вони не зберігають фотографії або індивідуальні шаблони облич, а лише URL-адреси для зображень, пов'язаних з рисами обличчя. Вони закликають користувачів шукати лише свої власні обличчя.

7.15. Пошукова система за обличчями BetaFace

Пошукова система BetaFace відрізняється від інших систем пошуку осіб тим, що надає різні варіанти обробки зображення, щоб вибрати найкращий збіг із вхідним фото відкритої мережі Інтернет. Ці варіанти включають визначення статі, віку, етнічної приналежності та емоцій, виявлення контенту "для дорослих", визначення базових точок обличчя та розширені геометричні та колірні виміри, такі як колір шкіри та зачіски. Крім того, є спеціальний фільтр для покращення якості фотозображення.

Після вибору бажаних параметрів обробки ви можете завантажити зображення обличчя, яке ви хочете знайти. Обробка зображення може займати деякий час залежно від обраних параметрів. Після завершення обробки на екрані буде виведено результат.

У вашому випадку при введенні базового зображення колаборантки Євгенії Більченко (рис. 7.23) у систему BetaFace ви отримали результат, відображений на рис. .

Система BetaFace, здається, призначена для більш широкого спектру використання, яке може включати в себе не лише пошук осіб, але й аналіз їхніх параметрів, порівняння з відомими знаменитостями, пошук у Вікіпедії тощо (рис. 7.24).

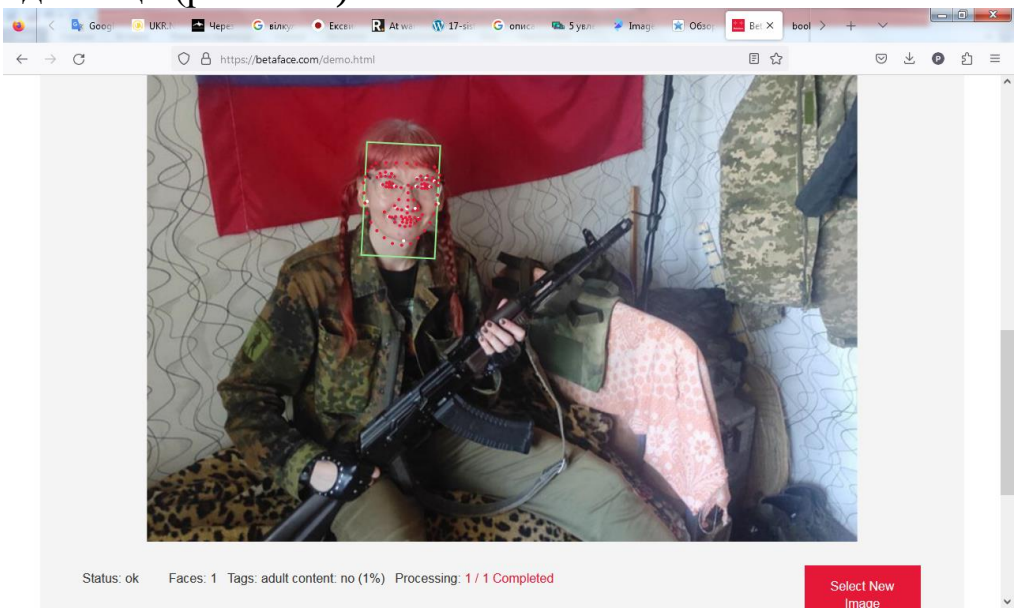


Рис. 7.23. Фотозображення після обробки оболонкою BetaFace

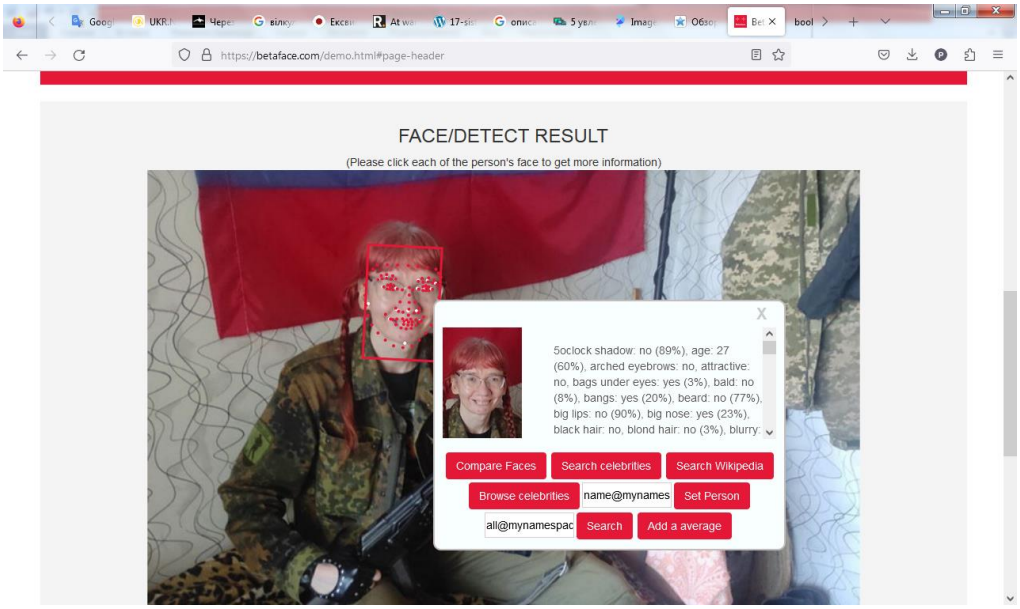


Рис. 7.24. Параметри обличчя, які розпізнала система BetaFace

Ці параметри можуть бути корисними для різних цілей, таких як ідентифікація знайомих або перевірка інформації про відомих осіб.

Однак, як ви вказали, ця система може бути менш корисною для правоохоронних органів, якщо їхня основна мета полягає у пошуку невідомих осіб або порівнянні з великою базою даних. Це може обмежити її застосування у таких сценаріях, де необхідно швидко та ефективно встановити ідентичність осіб на великій кількості зображень.

7.16. Пошукова система PicTriev

Ця система пошуку осіб працює наступним чином: для пошуку особи необхідно завантажити в систему фотозображення або використати URL-адресу зображення з Інтернету. Після цього система надає атрибути особи, визначаючи, чи є вона чоловіком чи жінкою, а також встановлює її вік. Потім система шукає фотографії цієї особи в Інтернеті і показує їх у результатах разом з відсотком подібності.

