МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ
КАФЕДРА КРИМІНАЛЬНОГО АНАЛІЗУ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОЛГІЙ

Ганна ФОРОС, Володимир КАЛУГІН

Навчально-методичні рекомендації до вивчення навчальної дисципліни

ПОШУК ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ (OSINT) ПРАЦІВНИКАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ

Для здобувачів вищої освіти освітнього ступеня «бакалавр»
«бакалавр»галузь знань 26 «Цивільна безпека»
спеціальність 262 «Правоохоронна діяльність»

Навчально-науковий інститут підготовки фахівців для підрозділів кримінальної поліції Національної поліції України

2026 рік

Схвалено та рекомендовано до друку Науково-методичною радою Одеського державного університету внутрішніх справ (протокол № 11 від 25.12.2025 р.)

Рецензенти:
Олексій ВОЛОШКО - начальник Управління кримінального аналізу ГУНП України в Одеській області, полковник поліції
Дмитро ЛІСНІЧЕНКО - старший науковий співробітник науково-дослідної лабораторії з актуальних питань кримінального аналізу Одеського державного університету внутрішніх справ кандидат юридичних наук, доцент

Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції: навчально-методичні рекомендації/уклад. Форос Г.В., Калугін В.Ю./ Одеса ОДУВС, 2026. 37 с.

Навчально-методичні рекомендації «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції» присвячені розкриттю сучасних підходів, методів та інструментів, що застосовуються у процесі збору, аналізу та верифікації інформації з відкритих джерел у діяльності підрозділів кримінальної поліції. Висвітлено теоретичні засади OSINT, класифікацію відкритих джерел, алгоритми пошуку даних у соціальних мережах, медіапросторі, картографічних сервісах, доменних реєстрах та інших ресурсах мережі Інтернет.

Окрему увагу приділено питанням оцінки достовірності, релевантності та доказової цінності отриманої інформації, а також організації безпечної роботи в інформаційному середовищі. Навчально-методичні рекомендації містить практичні рекомендації щодо використання спеціалізованих інструментів OSINT, формування ефективних пошукових запитів, документування результатів та інтеграції здобутих даних у процес аналітичної та оперативно-розшукової діяльності.

ЗМІСТ

ПОЯСНЮВАЛЬНА ЗАПИСКА

Навчальна дисципліна «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції» є комплексом теоретичних положень та практичних завдань щодо нормативно-правового забезпечення, юридичних підстав застосування та пошуку інформації з відкритих джерел (OSINT) оперативними підрозділами поліції України під час виконання доручень слідчих органів, попередження, припинення, запобігання кримінальним правопорушенням та з метою їх своєчасного, ефективного виявлення, документування та забезпечення розслідування кримінальних проваджень.

Метою викладання навчальної дисципліни «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції» є навчання здобувачів вищої освіти діям зі збору інформації в мережі інтернет, формування професійних навичок, пов'язаних з професійною діяльністю в сфері аналізу інформації, виробленого в різних галузях наукових досліджень; загальних і приватних принципів здійснення аналітичної діяльності та вирішенні управлінських завдань; створення уявлення про цілі управління, формулюванні завдання інформаційно- аналітичної роботи.

Завданням вивчення навчальної дисципліни «Пошук інформації з відкритих джерел (OSINT) працівниками кримінальної поліції» є формування теоретичної бази знань щодо сутності поняття «OSINT» та його значення у діяльності кримінальній поліції; класифікації джерел відкритої інформації, основних етапів OSINT-розвідки; принципів планування OSINT-збору; правових засад використання відкритих джерел в Україні та ЄС; особливостей роботи з публічними реєстрами та державними базами даних; принципами перевірки достовірності інформації, отриманої з відкритих джерел, а також отримання практичних навичок з здійснення пошуку інформації про суб'єкт господарювання за допомогою відкритих реєстрів (YouControl, Opendatabot тощо), здійсненння ідентифікації особи за допомогою аналізу соціальних мереж (Facebook, Instagram, TikTok) із застосуванням OSINT-алгоритму; аналізу геолокаційних даних на основі відкритих мап (Google Maps, OpenStreetMap, Mapillary); здійснення зворотного пошуку зображення (Google Reverse Image, TinEye, Yandex); аналізу активності підозрюваної особи у Telegram-каналах (виявлення публікацій, згадок, груп); застосування техніки OSINT для збору інформації про транспортний засіб; пошуку даних у даркнет-джерелах із використанням спеціалізованих платформ (без доступу до нелегального контенту); підготовки стислого OSINT-звіт за результатами дослідження умовної події.

Перелік компетентностей, формування яких забезпечує вивчення навчальної дисципліни (з ОПП).

Інтегральна компетентність: Здатність вирішувати складні спеціалізовані задачі та практичні проблеми у сфері правоохоронної діяльності або у процесі навчання, що передбачає застосування певних теорій та методів правоохоронної діяльності і характеризується комплексністю та невизначеністю умов.

Загальні компетентності: ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області та розуміння. професійної діяльності. ЗК4. Здатність використовувати інформаційні та комунікаційні технології. ЗК5. Здатність вчитися і

оволодівати сучасними знаннями. ЗК7. Здатність до адаптації та дії в новій ситуації. ЗК8. Здатність приймати обґрунтовані рішення. ЗК9. Здатність працювати в команді. ЗК12. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.

Спеціальні компетентності: СК3. Здатність до критичного мислення та системного аналізу правових явищ. СК4. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел. СК5. Здатність визначати придатні для юридичного аналізу факти, систематизувати одержані результати, встановлювати причинно-наслідкові зв'язки, формулювати аргументовані висновки та рекомендації. СК8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних посягань. СК10. Здатність до аналізу та оцінки причин, умов та факторів, що впливають на вчинення кримінальних та адміністративних правопорушень. СК11. Здатність визначати особу правопорушника, аналізувати кількісні та якісні показники злочинності. СК16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.

Результати навчання: РН3. Розуміти та професійно застосовувати понятійний апарат права та правоохоронної діяльності. РН4. Формулювати і перевіряти гіпотези, виокремлювати юридично значущі факти, виявляти причинно-наслідкові зв'язки в діях і явищах для прийняття оптимального рішення в конкретних ситуаціях. РН6. Знати і розуміти принципи доброчесності та норми етичної поведінки, дотримуватися їх у професійній діяльності. РН7. Взаємодіяти із суб'єктами забезпечення публічної (громадської) безпеки і порядку, а також здійснювати комунікацію з фізичними та юридичними особами з метою виконання завдань у сфері правоохоронної діяльності. РН8. Здійснювати пошук інформації у доступних джерелах, аналізувати і оцінювати її для повного та всебічного встановлення обставин, необхідних для виконання професійних завдань. РН9. Використовувати інформаційно-комунікаційні системи та інші інформаційні ресурси, у тому числі ті, що мають технічний та криптографічний захист, поштовий зв'язок спеціального призначення, фельд'єгерський зв'язок, системи цифрового зв'язку суб'єктів сектору безпеки і оборони з метою виконання професійних завдань у сфері правоохоронної діяльності. РН14. Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності. РН15. Працювати самостійно та в команді при виконанні службових (посадових) обов'язків та під час розв'язання складних спеціалізованих задач у сфері правоохоронної діяльності. РН21. Організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.

Міждисциплінарні зв'язки: криміналістика, кримінальний процес, поліцейська діяльність, інформаційні та комунікаційні технології, інформаційно-аналітичне забезпечення професійної діяльності, оперативно-розшукова діяльність.

2. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальної дисципліни
		денна форма навчання
Кількість кредитів – 3	Галузь знань 26 «Цивільна безпека»	Вибіркова
Модулів – 1	Спеціальність 262 «Правоохоронна діяльність»	Рік підготовки
		3
Загальна кількість годин – 90		Семестр
		5
Освітній ступінь: «бакалавр»		Лекції 6 год.
		Семінарські заняття 12 год.
		Практичні заняття 22 год.
		Самостійна робота 50 год.
		Вид контролю: залік

Тематичний план

	Назви змістових модулів і тем	Кількість годин				
		денна форма				
		усього	у тому числі			
			л	с	п	с.р.
1	Тема 1. Поняття, правові підстави та основні завдання пошуку інформації з відкритих джерел (OSINT)	10	2	2		8
2	Тема 2. Оцінка даних за системою 4х4 під час здійснення пошуку інформації з відкритих джерел (OSINT)	12		2	2	8
3	Тема3. Використання інформаційно- пошукових систем під час здійснення пошуку інформації з відкритих джерел (OSINT) Безпечне використання мережі Інтернет	16	2	2	4	8
4	Тема 4. Застосування пошуку та аналізу текстів, фото-, відеоінформації, Google-карт під час проведення пошуку інформації з відкритих джерел (OSINT)	10		2	6	8
5	Тема 5. Проведення пошуку інформації з відкритих джерел (OSINT) в соціальних мережах	16		2	6	9
6	Тема 6. Напрямки використання пошукової інформації з відкритих джерел (OSINT) працівниками кримінальної поліції	14	2	2	4	9
Усього за семестр		**90**	**6**	**12**	**22**	**50**

3. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Сучасний етап розвитку інформаційного суспільства характеризується стрімким зростанням обсягів відкритої інформації, доступної через мережу Інтернет, електронні бази даних, соціальні мережі, медіа та інші публічні джерела. У цих умовах особливого значення для правоохоронних органів набуває OSINT (Open Source Intelligence) - розвідка на основі відкритих джерел інформації. В умовах інформаційного суспільства відкриті джерела даних (OSINT - Open Source Intelligence) стають важливим інструментом у діяльності поліції. Їх використання дозволяє отримувати оперативну, аналітичну та доказову інформацію без порушення законодавства, що суттєво підвищує ефективність розкриття та розслідування злочинів, розшукових заходів і профілактичної роботи.

Застосування OSINT сприяє: удосконаленню аналітичного забезпечення розслідувань; оперативному виявленню зв'язків між особами, подіями та організаціями; моніторингу соціальних мереж, ЗМІ та публічних баз даних; попередженню кіберзлочинності та інформаційних загроз.