Особливістю цієї пошукової системи є обмеження на файли з фотозображеннями: вони повинні бути у форматі JPEG з максимальним розміром файлу 200 КБ. Якщо вам потрібно знайти зображення більшого розміру, необхідно зменшити розмір вихідного зображення, щоб відповідати вимогам системи.

Давайте розглянемо приклад роботи з пошуковою системою PicTriev. Наприклад, ми вводимо зображення колеги Євгенії Більченко. Після обробки фото отримуємо результат, який включає знайдені фотографії разом з відсотком подібності (рис. 7.25).

На представленому скріншоті показані результати пошуку фотозображень обличчя фігурантки Більченко за допомогою системи PicTriev (рис. 7.26).

Результати пошуку, які ми можемо спостерігати, є незадовільними. Алгоритм, що лежить в основі системи PicTriev, не зміг знайти фотографії фігурантки у мережі Інтернет. Найвищий збіг за критеріями вхідного фото із знайденими фотографіями інших осіб становить лише 10 відсотків. Це означає, що дана пошукова система може бути корисною лише для розважальних цілей, а не для застосування правоохоронними органами.

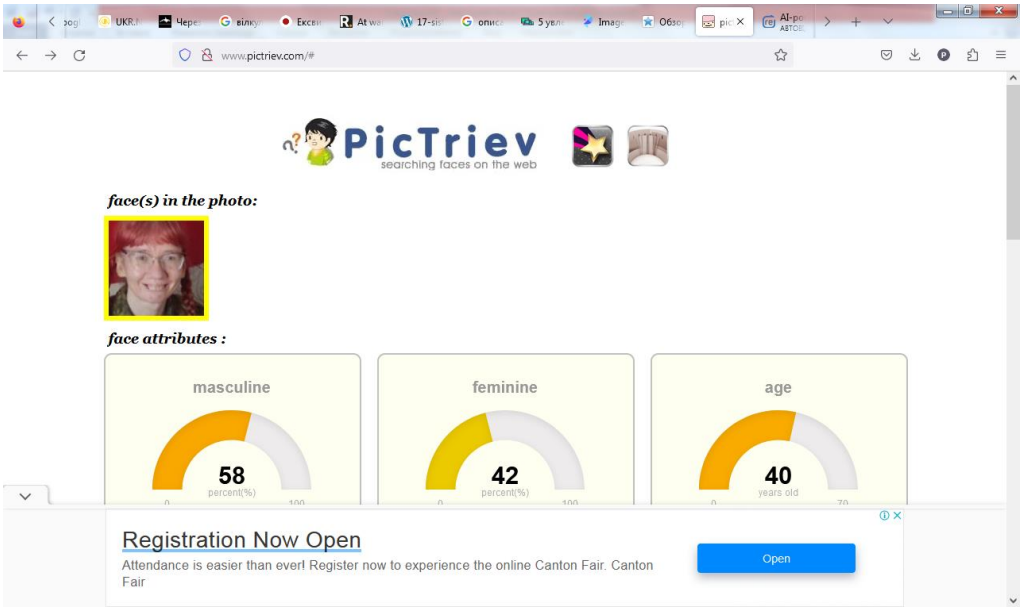


Рис. 7.25. Результат обробки фото системою PicTriev

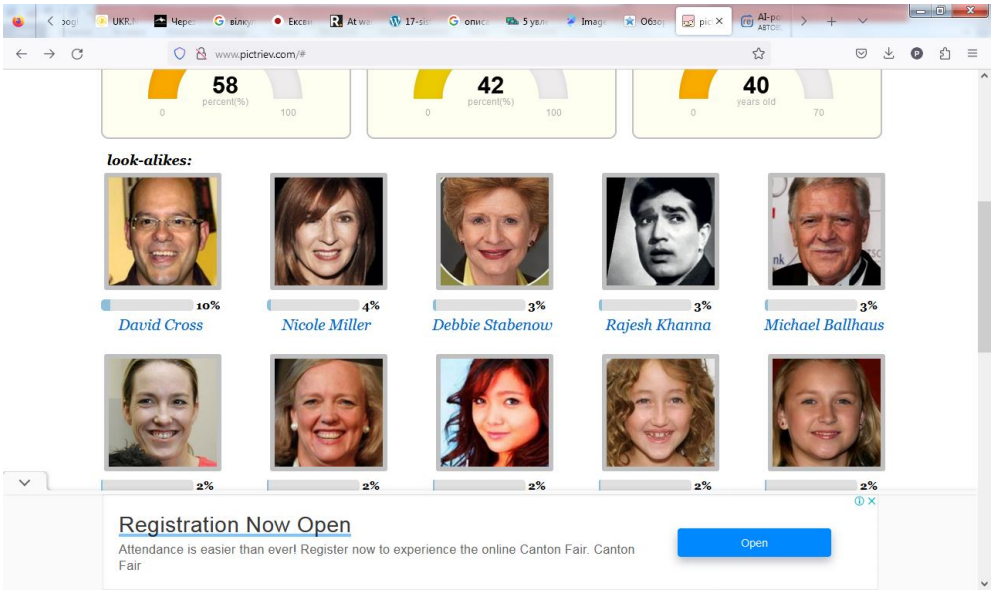


Рис. 7.26. Результат пошуку системою PicTriev

У цій главі ми описали основні методи та засоби розпізнавання осіб за обличчям, які використовуються як алгоритми для пошуку та ідентифікації в спеціалізованих системах. Також аналізували системи розпізнавання та пошуку осіб за обличчям серед фотозображень, що розміщені в Інтернеті. Найбільш корисною для правоохоронних органів є система Clearview AI, яка містить базу даних з понад 30 мільярдами фотозображень, скопійованих з відкритих джерел. Розробники Clearview AI створили потужні алгоритми пошуку з використанням штучного інтелекту. Методи розпізнавання облич на основі штучного інтелекту прискорюють процес ідентифікації шляхом порівняння введеного зображення з потужним масивом фото та відео. Це дозволяє Clearview AI не тільки ідентифікувати осіб, але й виявляти зачіпки, ідеї та зв'язки. Інформація, отримана за допомогою Clearview AI, допомагає в досудовому розслідуванні та ідентифікації осіб, які становлять інтерес для правоохоронних органів, а також встановленні жертв злочинів. Доступ до цієї системи надається тільки правоохоронним органам і широко використовується в Україні, де показала хороші результати.

Система PimEyes також показує непогані результати пошуку осіб за обличчями. За допомогою штучного інтелекту, вбудованого у пошукову систему PimEyes, вона спочатку розпізнає обличчя на вхідному зображенні, а потім шукає його на інших фотозображеннях в мережі Інтернет. Для використання PimEyes не потрібна реєстрація, але

користувач не може переглядати повністю знайдені зображення та отримати посилання на сайт. Недоліком є те, що повні результати доступні лише у платній версії, хоча є можливість безкоштовного використання для правоохоронних органів України під час війни.

Системи BetaFace та PicTriev показали незадовільні результати і не підходять для використання правоохоронними органами.

Опис та тестування систем для пошуку осіб за фотозображеннями буде корисним для працівників Національної поліції, науковців і студентів поліцейських навчальних закладів.

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ:

1. Які основні принципи роботи технологій розпізнавання облич на відео та фото?
2. Як технології розпізнавання облич використовуються у правоохоронній діяльності для ідентифікації підозрюваних?
3. Які методи машинного навчання є найефективнішими для розпізнавання облич?
4. Які є приклади успішного використання систем розпізнавання облич для забезпечення громадської безпеки в різних країнах?
5. Які етичні питання виникають при використанні розпізнавання облич, особливо у публічних місцях?
6. Яким чином забезпечується конфіденційність даних при використанні технологій розпізнавання облич?
7. Які загрози існують для приватності особистої інформації у зв’язку з використанням розпізнавання обличчя?
8. Як регулюється законодавством використання розпізнавання облич у правоохоронній сфері в різних країнах?
9. Які альтернативні технології можуть бути використані для ідентифікації осіб, якщо розпізнавання облич є недоступним або неефективним?
10. Які перспективи розвитку технологій розпізнавання облич у сфері штучного інтелекту та аналітики даних?

ЛІТЕРАТУРА ЗА РОЗДІЛЛОМ:

1. Face ID. URL: https://uk.wikipedia.org/wiki/Face_ID.
2. OpenCV: OpenCV Tutorials. URL: https://docs.opencv.org/2.4/doc/tutorials/tutorials.html.
3. Dlib Python API Tutorials. URL: http://dlib.net/python/index.html.
4. Face Detection Algorithms and Techniques. URL: https://facedetection.com/algorithms/.
5. Sominite T. Facebook Creates Software That Matches Faces Almost as

Well as You Do. URL: https://www.technologyreview.com/s/525586/facebookcreates-software-that-matches-faces-almost-as-well-as-you-do/.

6. About Face ID advanced technology. URL: https://support.apple.com/enus/HT208108.

7. Face ID for iPhone X. URL: http://blog.maconline.com/face-id-iphone-x/.

8. What is the Azure Face API? URL: https://docs.microsoft.com/enus/azure/cognitive-services/face/overview.

9. Aware. Biometrics Software Products. URL: https://www.aware.com/biometrics/.

10. Samsung security. Face recognition. Iris recognition. URL: http://www.samsung.com/uk/smartphones/galaxy-s8/security/.

11. Rybchak Z., Basystiuk O. Analysis of computer vision and image analysis technics. Econtechmod: an international quarterly journal on economics of technology and modelling processes. Lublin : Polish Academy of Sciences, 2017. Vol. 6. № 2. S. 79–84.

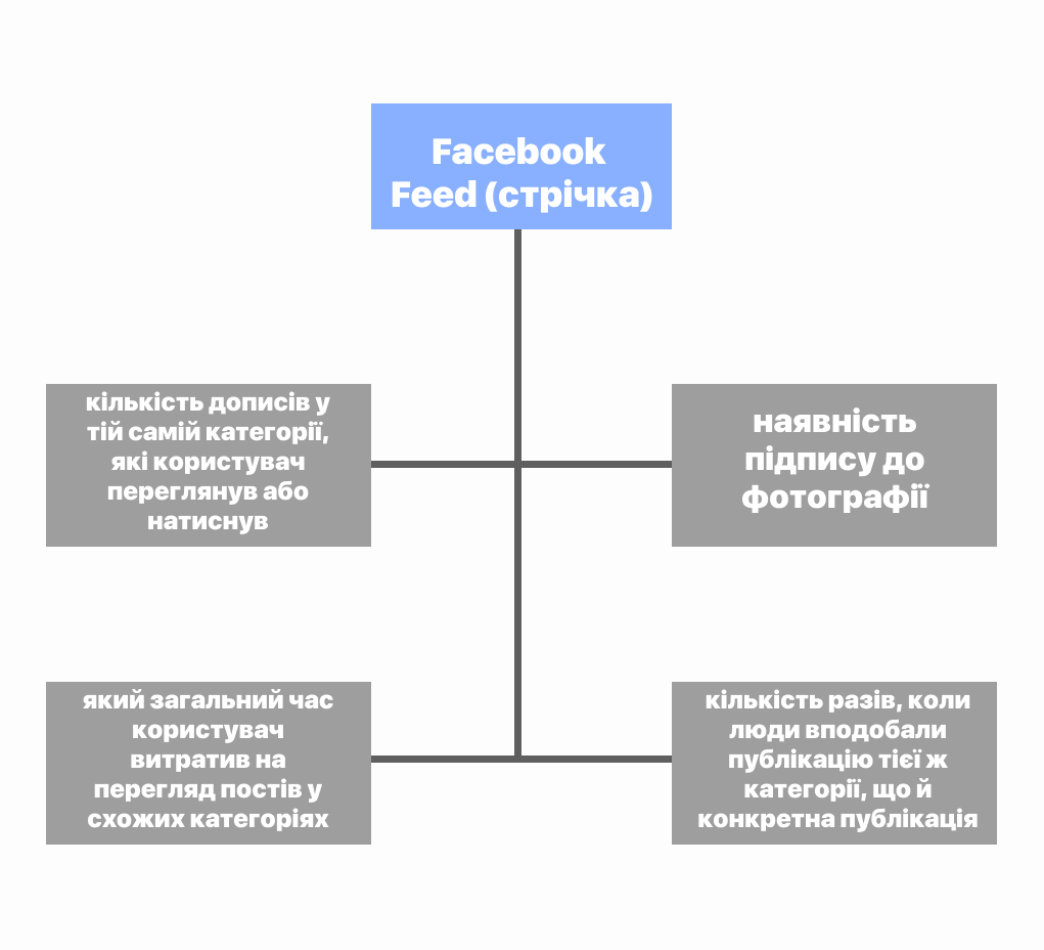
12. Raja R. Face Detection Using OpenCV and Python. URL: https://www.superdatascience.com/opencv-face-detection/.