Використання OSINT забезпечує можливість отримання, аналізу та систематизації інформації, що може бути використана у процесі розслідування злочинів, проведення оперативно-розшукових заходів, а також у профілактичній діяльності поліції.

Методи які використовуються в ході пошуку: контекстний пошук (Google Dorking, спеціалізовані бази); соціальний моніторинг (аналіз профілів, мережевих зв'язків, активності користувачів); геоінформаційний аналіз (визначення місць подій за фото/відео); аналіз метаданих (EXIF, IP-логів, цифрових слідів); візуальна аналітика (створення графічних моделей зв'язків).

ТЕМА № 1. Поняття, правові підстави та основні завдання пошуку інформації з відкритих джерел (OSINT)

Загальна характеристика поняття пошуку інформації з відкритих джерел OSINT. Визначення основних завдань пошуку інформації з відкритих джерел (OSINT).

Нормативно-правове забезпечення та юридичні підстави застосування пошуку інформації з відкритих джерел (OSINT). Роль пошуку інформації з відкритих джерел (OSINT) у діяльності кримінальної поліції та органів досудового розслідування. Забезпечення розслідування міжнародних воєнних злочинів з використанням інструментарію OSINT. Аналітична підтримка Європолу.

Характеристика історичних етапів виникнення, становлення та розвитку пошуку інформації з відкритих джерел (OSINT). Основні особливості пошуку інформації з відкритих джерел (OSINT) з кінця XX століття до теперішнього часу.

Функціонування спільної слідчої групи з розслідування міжнародних злочинів, скоєних в Україні.

Методичні рекомендації

При підготовці до заняття необхідно звернути увагу на те, що розвідка відкритих джерел (англ. Open source intelligence, OSINT) - концепція, методологія і технологія добування з відкритих джерел військової, політичної, економічної та іншої безпекової інформації і використання її для підтримки прийняття рішень у сфері національної оборони і безпеки, і виступає невід`ємною частиною багатьох видів розвідки. Методологію і технологію OSINT почали активно вивчати і використовувати у сфері бізнесу. У бізнесі OSINT споріднена з Competitive Intelligence (Конкурентною розвідкою) і принципово відрізняється від Industrial espionage (промислового шпигунства). OSINT у військовій сфері подібна до застосування Competitive Intelligence (Конкурентної розвідки) у сфері бізнесу, яка часто закривається більш широким терміном «Аналіз консолідованої інформації».

Також необхідно зосередитись на тому, що пошук інформації з відкритих джерел, або OSINT, є системним процесом збирання, аналізу та використання відомостей, що знаходяться у вільному доступі. Його сутність полягає у виявленні, відборі та перевірці даних із загальнодоступних ресурсів для отримання цінної інформації. На відміну від закритих або таємних джерел, відкриті ресурси не потребують спеціального дозволу чи правового статусу для

доступу. Під відкритими джерелами розуміють широкий спектр інформаційних каналів: засоби масової інформації, інтернет-ресурси, офіційні звіти органів влади, наукові публікації, соціальні мережі, бази даних та інші ресурси, що перебувають у вільному доступі. Розвиток цифрових технологій значно розширив обсяг і швидкість отримання такої інформації, зробивши OSINT одним із ключових інструментів сучасної аналітичної діяльності.

Для покращення розуміння теми необхідно ознайомитися з використанням спеціальних символів і операторів:

" "	точна фраза (наприклад: "cyber crime Ukraine")
site	пошук на певному сайті (site:facebook.com)
filetype	пошук за типом файлу (filetype:pdf)
inurl	пошук у назві сторінки
intitle	пошук у заголовку сторінки

Для ефективності процесу OSINT використовуються спеціалізовані інструменти, які дозволяють здійснювати моніторинг джерел, пошук зв'язків між об'єктами та аналіз цифрових слідів.Їх можна класифікувати за функціональним призначенням:

Інструменти збору даних

Google Dorking	використання розширених операторів пошуку Google для виявлення прихованої або малодоступної інформації
Shodan	пошукова система, що сканує пристрої, підключені до Інтернету, та надає дані про сервери, вебкамери, маршрутизатори тощо
Censys	аналог Shodan, який дозволяє глибше аналізувати сертифікати безпеки та структуру Інтернету
theHarvester	інструмент для збору адрес електронної пошти, доменів, IP-адрес і метаданих із різних джерел

Інструменти аналізу та візуалізації даних (системи побудови зв'язків, аналізу мережевих графів)

Maltego	потужна платформа для побудови графічних зв'язків між об'єктами (особами, організаціями, доменами, акаунтами)
SpiderFoot	система автоматизованого збору та аналізу інформації з понад 100 джерел, включно з соціальними мережами та базами даних
Kibana	інструмент для візуалізації великих масивів даних у вигляді інтерактивних панелей
Gephi	програма для побудови соціальних графів і дослідження мережевих взаємозв'язків

Інструменти перевірки та геолокації

Google Earth / Google Maps	використовуються для підтвердження місця подій за супутниковими знімками
ExifTool	аналіз метаданих зображень (дата, місце зйомки, тип пристрою)
FotoForensics	перевірка автентичності зображень і виявлення цифрових маніпуляцій
InVID	плагін для аналізу відео, що дозволяє перевіряти фейки та визначати джерело відеоматеріалів

Інтегровані OSINT-платформи

IntelTechniques	набір вебінструментів для комплексного пошуку даних про осіб та організації
OSINT Framework	каталог інструментів і ресурсів для розвідки з відкритих джерел, упорядкований за напрямами (соціальні мережі, IP-адреси, зображення тощо)
Social Links / Paliscope	комерційні платформи, які поєднують збір, аналіз та документування OSINT-розслідувань

Необхідно зазначити, що для застосування методології OSINT такими нормами права є, насамперед, Конституція та закони України: «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про оперативно-

розшукову діяльність», «Про доступ до публічної інформації», «Про захист персональних даних», «Про телекомунікації» та ін. Не всі перелічені закони обов'язково повністю за своїм змістом призначені для регулювання інформаційної діяльності, однак саме вони містять основні положення щодо збору, накопичення, збереження, особливості використання інформації тощо.

На *самостійну підготовку* виноситься питання про етичні стандарти OSINT розслідувань, спираючись на той факт, що завдяки легкому доступу до величезної кількості інформації в інтернеті, індивіди та організації можуть використовувати OSINT для виявлення особистої інформації про людей без їхньої згоди і відому. Крім того, використання OSINT утруднює захист особистих даних, оскільки багато інформації публікуються самими користувачами в соціальних мережах, форумах та інших платформах. Етичні межі, які стосуються інформації з відкритих джерел, постійно змінюються та розвиваються. Однак однією з найбільш стабільних позицій є та, відповідно до якої дані, зібрані з відкритих джерел, повинні використовуватися таким чином, щоб не порушити існуючи закони про конфіденційність, не повинні використовуватися у злочинних цілях і мають збиратися тільки тоді, коли це необхідно. Форма педагогічного контролю – усне опитування під час проведення семінарського заняття.

Семінарське заняття – 2 години

Учбові питання:

1. Загальна характеристика поняття пошуку інформації з відкритих джерел (OSINT). Визначення основних завдань пошуку інформації з відкритих джерел (OSINT).
2. Характеристика історичних етапів виникнення, становлення та розвитку пошуку інформації з відкритих джерел (OSINT).
3. Нормативно-правове забезпечення та юридичні підстави застосування пошуку інформації з відкритих джерел (OSINT).
4. Джерела відкритої інформації.
5. Роль пошуку інформації з відкритих джерел (OSINT) у діяльності кримінальної поліції та органів досудового розслідування.

Питання для самоконтролю:

1. Суб'єкти використання та зміст діяльності щодо пошуку інформації з відкритих джерел (OSINT).
2. Які цілі та завдання передбачається досягти за результатами використання інформації з відкритих джерел (OSINT)?
3. Які нормативно-правові акти регулюють діяльність підрозділів кримінальної поліції щодо збору та обробки інформації з відкритих джерел (OSINT?
4. Які вимоги до збереження такого роду інформації?
5. Назвіть методи та інструменти для аналізу та обробки інформації з відкритих джерел?
6. Які існують виклики інформаційно-аналітичного забезпечення в умовах розширення цифрового середовища та зростання обсягів інформації?
7. Які основні функції виконують підрозділи кримінальної поліції в контексті інформаційно-аналітичного забезпечення?
8. Історія становлення та застосування пошуку інформації з відкритих джерел (OSINT).
9. Засоби та ресурси для інформаційно-аналітичного забезпечення в роботі підрозділів кримінальної поліції.
10. Нормативно-правове забезпечення інформаційно-аналітичного забезпечення в сфері кримінальної поліції.

ТЕМА № 2. Оцінка даних за системою 4x4 під час здійснення пошуку інформації з відкритих джерел (OSINT)

Сутність інформації, види джерел інформації, специфіка її передавання та принципи управління інформацією.

Визначення цінності елементів інформації з точки зору достовірності, надійності, відповідності та точності.

Висновок про релевантність для досліджуваного феномену.

Методичні рекомендації

При вивчення даної теми необхідно звернути інформацію звертаємо увагу, що «відкриті джерела» можна визначити як інформацію, надану будь-якою особою чи групою осіб «без очікування на конфіденційність. Іншими словами, це інформація, яка не захищена від публічного розголошення. Те, що інформація є загальнодоступною, не обов'язково означає, що вона безкоштовна або легкодоступна.