13. Raja R. Face Recognition Using OpenCV and Python. URL: https://www.superdatascience.com/opencv-face-recognition/.

Д О Д А Т К И

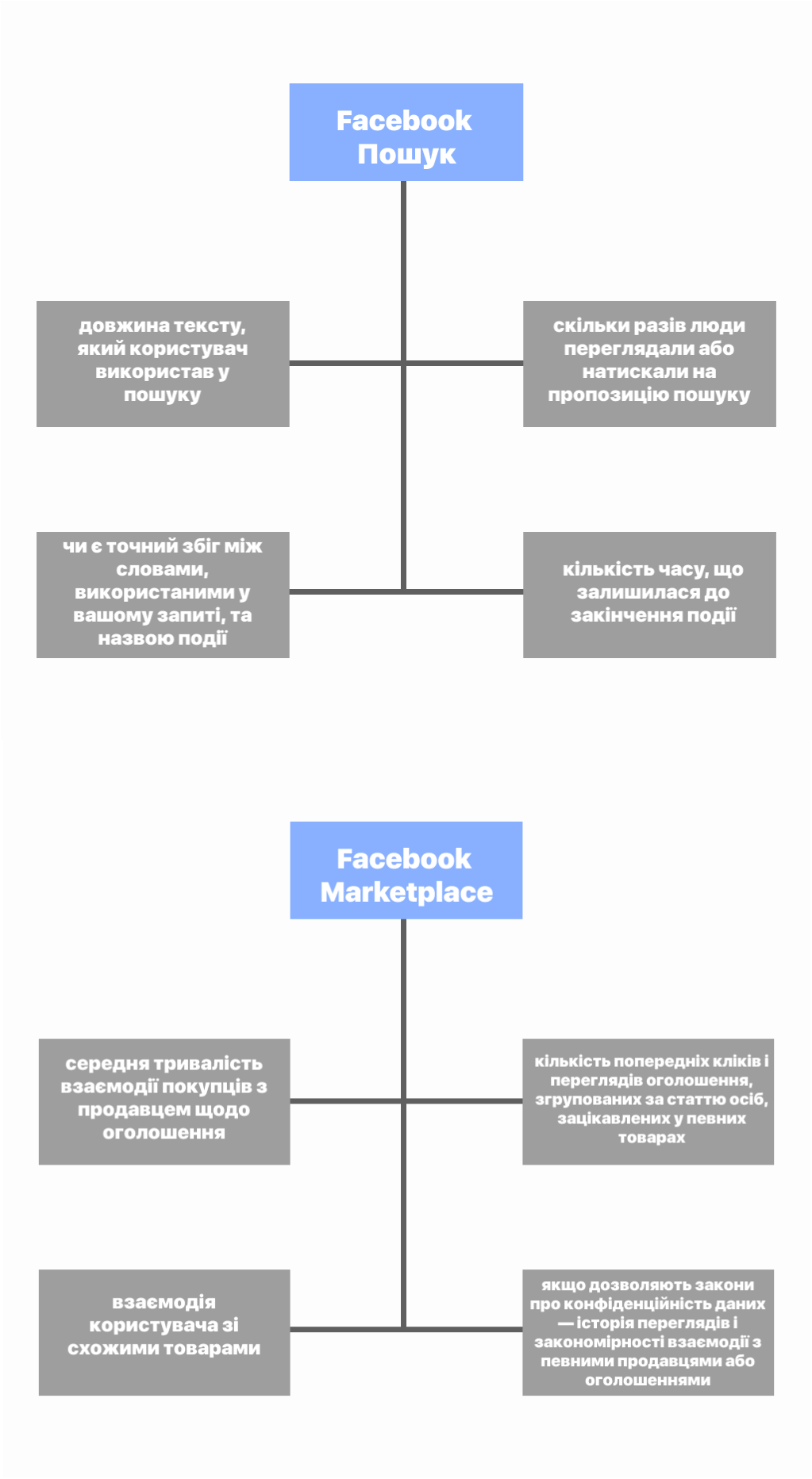
МОЖЛИВОСТІ АЛГОРИТМІВ АНАЛІЗУ ІНФОРМАЦІЇ КОРИСТУВАЧА У СОЦІАЛЬНИХ МЕРЕЖАХ

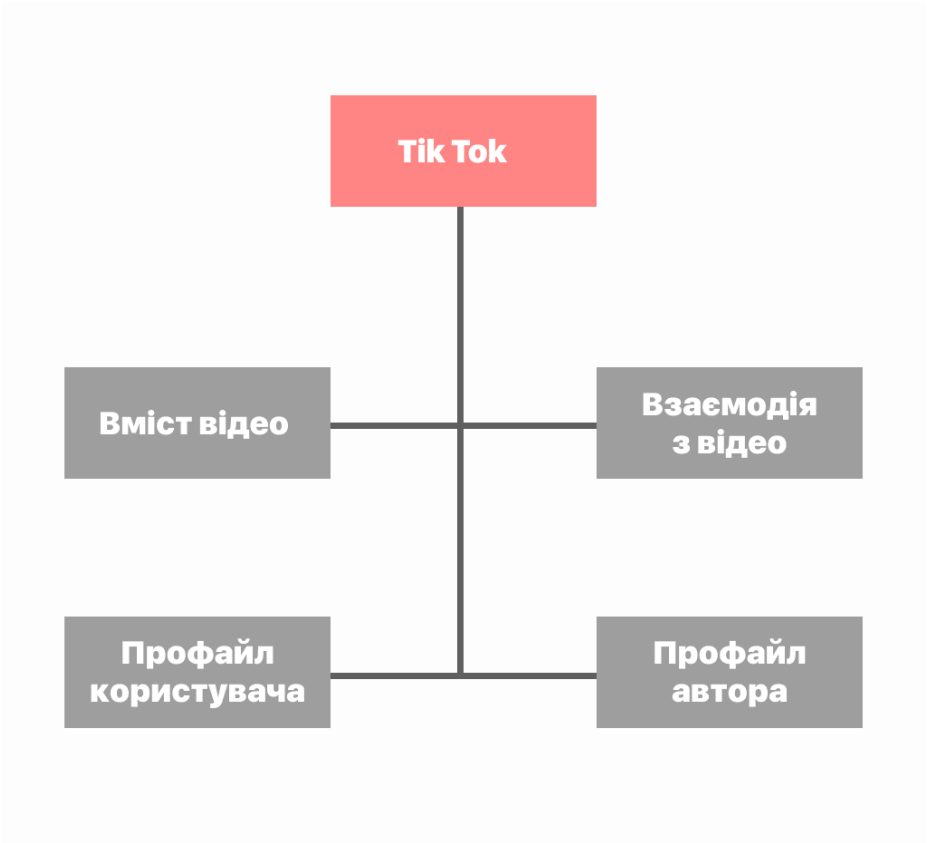
ДОДАТОК 1

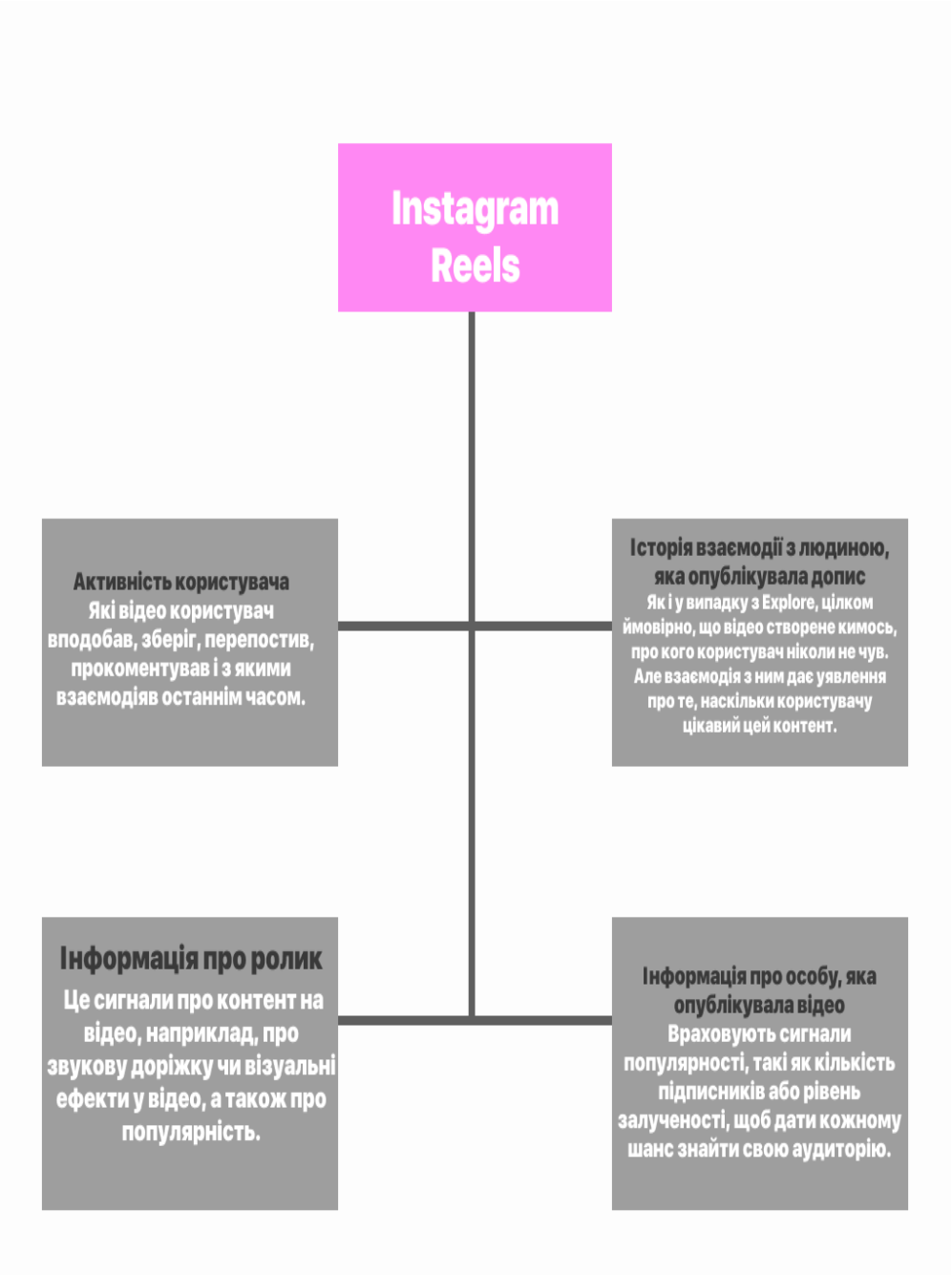


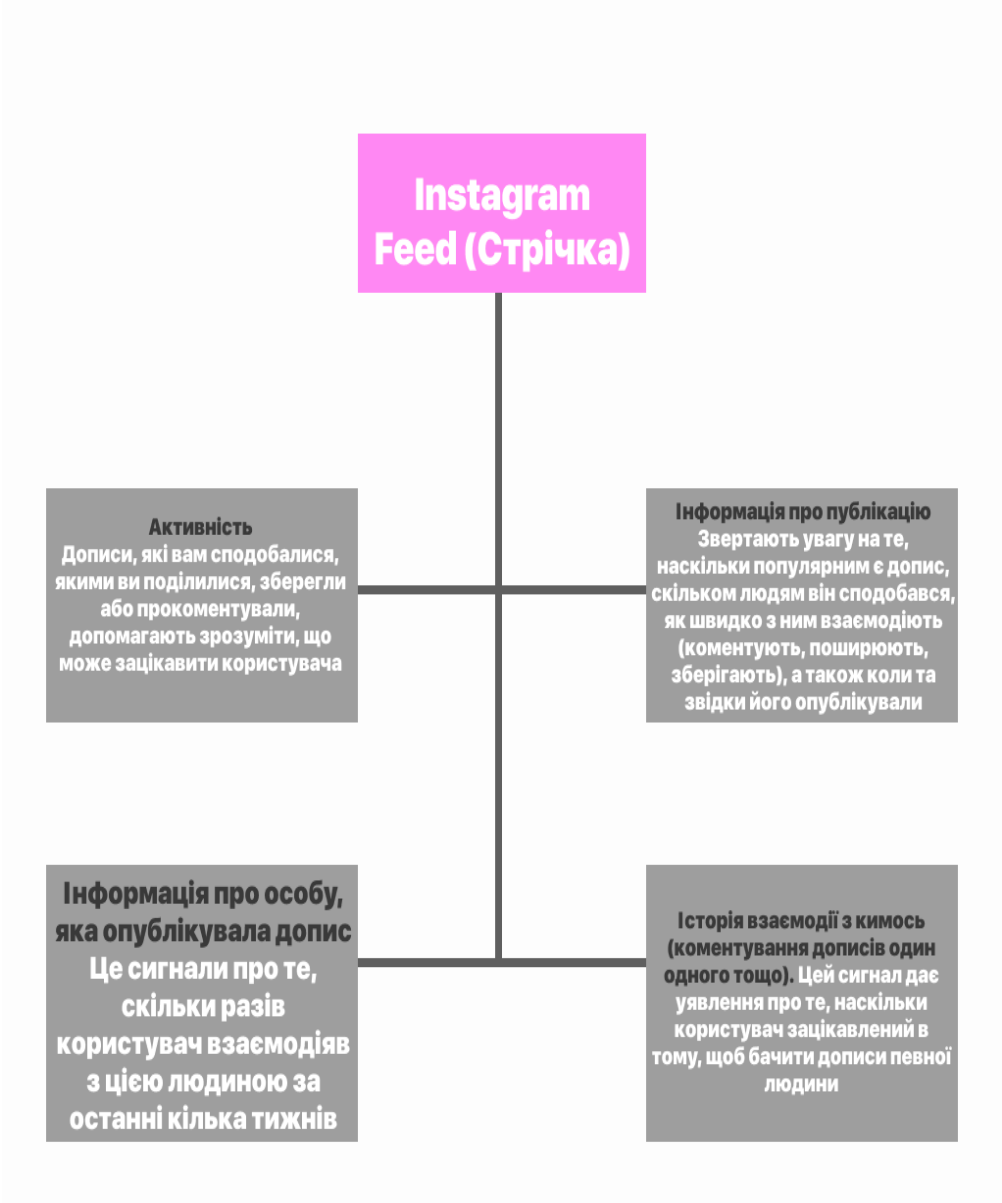

Facebook Reels
скільки разів ролик переглянули інші
які ролики користувач вподобав
які ролики натискав користувач, щоб переглянути їх в повноекранному режимі

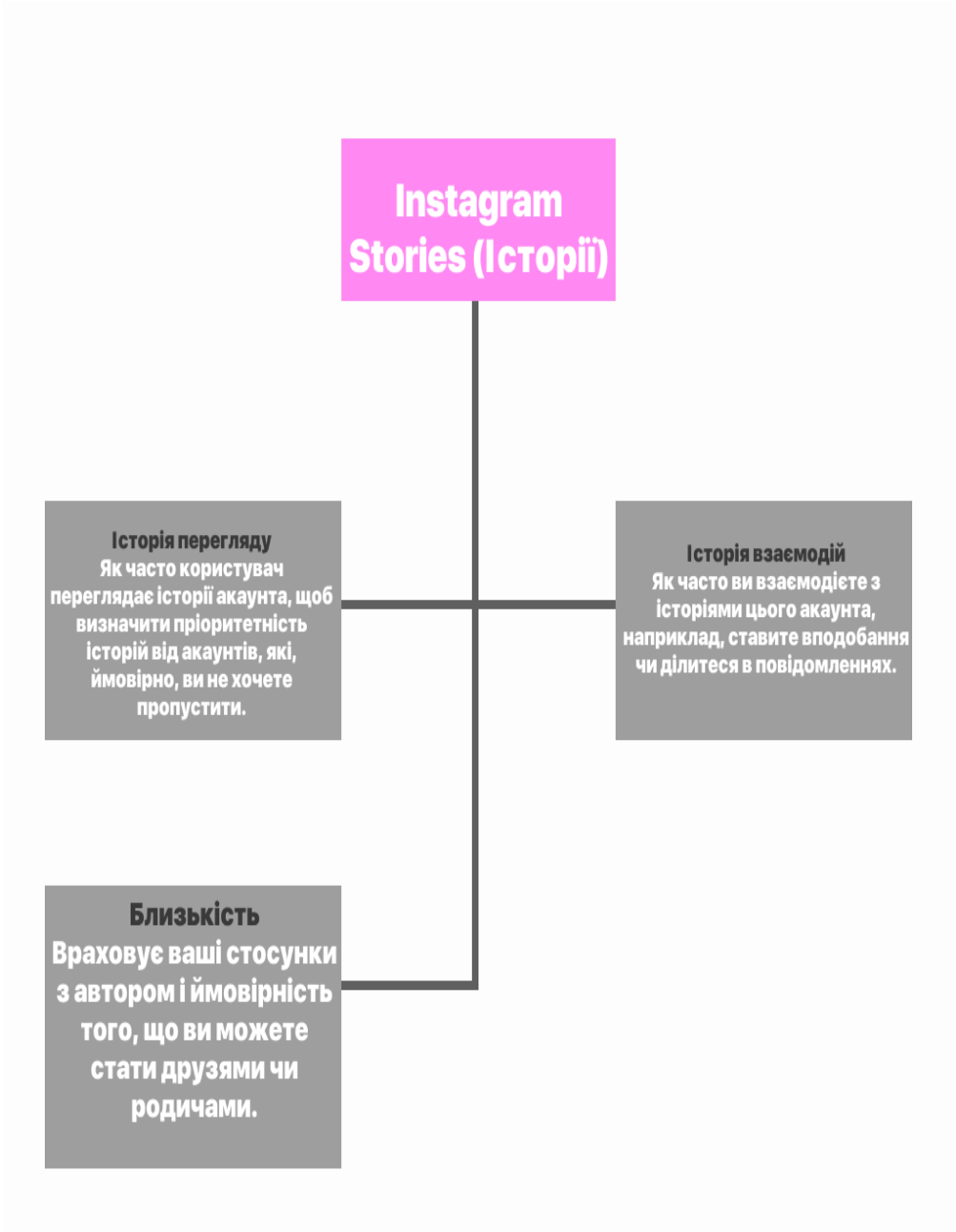

Facebook «Люди, яких ви можете знати» та «Сторінки, які можуть вам сподобатися»
скільки сторінок у Facebook користувач вподобав або за якими стежив
віковий діапазон користувача
скільки разів користувач надсилав запити на додавання в друзі людям із таким самим рівнем активності у Facebook, як і у запропонованої людини
скільки разів користувач надсилав запити на дружбу людям, які опублікували таку ж кількість фотографій профілю та обкладинки, як і запропонована людина
який відсоток друзів користувача у Facebook пов'язаний із запропонованою людиною (наприклад, є друзями друзів)