Власне, необхідно зазначити, що на даний момент існує безліч відкритих джерел, якими можуть користуватися аналітики при проведенні OSINT розслідувань. До найбільш популярних відносять наступні: Новини та ЗМІ - публікації в ЗМІ, радіо, телебачення, газети та інші види друкованих чи інших ЗМІ. 2. «Сіра» література - яка включає в себе будь-яку загальнодоступну немедійну інформацію про політику в приватному та державному секторах. 3. Соціальні мережі - можуть охоплювати весь спектр довгострокового контенту, а також короткотривалий контент (твіти, підписи в Instagram), фотографії, теги тощо. Метадані, пов'язані з вмістом соціальних мереж, є ключовими для OSINT аналітиків, допомагаючи у візуалізації зв'язків та розумінні хронології подій. 4.Темна мережа (DarkNet) - використовується для означення веб сторінок, які не проіндексовані та потребують спеціального програмного забезпечення для отримання доступу. 5. Всесвітня мережа «Інтернет»: онлайн-публікації, блоги, дискусійні групи (форуми), медіа громадян (наприклад, відео з мобільних телефонів, контент, створений користувачами). 6. Офіційні державні джерела: публічні урядові звіти, бюджети, слухання, телефонні довідники, прес-конференції, веб-сайти та виступи. 7. Професійні та академічні публікації: інформація, отримана з журналів, конференцій, симпозіумів, наукових праць, дипломів та дисертацій. 8. Комерційні дані: комерційні зображення, фінансові та промислові оцінки, бази даних. 9. Інша література: технічні звіти, патенти, робочі документи, ділові документи, неопубліковані роботи та інформаційні бюлетені.

При вивченні питання щодо оцінка інформаційної цінності слід зазначити, що у сучасному інформаційному суспільстві кількість відкритих джерел та обсяг доступної інформації зростають у геометричній прогресії. У межах OSINT (Open Source Intelligence) оцінка інформаційної цінності є необхідною умовою для відбору релевантних, достовірних і корисних відомостей, які можуть вплинути на прийняття рішень. Інформаційна цінність - це ступінь корисності, достовірності та значущості певних даних для вирішення конкретного завдання або досягнення поставленої мети. Вона визначає, наскільки отримана інформація: впливає на розуміння ситуації; допомагає прийняти ефективне рішення; є новою, унікальною або уточнює вже наявні знання. Оцінка інформаційної цінності дозволяє відокремити інформаційний шум від справді важливих фактів.

На *самостійну підготовку* виноситься більш детальний розгляд міжнародних стандартів у сфері оцінки достовірності інформації. Варто зауважити, що правоохоронні органи загалом застосовують уніфіковані (міжнародні) стандарти та системи у сфері оцінки достовірності інформації, яка передбачає окреме оцінювання джерела на надійність, а змісту інформації – безпосередньо на достовірність, наприклад: «4×4», «5×5», «6×6» або «4×4×4», «5×5×5», «6×6×6», де третім критерієм є приватність інформації. У світовій правоохоронній практиці прийняті такі позначення критеріїв надійності джерела: «A», «B», «C», «D». Для узгодженості з уже прийнятими нормативними актами України вважаємо за доцільне використовувати таке позначення критеріїв надійності джерела: «А», «Б», «В», «Г». Щодо критеріїв достовірності інформації пропонуємо аналогічні зі світовим досвідом позначення: «1», «2», «3», «4». Те саме стосується критеріїв оцінки приватності інформації: «1», «2», «3», «4». Форма педагогічного контролю – усне опитування під час проведення семінарських та практичних занять.

Семінарське заняття – 2 години

Учбові питання:

1. Сутність інформації, види джерел інформації, специфіка її передавання та принципи управління інформацією.
2. Визначення цінності елементів інформації з точки зору достовірності, надійності, відповідності та точності.

3. Висновок про релевантність для досліджуваного феномену.

Практичне заняття – 2 години

Завдання до практичного заняття - зробити висновок, яке з повідомлень є найбільш придатним для подальшого використання в аналітичному звіті.

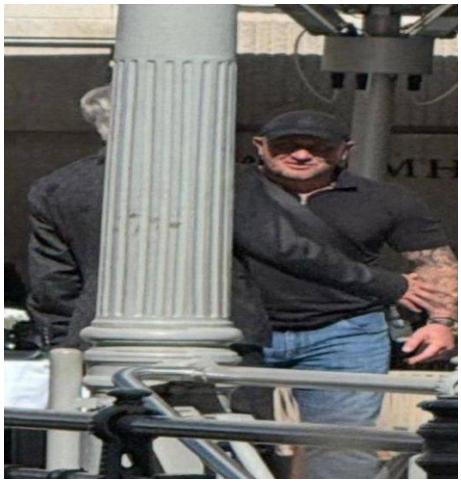
Форма звіту: з критеріями та вашими оцінками (наприклад, за шкалою від 1 до 4), коротке обґрунтування вибору.

Вам надано уривки з чотирьох різних новинних повідомлень. Необхідно проаналізувати кожне повідомлення за такими критеріями: достовірність; актуальність; точність; відповідність темі (релевантність); джерело походження.

Завдання 1.

Сили безпілотних систем атакували у Росії Рязанський нафтопереробний завод 🔥
https://t.me/+9dhK8I5F6xVkMDli

Завдання 2



Кримінальна сходка чи операція спецслужб: офіцер розвідки фігурує у підозрілій зустрічі з проросійськими авторитетами

На одному з оприлюднених відео зафіксовано зібрання великої кількості озброєних осіб та кортежів броньованих автомобілів. В одному з авто був помічений підполковник Головного управління розвідки Міноборони Віктор Торкотюк, позивний «Титан».

За попередніми даними, зустріч мала відбутись між офіцером ГУР і представниками кримінальних угруповань кавказького походження, які мають російські зв'язки та проживають як в Україні, так і за її межами.

За інформацією журналістів, між ними планувалась масована сутичка, яка судячи з кількості людей мала б фатальні наслідки.

Однак відкрита конфронтація не відбулася — сторони розійшлися без стрілянини. За інформацією джерел, «Титан» за короткий час зібрав значні сили, після чого кавказькі опоненти, не наважилися доїхати до місця зустрічі.

Офіційні коментарі від силових структур або представників влади поки що відсутні. Також не зрозуміло, чому такі ситуації не врегульовуються іншими методами, та яким чином проросійський вплив досі зберігся в Україні.

При цьому більшість провідних ЗМІ не надали розголосу цій події.

(https://t.me/+IffoCwNTQWUwNzhi)

Завдання 3.

ВСУ разрабатывают крылатую ракету Ан-204 — дальность будет достигать 2830 км, а длинна 200 метров", — росвоєнкор

Державне підприємство «Антонов», відоме авіаперевезеннями та виробництвом літаків серії «Ан», з початку війни також займається виробництвом безпілотників, зокрема БпЛА.

За даними джерел, на підприємстві почали розробку КРНБ — крилатої ракети наземного базування.

Ракети отримають маркування Ан-202, Ан-203, Ан-204, остання з яких матиме дальність до 2830 км.

Виробництво відбувається на одному конвеєрі з ракетами «Фламінго». Деталі про платформу запуску поки невідомі — це може бути як колесна база, так і пускова на причепі.

Планується, що до кінця року ракета буде готова до випробувань з метою досягнення радіусу ураження до 3000 км.

Цікаво, що Зеленський в інтерв'ю Le Point сказав, що Україна вже має ракети з дальністю 3000 км.

За його інформацією ракета має довжину 200 метрів»

(https://t.me/+9dhK8I5F6xVkMDli)

Завдання 4.

Так спецслужби КНДР «зачищають» сліди свого вождя Кім Чен Ина по місцях його перебування в Китаї — вони мають зробити все, щоб жодні елементи ДНК північнокорейського диктатора не опинилися у його противників

Свита Кім Чен Ина буцімто запобігає виникненню небажаних обставин, які б негативно позначилися на ньому:

«Нічого не можна залишати, оскільки це може зашкодити майбутньому».

(https://t.me/+9dhK8I5F6xVkMDli)

Питання для самоконтролю:

1. Вкажіть сутність інформації.
2. Які види джерел інформації Ви Знаєте?
3. Яким чином здійснюється визначення цінності елементів інформації з точки зору достовірності, надійності, відповідності та точності?
4. В чому полягає мета оцінки інформації?
5. Вкажіть критерії оцінки інформації.
6. Вкажіть оцінки (градації) достовірності джерела походження інформації та достовірності інформації.
7. Охарактеризуйте уніфіковані (міжнародні) стандарти і норми у сфері оцінки достовірності джерел інформації та змісту інформації (4×4), (5×5×5), (6×6).

ТЕМА № 3. Використання інформаційно-пошукових систем під час здійснення пошуку інформації з відкритих джерел (OSINT)

Класифікація джерел інформації. Загальна характеристика відкритих (доступних для загального користування) джерел інформації. Загальна характеристика закритих (спеціальних джерел, які містять інформацію, що отримується негласними методами) джерел інформації.

Загальна характеристика внутрішньовідомчих джерел даних (бази даних; системи інформаційно-аналітичного забезпечення). Загальна характеристика зовнішніх джерел інформації (відомості від центральних органів виконавчої влади держави. Відомості інших правоохоронних органів держави; дані від правоохоронних органів інших держав; відомості із засобів масової інформації; інтернет-ресурси тощо. Характеристика інструментів та методів пошуку інформації з відкритих джерел (OSINT).

Методичні рекомендації

При вивченні даної теми необхідно зазначити, що спеціальні інструменти пошуку мають спеціальні засоби організації пошуку, що забезпечують ефективний пошук потрібної інформації в Інтернеті. Знайдену в результаті пошуку інформацію обов'язково потрібно проаналізувати.

До найбільш популярних відкритих джерел при проведенні OSINT розслідувань відносять наступні:

1. Новини та ЗМІ - публікації в ЗМІ, радіо, телебачення, газети та інші види друкованих чи інших ЗМІ.

2. «Сіра» література яка включає в себе будь-яку загальнодоступну немедійну інформацію про політику в приватному та державному секторах. Сюди включаються документи та звіти благодійних та неурядових організацій, міжурядових установ і аналітичних центрів, а також статистику злочинності, дані перепису та інформацію, що міститься в академічних базах даних, журналах і звітах

3. Соціальні мережі, які можуть охоплювати весь спектр довгострокового контенту. Значна частина найкориснішої інформації в соціальних мережах не проіндексована і зберігається в «глибокій мережі», що робить стандартні вебпереглядачі неспроможними її виявити.