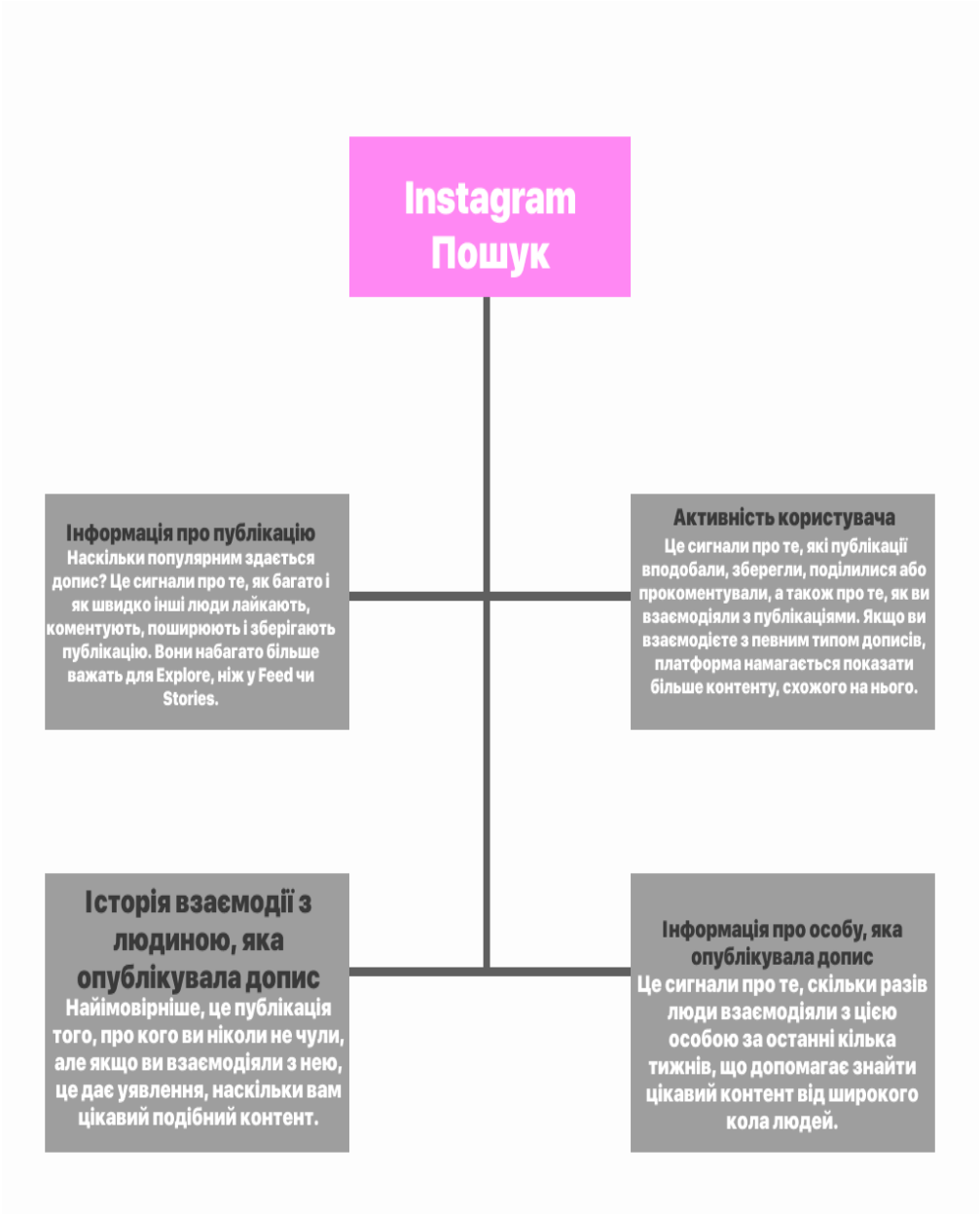

Facebook Пошук
довжина тексту, який користувач використав у пошуку
скільки разів люди переглядали або натискали на пропозицію пошуку
чи є точний збіг між словами, використаними у вашому запиті, та назвою події
кількість часу, що залишилася до закінчення події
Facebook Marketplace
середня тривалість взаємодії покупців з продавцем щодо оголошення
кількість попередніх кліків і переглядів оголошення, згрупованих за статтю осіб, зацікавлених у певних товарах
взаємодія користувача зі схожими товарами
якщо дозволяють закони про конфіденційність даних — історія переглядів і закономірності взаємодії з певними продавцями або оголошеннями


Tik Tok
Вміст відео
Взаємодія з відео
Профайл користувача
Профайл автора


Instagram Reels
Активність користувача
Які відео користувач вподобав, зберіг, перепостив, прокоментував і з якими взаємодіяв останнім часом.
Історія взаємодії з людиною, яка опублікувала допис
Як і у випадку з Explore, цілком ймовірно, що відео створене кимось, про кого користувач ніколи не чув. Але взаємодія з ним дає уявлення про те, наскільки користувачу цікавий цей контент.
Інформація про ролик
Це сигнали про контент на відео, наприклад, про звукову доріжку чи візуальні ефекти у відео, а також про популярність.
Інформація про особу, яка опублікувала відео
Враховують сигнали популярності, такі як кількість підписників або рівень залученості, щоб дати кожному шанс знайти свою аудиторію.