4. Темна мережа (DarkNet), що використовується для позначення веб сторінок, які не проіндексовані та потребують спеціального програмного забезпечення для отримання доступу. У «темній мережі» користувачів і операторів не можна відстежити, і, як наслідок, це дуже зручне місця для вчинення злочинів. Аналітики повинні проявляти обережність, щоб не розкривати власну особу та не розкрити своє розслідування, а також не наближатися до шкідливого програмного забезпе чення чи впливу незаконних ЗМІ. Крім того, аналітики також повинні використовувати OSINT-інструменти, щоб уникнути непотрібного контакту з потенційно травматичним матеріалом під час перегляду темної мережі.

До зовнішніх джерел інформації від центральних органів виконавчої влади держави. Інформація з Єдиного державного реєстру юридичних осіб, фізичних осіб – підприємців та громадських формувань (ЄДР), Реєстр нерухомості (https://kap.minjust.gov.ua), Кадастрова карта

(http://map.land.gov.ua/kadastrova-karta), реєстр судових рішень (http://www.reyestr.court.gov.ua/), Єдиний державний реєстр судових рішень.

Особливу увагу слід звернути на загальні поради з пошуку інформації в інтернеті, а саме:

- обміркуйте зміст свого запиту. Можливо, частково ви вже знаєте відповідь. Щоб знайти інформацію, шукайте одночасно ключові слова із запитання і відомої вам відповіді;
- використовуйте перевірені вами пошукові системи. Якщо ви новачок у цій сфері, то вам не завадить приділити деякий час вивченню наявних для цього мережевих засобів і принципів їхньої роботи;
- кількість документів, отриманих у результаті пошуку, може бути величезною. Тому вирішальне значення для оптимального пошуку інформації має правильний набір ключових слів. Опис того, як складати ефективні запити, дається в самих пошукових ресурсах. Зазвичай будь-яка пошукова система має довідковий розділ;
- перевіряйте орфографію в написанні слова. Використовуйте синоніми, якщо список знайдених сторінок занадто малий;
- шукайте більше ніж по одному слову. Максимально звужуйте предмет пошуку;
- не починайте звичайні слова з великої літери, крім власних назв;
- використовуйте посилання «знайти схожі документи», якщо один із знайдених документів найбільш близький до шуканого;
- зверніть увагу, що контекст документа вже може містити відповідь, тобто не потрібно буде заходити в сам документ;
- у разі потреби використовуйте мову запитів і системи розширеного пошуку використовуваних пошукових систем.

З питань застосування пошуку та аналізу фото (зображень) з метою ідентифікації осіб, визначення локацій, виявлення вірусних фотографій, аналізу подій тощо, необхідно звернути увагу на той факт, що ідентифікація осіб за допомогою аналізу фотографій є однією з найпоширеніших практик у сфері цифрової криміналістики, безпеки та OSINT.

Семінарське заняття – 2 години

Учбові питання:

1. Загальна характеристика пошуку та аналізу текстової інформації із засобів масової інформації; інтернет-ресурсів.
2. Загальна характеристика внутрішньовідомчих джерел даних (бази даних; системи інформаційно-аналітичного забезпечення).
3. Загальна характеристика зовнішніх джерел інформації (відомості від центральних органів виконавчої влади держави.
4. Відомості інших правоохоронних органів держави; дані від правоохоронних органів інших держав; відомості із засобів масової інформації; інтернет-ресурси тощо.
5. Характеристика інструментів та методів пошуку інформації з відкритих джерел (OSINT).

Практичні заняття – 4 години

Завдання до практичного заняття

Завдання 1. На місті вчинення злочину свідки бачили 2 автомобілі: LEXUS (мабуть чорного або темно синього кольору) з державним номером ВН9291ЕЕ та DAEWOO-LANOS (мабуть сірого кольору) з державним номером АА7061ВС.

Перевірити за допомогою розшукових сервісів МВС України (https://wanted.mvs.gov.ua) усі дані на ці автомобілі, що можуть бути в угоні.

Завдання 2. Під час бойових дій був знайдений труп вбитого російського військовослужбовця, без погон та знаків розрізнення, за ознаками – за національністю можливо кримського чи російського (казанського) татарина.

При ньому був знайдений значно пошкоджене посвідчення офіцера, видане (російською) на прізвище «Мамедов», ім’я «Самир», по-батькові – пошкоджено. Перевірити по сервісу МВС України «Потерь.НЕТ» (https://poternet.site) наявність даних на зазначену особу та його офіцерське звання.

Завдання 3. Визначити за допомогою інструментарію OSINT підприємство та створити досьє на юридичну особу.

Завдання 4. Визначити за допомогою інструментарію OSINT підприємство та створити досьє на юридичну особу

Завдання 5. Визначити за допомогою інструментарію OSINT локацію об’єкта

Питання для самоконтролю:

1. Класифікація джерел інформації
2. Відкриті (доступні для загального користування) джерела інформації.
3. Внутрішньовідомчі джерела даних.
4. Методи пошуку інформації з відкритих джерел (OSINT)?
5. Принципи роботи і можливості розшукових ресурсів веб-порталу Міністерства внутрішніх справ (МВС) України.
6. Можливості розшукових ресурсів інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України».

ТЕМА № 4. Застосування пошуку та аналізу текстів, фото-, відеоінформації, Google-карт під час проведення пошуку інформації з відкритих джерел

Семінарське заняття – 2 години

Особливості застосування пошуку та аналізу текстів з метою пошуку інформації в текстовому форматі, включаючи новини, статті, блоги, форуми та інше для виявлення потенційних загроз чи ризиків. Застосування пошуку та аналізу фото (зображень) з метою ідентифікації осіб, визначення локацій, виявлення вірусних фотографій, аналізу подій тощо.

Застосування відео-пошуку з метою виявлення відеоматеріалів про події, моніторинг відеоблогів, аналіз вірусного відео. Особливості застосування Google-карт для визначення маршрутів пересування, аналізу місцевості, моніторингу геолокаційних даних.

Методичні рекомендації

При вивченні даної теми акцентуємо увагу на тому, що пошук інформації – завдання, яке найчастіше доводиться виконувати користувачу глобальної мережі.

Важливо зазначити, що текстова інформація є багатошаровою і може містити як явні, так і приховані сигнали загрози. Наприклад, новини про політичну нестабільність у регіоні можуть свідчити про можливі соціальні заворушення. Аналіз статей і блогів може виявити настрої населення, які можуть призвести до протестів чи інших небезпечних дій. Таким чином, систематичний підхід до збору та аналізу текстів може допомогти виявити потенційні ризики на ранніх стадіях.

Використання алгоритмів машинного навчання для аналізу текстів може значно підвищити ефективність пошуку. Наприклад, класифікація текстів за темами або емоційний аналіз можуть допомогти виявити, які теми викликають найбільше занепокоєння у суспільстві. Це дозволяє правоохоронним органам або аналітичним підрозділам швидко реагувати на потенційні загрози.

Контекстуальний аналіз текстів є ще одним важливим аспектом. Одна й та ж інформація може мати різні значення залежно від контексту, в якому вона подається. Наприклад, обговорення певної теми в політичному контексті може мати інші наслідки, ніж те ж обговорення в економічному. Тому важливо враховувати контекст, у якому з'являється інформація, щоб правильно оцінити її потенційні загрози.

Важливим аспектом є етичні питання, пов’язані з аналізом текстів. Використання особистої інформації з відкритих джерел може викликати занепокоєння з приводу приватності. Тому необхідно дотримуватися етичних норм і законодавчих вимог при зборі та аналізі текстової інформації. Це включає в себе забезпечення анонімності джерел та уникнення дискримінації на основі отриманих даних.

Крім того, ідентифікація осіб за допомогою аналізу фотографій є однією з найпоширеніших практик у сфері цифрової криміналістики, безпеки та OSINT, що дозволяє швидко ідентифікувати особу серед тисячі інших, зіставляючи біометричні параметри обличчя — відстань між очима, форму носа, підборіддя, контури губ, що особливо важливо для правоохоронних органів та спецслужб.

Фото з камер спостереження, соцмереж або публічних заходів може стати вирішальним доказом того, де востаннє бачили людину. Також цей метод застосовують у гуманітарних місіях для встановлення особи жертв катастроф.

Геолокація за фотографіями є ключовим напрямом OSINT-аналізу, коли потрібно встановити, де саме було зроблено знімок. Це особливо важливо для перевірки достовірності інформації у медіа та під час військових конфліктів та для розслідувань злочинів та терористичних актів. Наприклад, фото зі соцмереж може вказати на точне місце перебування злочинця чи місце зберігання зброї.

Також слід звернути увагу на те, що фото є потужним доказовим матеріалом, який допомагає відтворити перебіг подій. Завдяки зображенням можна зрозуміти, що саме сталося, у який час і за яких обставин та передбачає встановлення деталей: кількість учасників, їхні дії, емоції, наявність техніки чи зброї. Це особливо важливо при дослідженні масових заворушень або військових конфліктів.

Семінарське заняття – 2 години

Учбові питання:

1. Загальна характеристика пошуку та аналізу текстової інформації із засобів масової інформації; інтернет-ресурсів.
2. Загальна характеристика внутрішньовідомчих джерел даних (бази даних; системи інформаційно-аналітичного забезпечення).
3. Загальна характеристика зовнішніх джерел інформації (відомості від центральних органів виконавчої влади держави.
4. Відомості інших правоохоронних органів держави; дані від правоохоронних органів інших держав; відомості із засобів масової інформації; інтернет-ресурси тощо.
5. Характеристика інструментів та методів пошуку інформації з відкритих джерел (OSINT).

Практичні заняття – 6 годин

Завдання до практичного заняття

Вибір об'єкта дослідження: Визначте конкретну організацію або особу, яку ви хочете дослідити. Може бути корисно вибрати об'єкт, який має певний інтерес для аналізу з точки зору безпеки, наприклад, компанію або публічну постать.

Збір відкритих даних: Використовуючи OSINT Framework (Фреймворк OSINT) , виконайте пошук та збір відкритої інформації про обраного об'єкта в Інтернеті. Врахуйте різні джерела, такі як соціальні мережі, новини, форуми, блоги тощо.

Аналіз зібраних даних: Після збору інформації проведіть аналіз даних, щоб виділити ключову інформацію, яка може мати важливе значення для безпеки або оцінки ризиків. Це може включати виявлення можливих загроз, ідентифікацію рекомендацій для покращення безпеки тощо.

Підготовка звіту: Напишіть звіт, в якому представите результати вашого дослідження. Зазначте джерела інформації, висновки та рекомендації щодо подальших заходів з точки зору безпеки.

Презентація результатів: Підготуйте коротку презентацію для представлення вашого дослідження перед групою або викладачем. Поясніть ваші висновки та рекомендації.

Це практичне завдання дозволить вам відпрацювати навички використання OSINT Framework для збору відкритих даних та їх аналізу з точки зору безпеки. Ви зможете виробити здатність знаходити корисну інформацію та робити аналіз її впливу на безпеку та ризики.

Питання для самоконтролю:

1. Використання OSINT для виявлення й обліку загроз для національної безпеки.
2. Застосування Google-карт для визначення маршрутів пересування, аналізу місцевості, моніторингу геолокаційних даних осіб, що серійно вчиняють розбійні напади.
3. Технології застосування пошуку та аналізу текстів з метою пошуку інформації в текстовому форматі, включаючи новини, статті, блоги, форуми та інше для виявлення потенційних загроз чи ризиків в умовах воєнного стану.
4. Які основні аспекти розвитку OSINT-технологій?
5. Яка роль OSINT-технологій в сучасному інформаційному середовищі та як вони можуть покращити діяльність підрозділів кримінальної поліції?
6. Які методи та інструменти для збору інформації з OSINT-джерел вам відомі?

ТЕМА № 5. Проведення пошуку інформації з відкритих джерел (OSINT) в соціальних мережах

Проведення пошуку інформації з відкритих джерел (OSINT) в соціальних мережах (Facebook, Instagram тощо) шляхом аналізу інформації, яку користувачі вказують у персональних профілях, та яка може містити дані про їхні інтереси, місцезнаходження, роботу, освіту. Застосування відео-пошуку з метою виявлення відеоматеріалів про події, моніторинг відеоблогів, аналіз вірусного відео.

Аналіз зв’язків між користувачами соціальних мереж, визначення кола знайомств та спільнот, що може бути корисно при вивченні осіб, які становлять інтерес. Пошук та вивчення публікацій за конкретними хештегами.

Безпечна поведінка при використанні мережі Інтернет.

Методичні рекомендації

При вивченні даної теми необхідно підкреслити, що інтереси є важливим показником, який дозволяє зрозуміти особистість користувача. Соціальні мережі надають простір для вираження своїх захоплень, уподобань у музиці, спорті, літературі чи політиці. Аналіз вподобань дає змогу вибудувати психолого-поведінковий портрет особи. Користувачі часто приєднуються до тематичних груп або підписуються на сторінки брендів, відомих людей, спортивних команд. Це створює інформаційний слід, який відображає систему цінностей та сферу зацікавлень. Для

OSINT-дослідників важливо не лише зафіксувати перелік інтересів, а й зрозуміти, як вони взаємопов'язані. Поєднання кількох інтересів може створювати профіль потенційної приналежності до певних груп чи середовищ. Аналіз інтересів корисний як для розслідувань, так і для маркетингу, безпеки чи психологічних досліджень. Однак слід пам'ятати про етичні обмеження: інформація використовується лише у відкритому доступі.

Необхідно враховувати, що соціальні мережі містять велику кількість даних про професійну діяльність користувачів. У Facebook, LinkedIn та інших платформах часто вказується місце роботи, посада та попередній досвід. Для OSINT-аналітиків така інформація є безцінною: вона дозволяє встановити професійний рівень, коло контактів, можливі компетенції. Це може стати основою для створення профілю особи. Публікації про робочі події, фото з корпоративів чи конференцій надають додаткові підтвердження реального місця роботи. Це особливо корисно для перевірки біографії людини. Важливим є і аналіз колег та ділових зв'язків. Соцмережі дозволяють простежити, з ким взаємодіє користувач у професійному середовищі, які проекти підтримує.

Відеоблоги стали одним із найпопулярніших каналів масової комунікації. Мільйони людей щодня переглядають відео на YouTube, TikTok чи інших платформах. Для OSINT та аналітики моніторинг блогів дає уявлення про настрої суспільства, інформаційні тренди та особистості, які впливають на громадську думку. Аналіз відеоблогів допомагає визначати ключових лідерів думок, їхню аудиторію та рівень впливу. Це може бути корисним як для державних структур (у сфері інформаційної безпеки), так і для приватного бізнесу (маркетингові дослідження). Моніторинг здійснюється за допомогою систем аналітики, які збирають дані про перегляди, коментарі, лайки, поширення. Завдяки цьому можна відслідковувати, які теми викликають найбільший інтерес у суспільстві.

Аналіз зв'язків між користувачами соціальних мереж, визначення кола знайомств та спільнот, що може бути корисно при вивченні осіб, які становлять інтерес - ще одне актуальне питання. Коло знайомств користувача в соціальних мережах часто відображає його реальні соціальні контакти. Аналіз цього кола дозволяє зрозуміти, з ким людина найбільше взаємодіє, кому довіряє та хто впливає на її думку. Зазвичай у соцмережах виділяють три рівні знайомств: найближче коло (родичі, близькі друзі), середнє коло (колеги, однокласники, знайомі), а також віддалене коло (користувачі з мінімальною взаємодією).

Особливої уваги потребує дослідження спільнот. Соціальні мережі дозволяють користувачам вступати у групи, підписуватися на спільноти та брати участь у форумах. Дослідження таких об'єднань надає інформацію про інтереси, погляди та можливу ідеологічну орієнтацію особи. У закритих або тематичних групах користувачі часто діляться інформацією, яку не публікують у відкритому доступі. Це може бути корисним для OSINT-аналізу чи журналістських розслідувань. Вивчення спільнот також дозволяє визначити лідерів думок, яким довіряє користувач. Якщо одна людина має вплив на велику кількість учасників, це робить її ключовою фігурою для аналізу. Аналіз взаємодії у групах показує ступінь активності користувача.

Окрім офіційних «друзів» і «груп», у соцмережах часто існують приховані або неформальні мережі контактів. Їх можна виявити шляхом аналізу взаємодій - коментарів, реакцій, спільних подій. Неформальні мережі важливі, бо вони показують справжні зв'язки між людьми, які не завжди видно через «офіційний список друзів». Наприклад, користувач може бути близько знайомим із людиною, але не мати її у друзях. Для виявлення таких мереж використовуються методи соціальної аналітики, коли відстежується частота взаємодій, час комунікацій і навіть контекст коментарів.

Семінарське заняття – 2 години

Учбові питання:

1. Пошук інформації з відкритих джерел (OSINT) в соціальних мережах (Facebook, Instagram тощо) шляхом аналізу інформації, яку користувачі вказують у персональних профілях, та яка може містити дані про їхні інтереси, місцезнаходження, роботу, освіту.
2. Відео-пошук з метою виявлення відеоматеріалів про події, моніторинг відеоблогів, аналіз вірусного відео.
3. Аналіз зв'язків між користувачами соціальних мереж, визначення кола знайомств та спільнот,

що може бути корисно при вивченні осіб, які становлять інтерес.
4. Пошук та вивчення публікацій за конкретними хештегами.
5. Безпечна поведінка при використанні мережі Інтернет.

Практичні заняття – 6 годин

Завдання до практичного заняття

Ситуаційне завдання 1. Ірину Фаріон було вбито ввечері 19 липня 2024 року неподалік її дому у Львові. Невідомий вистрілив у неї й утік. Попри операцію та зусилля медиків, життя мовознавиці врятувати не вдалося.

Завдання: Використати засоби (OSINT) для установлення фактичних даних, що підлягають доказуванню у матеріалах кримінального провадження.

Ситуаційне завдання 2. Влітку 2008 року з Одеського музею західного та східного мистецтва викрали картину Караваджо «Взяття Христа під варту», або «Поцілунок Іуди». Грабіжники вночі через вікно залізли в зал і вирізали картину з рами.

Завдання**:** Використати засоби (OSINT) для установлення фактичних даних, що підлягають доказуванню у матеріалах кримінального провадження.

Ситуаційне завдання 3. Громадського діяча з Одеси Дем'яна Ганула вбили вранці 14 березня у центрі Одеси. У нього здійснили кілька пострілів, він загинув на місці. Момент вбивства та людина, яка стріляла в активіста, потрапили на камери відеоспостереження.

Завдання: Використати засоби (OSINT) для установлення фактичних даних, що підлягають доказуванню у матеріалах кримінального провадження.

Питання для самоконтролю:

1. Визначте структуру та наповнення соціальних мереж як джерела інформації для OSINT-досліджень.
2. Які данні можна зібрати з профілів користувачів у соціальних мережах без порушення політики конфіденційності?
3. Вкажіть переваги та недоліки використання відкритих профілів під час OSINT-аналізу.
4. Перелічіть інструменти та сервіси які дозволяють автоматизувати збір інформації з Facebook, Instagram, X (Twitter), TikTok чи інших соцмереж.
5. Як здійснюється пошук та виявлення прихованих або непрямих зв'язків між користувачами?
6. Верифікація отриманої з соціальних мереж інформації та встановлення її достовірності.
7. Які ознаки можуть свідчити про фейковість акаунта в соціальній мережі?
8. Вкажіть ризики та правові обмеження під час збору інформації з соціальних мереж.

ТЕМА № 6. Напрямки використання пошукової інформації з відкритих джерел (OSINT) працівниками кримінальної поліції

Семінарське заняття – 2 години

Складання звітів та використання результатів пошуку інформації з відкритих джерел (OSINT) під час виконання завдань оперативно-розшукової діяльності та кримінального судочинства.