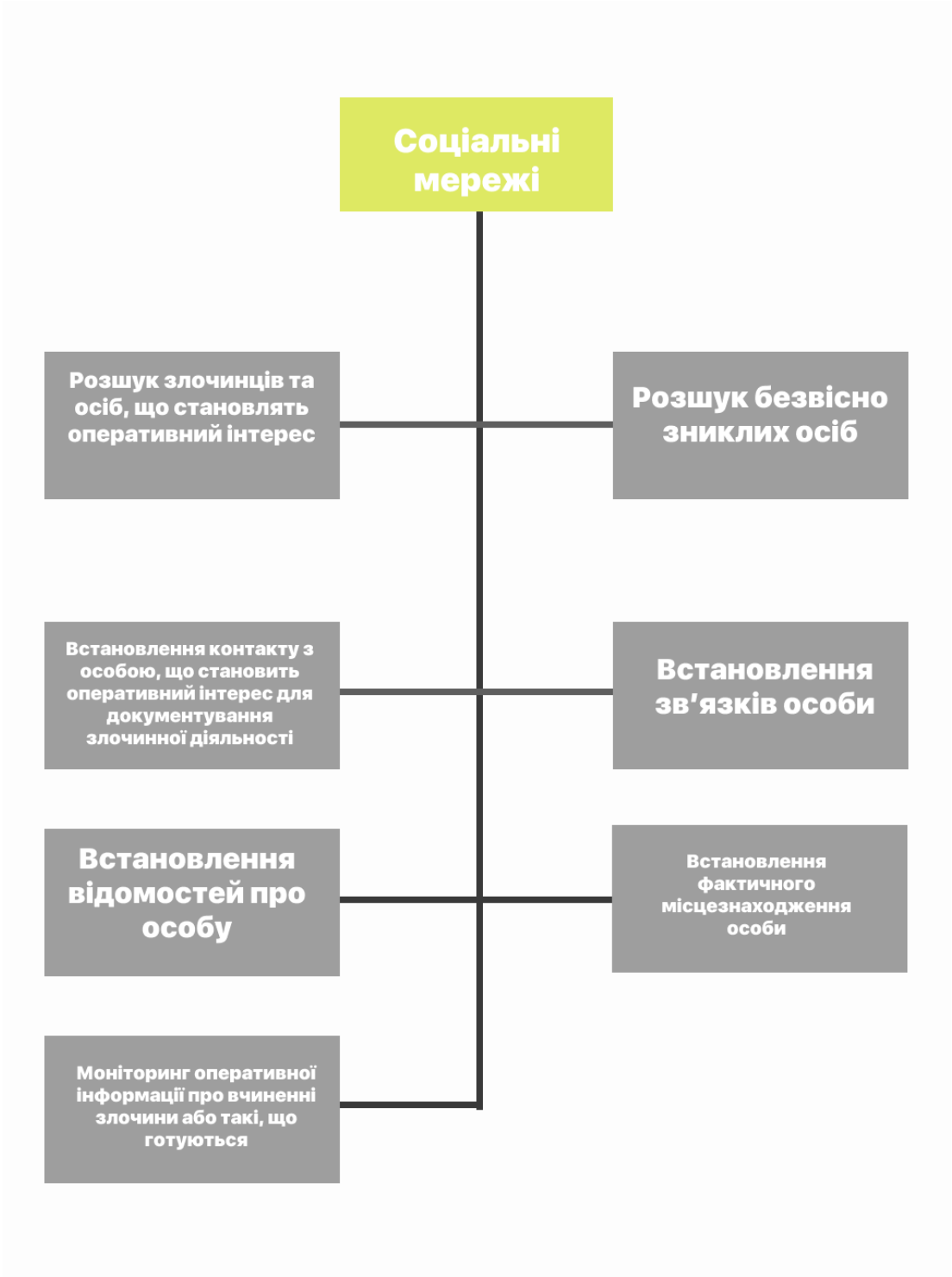

Instagram Feed (Стрічка)
Активність
Дописи, які вам сподобалися, якими ви поділилися, зберегли або прокоментували, допомагають зрозуміти, що може зацікавити користувача
Інформація про публікацію
Звертають увагу на те, наскільки популярним є допис, скільком людям він сподобався, як швидко з ним взаємодіють (коментують, поширюють, зберігають), а також коли та звідки його опублікували
Інформація про особу, яка опублікувала допис
Це сигнали про те, скільки разів користувач взаємодіяв з цією людиною за останні кілька тижнів
Історія взаємодії з кимось (коментування дописів один одного тощо). Цей сигнал дає уявлення про те, наскільки користувач зацікавлений в тому, щоб бачити дописи певної людини


Instagram Stories (Історії)
Історія перегляду
Як часто користувач переглядає історії акаунта, щоб визначити пріоритетність історій від акаунтів, які, ймовірно, ви не хочете пропустити.
Історія взаємодій
Як часто ви взаємодієте з історіями цього акаунта, наприклад, ставите вподобання чи ділитеся в повідомленнях.
Близькість
Враховує ваші стосунки з автором і ймовірність того, що ви можете стати друзями чи родичами.


Instagram
Пошук
Інформація про публікацію
Наскільки популярним здається допис? Це сигнали про те, як багато і як швидко інші люди лайкають, коментують, поширюють і зберігають публікацію. Вони набагато більше важать для Explore, ніж у Feed чи Stories.
Активність користувача
Це сигнали про те, які публікації вподобали, зберегли, поділилися або прокоментували, а також про те, як ви взаємодіяли з публікаціями. Якщо ви взаємодієте з певним типом дописів, платформа намагається показати більше контенту, схожого на нього.
Історія взаємодії з людиною, яка опублікувала допис
Найімовірніше, це публікація того, про кого ви ніколи не чули, але якщо ви взаємодіяли з нею, це дає уявлення, наскільки вам цікавий подібний контент.
Інформація про особу, яка опублікувала допис
Це сигнали про те, скільки разів люди взаємодіяли з цією особою за останні кілька тижнів, що допомагає знайти цікавий контент від широкого кола людей.

ОСНОВНІ НАПРЯМИ ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ В ОПЕРАТИВНО-РОЗШУКОВІЙ ДІЯЛЬНОСТІ

ДОДАТОК 2



Навчальне видання

ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Навчальний посібник

Колектив авторів

Редактор, оригінал-макет – *А. В. Самотуга*
Редактор *М. С. Касян*

Підп. до друку 13.11.2024. Формат 60х84/16. Друк – цифровий. Гарнітура – Times.
Ум.-друк. арк. 10,52. Обл.-вид. арк. 11,31. Зам. № 24/24-нп

Надруковано у Дніпровському державному університеті внутрішніх справ
49005, м. Дніпро, просп. Науки, 26, sed@dduvs.edu.ua
Свідоцтво про внесення до Державного реєстру ДК No 8112 від 13.06.2024