Пошук підозрюваних, установлення їх зв'язків та місцезнаходження за допомогою соціальних мереж, відкритих баз даних та інших відкритих джерел.

Здійснення моніторингу оперативної обстановки або стану криміногенної ситуації як напрям використання пошуку інформації з відкритих джерел (OSINT) у правоохоронній діяльності. Виявлення загроз публічній безпеці. Підтримка оперативно-розшукової та кримінальної процесуальної діяльності; збір інформації про можливих злочинців, їхні зв'язки та місцезнаходження тощо.

Методичні рекомендації

При розгляді даної теми ми акцентуємо увагу, що пошук підозрюваних у соціальних мережах базується на методах OSINT, що передбачають системний збір, аналіз та узагальнення інформації з відкритих джерел. У цьому контексті використовуються як прямі дані - ім'я, нікнейми, контактні телефони, електронна пошта, так і непрямі - стиль мовлення, звички, коло

інтересів. Завдяки цьому можливо ідентифікувати людину навіть за умов використання нею анонімних акаунтів. Значною перевагою є можливість автоматизації пошукових процесів. Існують спеціальні програми та алгоритми, які дозволяють відстежувати активність підозрюваних у режимі реального часу, аналізувати геолокаційні дані, взаємодії з іншими користувачами та навіть прогнозувати ймовірні дії. Такі інструменти суттєво підвищують ефективність оперативно-розшукових заходів. Не менш важливим є залучення інформації від адміністрацій соціальних платформ, які за офіційними запитами можуть надати додаткові відомості: історію входів у профіль, IP-адреси, прив'язку акаунта до номерів телефону. Такі дані дозволяють не лише підтвердити особу, а й встановити її цифровий слід.

Актуальним напрямком є установлення зв'язків підозрюваних через відкриті дані. Використання відкритих реєстрів (державних чи комерційних) розширює можливості встановлення офіційних і прихованих зв'язків. Наприклад, за допомогою баз даних про реєстрацію транспортних засобів чи підприємств можна виявити, що підозрюваний має спільну власність або бізнес із іншими особами. Це дає підстави для висунення версій про їхню співучасть у злочинах. Сучасні методи аналізу включають створення соціограм - графічних моделей, що відображають взаємозв'язки між людьми. Такий підхід дозволяє визначити структуру злочинної групи, виділити ключових учасників та їхні ролі. Важливо, що інструменти кримінального аналізу дають можливість відслідковувати навіть непрямі зв'язки, які не завжди помітні при звичайному перегляді профілів у соціальних мережах.

Також важливим напрямком є встанолення місцезнаходження підозрюваних. Важливим джерелом інформації виступають метадані цифрових файлів. Фотографії, зроблені смартфоном, можуть містити дані про координати зйомки, дату та час. Це дозволяє відтворити маршрут пересування підозрюваного або підтвердити його присутність у певному місці.

Не менш цінними є відкриті бази даних, що містять відомості про зареєстроване житло, автомобілі чи офіційні документи. Вони допомагають виявити адреси проживання, місця роботи чи навчання, що у поєднанні з даними із соціальних мереж створює повну картину можливого місця знаходження особи. Значну увагу приділяють і аналізу активності в Інтернеті: час публікацій, використання мови, коментарі на локальні теми, фотографії з характерними об'єктами на фоні. Це дозволяє не лише визначити країну чи місто перебування, але й конкретний район.

Моніторинг оперативної обстановки передбачає безперервний збір та аналіз інформації про події, які можуть становити загрозу публічній безпеці або свідчити про зростання злочинної активності в певному регіоні. Наприклад, повідомлення у соціальних мережах про конфлікти, насильницькі дії чи підозрілу поведінку осіб можуть сигналізувати про ймовірні правопорушення. Завдяки OSINT оперативні підрозділи отримують можливість відслідковувати тенденції та локалізувати «гарячі точки» у режимі реального часу.

Процес моніторингу включає кілька етапів: пошук релевантних повідомлень, їх перевірку, аналітичну обробку та представлення у вигляді звітів чи інформаційних довідок. Для цього активно використовуються автоматизовані системи збору інформації, спеціалізовані пошукові інструменти та аналітичні платформи, які дозволяють швидко відсівати незначимі дані та концентрувати увагу на тих, що становлять оперативний інтерес.

Результати моніторингу оперативної обстановки можуть використовуватися як у повсякденній роботі патрульних та слідчих, так і у стратегічному плануванні діяльності органів правопорядку. Вони допомагають визначати пріоритетні напрями оперативно-розшукової діяльності, розподіляти сили та засоби, своєчасно реагувати на зміни криміногенної ситуації. У судовій практиці така інформація здатна стати додатковим аналітичним підтвердженням при оцінці загального рівня загроз безпеці громадян.

У контексті правоохоронної діяльності, OSINT дозволяє:

– відстеження публікацій, коментарів, фото та відео, які можуть містити інформацію про злочинну діяльність, заплановані акції, або осіб, що становлять інтерес для правоохоронних органів;

– виявлення повідомлень про злочини, надзвичайні події, або інші події, які можуть мати криміногенні наслідки;

– моніторинг онлайнових спільнот, де можуть обговорюватися злочинні плани, відбуватися торги забороненими товарами, або поширюватися дезінформація;

– отримання інформації про осіб, що становлять інтерес для правоохоронних органів, з відкритих баз даних, реєстрів, соціальних мереж та інших джерел;

– виявлення потенційних загроз, зон підвищеного ризику, або тенденцій у злочинності.

Одним із ключових аспектів виявлення загроз публічній безпеці є використання інформаційно-аналітичних систем та відкритих джерел даних (OSINT). Соціальні мережі, інтернет-форуми, публічні реєстри й медіа-платформи виступають важливими джерелами для моніторингу криміногенної ситуації. Аналіз поведінки користувачів у мережі може сигналізувати про радикалізацію, підготовку до масових безпорядків чи інших деструктивних дій. Значну роль відіграють і спеціальні технічні засоби спостереження, включно з відео-аналітикою та системами розпізнавання обличчя. Вони дають змогу ідентифікувати підозрілих осіб у місцях масового скупчення людей, своєчасно виявляти порушення громадського порядку та реагувати на них. Поєднання цих технологій із базами даних правоохоронних органів дозволяє оперативно перевіряти осіб на предмет причетності до злочинів.

Важливим елементом є аналіз соціально-економічних, політичних та кримінальних чинників, що впливають на загальний рівень безпеки. Дослідження тенденцій у сфері злочинності, рівня соціальної напруги, поширення наркотичних засобів чи нелегальної зброї допомагає прогнозувати можливі загрози. Таким чином, виявлення небезпек має комплексний характер і включає як мікро-, так і макрорівень аналізу.

Особливу увагу правоохоронні органи приділяють попередженню терористичних загроз та екстремістської діяльності. Своєчасне виявлення осередків радикальних груп, їхніх каналів комунікації та фінансування дозволяє запобігти масштабним загрозам для публічної безпеки. У цьому контексті тісна міжнародна співпраця є надзвичайно важливою, адже сучасні виклики не мають кордонів.

Перед тим, як здійснити будь-який пошук в Інтернеті, треба подбати про захист персональної інформації та пристрою під час роботи в мережі. Це можна забезпечити завдяки використанню VPN та «замаскуванню» власної персони через створення віртуальної PERSONA. VPN (віртуальна приватна мережа) – узагальнена назва мереж, що створюються поверх інших мереж, які мають менший рівень довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі і користуватись її сервісами: внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет.

Технологія VPN дає змогу об’єднати декілька географічно віддалених мереж (або окремих клієнтів) у єдину мережу з використанням для зв’язку між ними непідконтрольних каналів. Багато провайдерів пропонують свої послуги як з організації VPN-мереж для бізнес-клієнтів, так і для виходу в мережу Інтернет. VPN є клієнт-серверною технологією.

Оперативно-розшукова діяльність (ОРД) є важливим елементом забезпечення національної безпеки та правопорядку, оскільки вона спрямована на попередження, виявлення та розкриття злочинів. У сучасних умовах розвитку інформаційних технологій суттєво зростає роль відкритих джерел інформації (OSINT) у підтримці цієї діяльності. Соціальні мережі, інтернет-ресурси, публічні реєстри та електронні бази даних стають невід’ємними інструментами у роботі оперативних підрозділів.

Інформація з відкритих джерел часто використовується для верифікації оперативних відомостей, отриманих у ході негласних заходів. Наприклад, дані агентури або перехоплені комунікації можуть підтверджуватися фактами з соціальних мереж чи баз реєстрації підприємств. Це підвищує точність та об’єктивність слідчих дій.

Важливим аспектом є підтримка кримінальної процесуальної діяльності. Дані з відкритих джерел можуть застосовуватися для формування доказової бази, підтвердження алібі чи, навпаки, викриття неправдивих показів підозрюваних. При цьому важливо правильно процесуально закріплювати таку інформацію, аби вона мала юридичну силу у судовому провадженні.

Соціальні мережі дозволяють отримати відомості про поведінку підозрюваних, їхні інтереси, місця відпочинку та проживання. Багато користувачів публікують фотографії та геотеги, що прямо чи опосередковано вказують на їхнє місцезнаходження. Це робить соціальні платформи одним із найефективніших джерел для збору відомостей.

Не менш важливим напрямом є встановлення кола контактів підозрюваних. Через аналіз друзів, підписників, коментарів і груп можна сформувати соціограму, яка відображає структуру зв'язків особи. Такий підхід дає можливість виділити не лише безпосередніх співучасників, а й опосередкованих партнерів чи посередників.

Суттєве значення має й аналіз цифрових слідів. До них належать IP-адреси, електронні пошти, контактні телефони, які можна співставляти для встановлення реальної особи. Навіть за умов використання фейкових акаунтів чи підроблених даних можливо ідентифікувати людину за стилем спілкування, часовою активністю чи повторюваними діями.

Оперативні підрозділи активно застосовують програмні засоби для автоматизованого збору та аналізу великих масивів даних. Такі системи дозволяють створювати аналітичні моделі, що визначають рівень ризику, прогнозують ймовірні дії підозрюваних та допомагають планувати подальші слідчі заходи.

На *самостійну підготовку* технології виносяться питання щодо визначення тенденцій, які можуть вказувати на зростання або зміну закономірностей у кримінальному світі. Також додаткового розгляду потребує питання щодо реалізації відповідної управлінської функції керівниками правоохоронних органів щодо використання наявних ресурсів (сили, засоби, технічні можливості, особовий склад, негласне співробітництво тощо). . Форма педагогічного контролю – усне опитування під час проведення семінарських та практичних занять.

Семінарське заняття – 2 години

Учбові питання:

1. Правила складання звітів та використання результатів пошуку інформації з відкритих джерел (OSINT) під час виконання завдань оперативно-розшукової діяльності та кримінального судочинства.
2. Особливості пошуку підозрюваних, установлення їх зв'язків та місцезнаходження за допомогою соціальних мереж, відкритих баз даних та інших відкритих джерел.
3. Моніторинг оперативної обстановки або стану криміногенної ситуації як напрям використання пошуку інформації з відкритих джерел (OSINT) у правоохоронній діяльності.
4. Виявлення загроз публічній безпеці.

Практичне заняття – 4 години

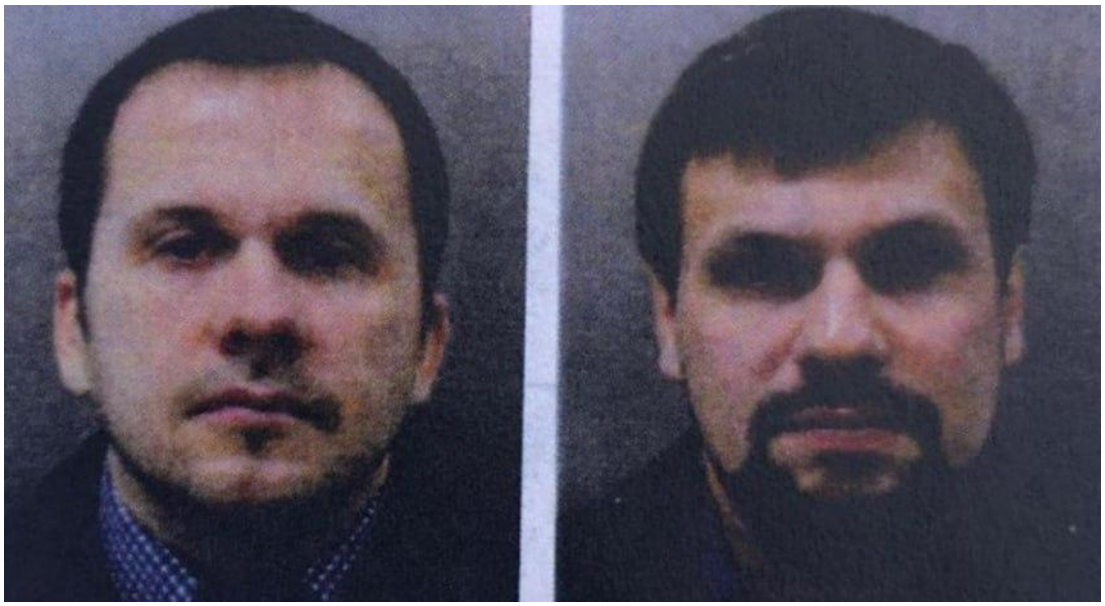
Завдання до практичного заняття

Ситуаційне завдання 1.

У парку було виявлено труп чоловічої статі на лівій руці якого було татуювання у вигляді троянди, яка проткнута кинджалом.

Завдання: Використати засоби (OSINT) для установлення фактичних даних, що підлягають доказуванню у матеріалах кримінального провадження.

Ситуаційне завдання 2.



Завдання: Використати засоби (OSINT) для встановлення причетності зазначених осіб до вчинення кримінальних злочинів

Питання для самоконтролю:

1. Сутність використання OSINT у діяльності працівників кримінальної поліції
2. Основні напрями застосування OCINT у процесі документування злочинної діяльності
3. Складання звітів та використання результатів пошуку інформації з відкритих джерел (OSINT) під час виконання завдань оперативно- розшукової діяльності та кримінального судочинства.
4. Засоби пошуку підозрюваних, установлення їх зв'язків та місцезнаходження за допомогою соціальних мереж, відкритих баз даних та інших відкритих джерел.
5. Моніторинг оперативної обстановки або стану криміногенної ситуації як напрям використання пошуку інформації з відкритих джерел (OSINT) у правоохоронній діяльності.
6. OSINT як інструмент зв'язків між фігурантами кримінального провадження.
7. Роль соціальних мереж у зборі розвідувальної інформації для оперативно-розшукової діяльності.
8. OSINT як інструмент для ідентифікації місцезнаходження розшукуваних осіб.
9. Використання OSINT для прогнозування злочинної активності та оцінки ризиків
10. Правові та етичні обмеження під час збору та використання пошукової інформації з відкритих джерел.

4. ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ ОСВІТНЬОЇ ДІЯЛЬНОСТІ

Система оцінювання передбачає накопичення 100 балів з кожної навчальної дисципліни, які перераховуються в національну шкалу та шкалу оцінювання ЄКТС.

Оцінювання результатів вивчення навчальної дисципліни у формі заліку.

Підсумковий контроль у формі заліку проводиться після проведення всіх видів занять передбачених робочою навчальною програмою відповідної освітньої компоненти.

Оцінювання здійснюється за результатами накопичених балів з аудиторної та самостійної робіт.

Результати навчання з аудиторної роботи обчислюються за таким алгоритмом:

– результат аудиторної роботи визначається, як середній бал помножений на коефіцієнт 16 та заокруглюється до цілого балу за математичними правилами (до 0,5 включно – до попереднього цілого числа, 0,5 і більше – до наступного цілого числа);

– середній бал дорівнює сумі усіх одержаних позитивних оцінок (балів) поділених на відповідну кількість, при цьому:

а. мінімальна кількість оцінок має складати не менше 1/3 (33 %) від загальної можливої кількості занять (семінарських, практичних, лабораторних) передбачених робочою навчальною програмою навчальної дисципліни. Якщо 1/3 (33 %) від кількості занять складає дробове число, то до розрахунку береться наступне ціле число;

б. якщо кількість отриманих оцінок менша за 1/3 (33 %), то кожна недостаюча оцінка враховується, як «нуль» балів;

в. кількість позитивних оцінок, які перевищують визначену мінімально-допустиму («додаткових») враховуються з коефіцієнтом 0,7, такий коефіцієнт застосовується з метою мотивування здобувачів вищої освіти до покращення результатів оцінювання за аудиторну роботу;

г. невідпрацьовані «незадовільні» оцінки та пропущені заняття враховуються як «нуль» балів;

д. відпрацювання усіх «незадовільних» оцінок та пропущених занять не є обов'язковим.

У випадку, якщо за результатами оцінювання аудиторної роботи сума накопичувальних балів перевищує 80, то здобувачу вищої освіти нараховується максимально допустимий результат – 80 балів.

Формула розрахунку:

$$РАР = \frac{СОБ}{МКО + КДО*0,7+КНО} * 16$$

де:

- РАР – результат аудиторної роботи;
- СОБ – сума отриманих оцінок у балах;
- МКО – мінімальна кількість оцінок (1/3 (33 %) від кількості семінарських, практичних, лабораторних занять передбачених робочою навчальною програмою навчальної дисципліни). При цьому, якщо МКО складає дробове число, то до розрахунку береться наступне ціле число;
- КДО – кількість «додаткових» оцінок – оцінок, що перевищують МКО;
- КНО – кількість невідпрацьованих «незадовільних» оцінок та невідпрацьованих пропущених занять.

Загальна кількість балів за самостійну роботу визначається, як сума отриманих балів за виконання видів робіт, передбачених робочою навчальною програмою навчальної дисципліни.

Підсумкова кількість балів отриманих під час складання заліку визначається, як сума отриманих балів за аудиторну (максимум 80 балів) та самостійну роботу (максимум 20 балів).

Поточний контроль		**Підсумковий контроль**
Аудиторна робота (РАР) (семінарські/практичні заняття та контрольні заходи)	Самостійна робота (РСР)	ЗАЛІК (З)
≤ 80	≤20	
≤ 100		
Підсумкова кількість балів = РАР+РСР ≤ 100		

У разі, якщо здобувач вищої освіти під час складання заліку отримав менше 60 балів – «не зараховано» він ліквідовує академічну заборгованість за окремим графіком на вище визначених умовах.

Такий здобувач повинен покращити результати поточного контролю (відпрацювати пропущені заняття та/або незадовільні оцінки, відпрацювати тему для одержання оцінки, виконати самостійну роботу тощо) до моменту ліквідації академічної заборгованості.

У разі повторного не складання заліку ліквідація академічної заборгованості здійснюється перед комісією без врахування результатів навчання отриманих за результатами аудиторної та самостійної роботи за 100 бальною шкалою. При ліквідації академічної заборгованості перед комісією здобувач вищої освіти може одержати не більше 74 балів.

Шкала оцінювання: національна та ECTS

За внутрішньою шкалою закладу вищої освіти в балах	**За шкалою ECTS /За національною шкалою**	
	Вноситься до відомості	
	екзамен	залік
90 – 100	A/Відмінно	A,B,C,D,E/Зараховано
82-89	B/Добре	
75-81	C/Добре	
64-74	D/Задовільно	
60-63	E/Задовільно	
35-59	FX/Незадовільно	FX/Не зараховано
	з можливістю повторного складання	
0-34	F/Незадовільно	F/Не зараховано
	з обов'язковим повторним вивченням курсу	

Критерії оцінювання знань на заліку

Оцінка «зараховано» / A, B, C, D, E – виставляється, якщо здобувач вищої освіти виявив достатньо повні знання матеріалу навчальної дисципліни; вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями, дає правильні, хоча і не завжди повні відповіді на поставлені запитання; припускається помилок у розкритті окремих теоретичних положень, норм та визначень.

Оцінка «не зараховано»/ FX,F – виставляється, якщо здобувач вищої освіти виявив слабкі знання; не зміг дати визначення основних термінів та понять; викладає матеріал непослідовно, нелогічно, фрагментарно, неточно, стисло; відсутня переконливість у викладенні матеріалу.

5. ПИТАННЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Загальна характеристика поняття пошуку інформації з відкритих джерел (OSINT).
2. Визначення основних завдань пошуку інформації з відкритих джерел (OSINT).
3. Роль пошуку інформації з відкритих джерел (OSINT) у діяльності правоохоронних органів.
4. Характеристика історичних етапів виникнення, становлення та розвитку пошуку інформації з відкритих джерел (OSINT).
5. Характеристика стану розвідки з відкрити джерел на початку XX століття.
6. Характеристика методів збору відкритої інформації під час другої світової війни та холодної війни.
7. Особливості діяльності з пошуку відкритої інформації у середині XX століття.
8. Основні ознаки пошуку інформації з відкритих джерел (OSINT) з кінця XX століття до теперішнього часу.
9. Нормативно-правове забезпечення та юридичні підстави застосування пошуку інформації з відкритих джерел (OSINT).
10. Правові підстави та особливості здійснення пошуку інформації з відкритих джерел (OSINT) правоохоронними органами України.
11. Умови та межі застосування пошуку інформації з відкритих джерел (OSINT) співробітниками правоохоронних органів.
12. Сутність інформації, види джерел інформації, специфіка її передавання та принципи управління інформацією.
13. Етичні вимоги щодо здійснення пошуку інформації з відкритих джерел.
14. Визначення цінності елементів інформації з точки зору достовірності, надійності, відповідності та точності.
15. Висновок про релевантність для досліджуваного феномену.

16. Мета оцінки інформації.
17. Критерії оцінки інформації.
18. Оцінки (градації) достовірності джерела походження інформації та достовірності інформації.
19. Уніфіковані (міжнародні) стандарти і норми у сфері оцінки достовірності джерел інформації та змісту інформації (4×4), (5×5×5), (6×6).
20. Класифікація джерел інформації.
21. Загальна характеристика відкритих (доступних для загального користування) джерел інформації.
22. Загальна характеристика відомостей інших правоохоронних органів держави; дані від правоохоронних органів інших держав; відомості із засобів масової інформації; інтернет-ресурси тощо джерел інформації.
23. Загальна характеристика внутрішньовідомчих джерел даних (бази даних; системи інформаційно-аналітичного забезпечення).
24. Загальна характеристика зовнішніх джерел інформації (відомості від центральних органів виконавчої влади держави;).
25. Характеристика інструментів та методів пошуку інформації з відкритих джерел (OSINT).
26. Використання інформаційно-пошукових систем для здійснення загального пошуку інформації в мережі інтернет.
27. Використання інформаційно-пошукових систем для пошуку конкретних осіб та організацій (про конкретні особи, їхні профілі в соціальних мережах, біографічні дані, новини, пов'язані з ними, коло спілкування, місця перебування, спосіб життя).
28. Використання інформаційно-пошукових систем для моніторингу відомостей із ЗМІ (відстеження новин, статей та інших матеріалів з різних джерел для оновлення інформації про поточні тенденції).
29. Використання інформаційно-пошукових систем для виявлення фото, відео та інших медіа файлів відносно осіб, які становлять інтерес.
30. Використання інформаційно-пошукових систем для інформаційного супроводу правоохоронної діяльності.
31. Особливості застосування пошуку та аналізу текстів з метою пошуку інформації в текстовому форматі, включаючи новини, статті, блоги, форуми та інше для виявлення потенційних загроз чи ризиків.
32. Особливості застосування пошуку та аналізу фото (зображень) з метою ідентифікації осіб, визначення локацій, виявлення вірусних фотографій, аналізу подій тощо.
33. Особливості застосування відео пошуку з метою виявлення відеоматеріалів про події, моніторинг відеоблогів, аналіз вірусного відео.
34. Особливості застосування Google-карт для визначення маршрутів пересування, аналізу місцевості, моніторингу геолокаційних даних.
35. Проведення пошуку інформації з відкритих джерел (OSINT) в соціальних мережах (Facebook, Instagram тощо) шляхом аналізу інформації, яку користувачі вказують у персональних профілях та яка може містити дані про їхні інтереси, місцезнаходження, роботу, освіту.
36. Слідкування за публікаціями, коментарями та іншою активністю користувачів соціальних мереж для отримання розуміння про їхні дії та наміри, інтереси та взаємодію з іншими користувачами соціальних мереж.
37. Аналіз зв'язків між користувачами соціальних мереж, визначення кола знайомств та спільнот, що може бути корисно при вивченні осіб, які становлять інтерес.
38. Пошук та вивчення публікацій за конкретними хештегами, що дозволяє виявити тренди та теми обговорення.
39. Підготовка аналітичного звіту.
40. Основні правила складання аналітичних звітів.
41. Найпоширеніші помилки при складанні аналітичного звіту.
42. Репрезентування результатів аналітичного дослідження.
43. Пошук підозрюваних, установлення їх зв'язків та місцезнаходження за допомогою

соціальних мереж, відкритих баз даних та інших відкритих джерел.
44. Здійснення моніторингу оперативної обстановки або стану криміногенної ситуації як напрям використання пошуку інформації з відкритих джерел (OSINT) у правоохоронній діяльності.
45. Застосування пошуку інформації з відкритих джерел (OSINT) для здійснення упереджувальних (превентивних правоохоронних дій.
46. Виявлення загроз публічній безпеці.
47. Підтримка оперативно-розшукової та кримінальної процесуальної діяльності, зокрема, збір інформації про можливих злочинців, їхні зв'язки та місцезнаходження тощо.
48. Визначення тенденцій, які можуть вказувати на зростання або зміну закономірностей у кримінальному світі.
49. Використання інструментарію (OSINT) для виявлення тяжких злочинів у сфері незаконного обігу наркотичних засобів, торгівлі людьми, екологічних, міжнародних воєнних злочинів, розшуку безвісно зниклих та підозрюваних та оголошених в розшук осіб.
50. Взаємодія з Європолом при використанні інструментарію (OSINT).

ГЛОСАРІЙ

– А –

АБСТРАГУВАННЯ *(лат. abstrahere - відволікати)* – 1. Смислова операція, філософський і логічний метод «відволікання», який дає змогу переходити від конкретних предметів до загальних понять і законів розвитку. 2. Метод оперативного мислення, сутність якого полягає у виділенні та формуванні основного змісту інформації про оперативне явище шляхом відкидання його несуттєвих, другорядних ознак та виокремлення істотних ознак.

АЛГОРИТМ *(араб. аль-Хорезмі – ім'я середньовічного узбецького математика)* **–** система правил виконання обчислювального процесу, що призводить до розв'язання певного класу задач після скінченого числа операцій.

АЛГОРИТМ ВИЗНАЧЕННЯ ГІПОТЕЗ ТА ВИСНОВКІВ (ПРОПОЗИЦІЙ) – система операцій, що здійснюються за строго визначеними правилами і після послідовного їх виконання приводять до вирішення поставленого завдання.

АЛЬТЕРНАТИВА *(франц. alternative и лат. alter - один з двох)* – необхідність вибору між можливостями, що виключають одна одну.

АНАЛІЗ *(грец. analysis – розкладання)* – 1. Метод наукового дослідження предметів, явищ та ін. шляхом розчленування їх (у думці або фактично) на складові частини. 2. Усебічний розгляд, дослідження чого-небудь (фактів, явищ); визначення складу й властивостей якоїсь речовини.

АНАЛІЗ АВС – це простий, якщо йдеться про проведення, метод встановлення точок тяжіння та пріоритетів. Метою цього аналізу є виявлення зв'язків між затратами засобів та досягненням цілей і зосередження дій в тих сферах, які мають найбільше значення.

АНАЛІЗ ЗАГРОЗ – процес, у ході якого інформація про реальну чи потенційну загрози систематично і ретельно перевіряється і аналізується та корегується з метою виявлення значимих фактів і отримання висновків з них.

АНАЛІЗ ЗВ'ЯЗКІВ АБО АНАЛІЗ ПОСИЛАНЬ - це метод аналізу даних, який використовується в рамках мережевого аналізу для оцінки відносин (зв'язків) між вузлами (об'єктами). Відносини можуть бути визначені для різних типів вузлів: людей, організацій, операцій і т. д. Термін «аналіз взаємозв'язків» визначає процес аналізу сукупності взаємовідносин між різними об'єктами мережі для виявлення її характеристик.

АНАЛІЗ ІНФОРМАЦІЇ – процес обробки інформації, який базується на логічному та креативному мисленні, спрямований на одержання якісно нової інформації у вигляді гіпотез, висновків, припущень, ситуативних картин тощо.

АНАЛІЗ ІМПЛЕМЕНТАЦІЇ – етап стратегічного аналізу правоохоронної сфери, який передбачає ідентифікацію можливих обставин, що сприяють або перешкоджають реалізації прийнятої правоохоронним суб'єктом стратегії.

АНАЛІЗ РИЗИКІВ – інформаційно-аналітична діяльність, яка включає оцінку загроз, вразливості публічної безпеки і порядку, охорони прав і свобод людини, концепції протидії злочинності або правоохоронної системи та рівня негативного впливу на них, порівняння результатів оцінки та дослідження взаємозв'язків між ними з метою розробки пропозицій з підвищення рівня безпеки.

АНАЛІТИК *(грец. analytikos – аналітичний)* – 1. Фахівець, що володіє необхідними знаннями та досвідом аналізу управлінських ситуацій, підготовки аналітичних звітів, висновків та пропозицій. 2. Посадова особа підрозділу кримінального аналізу (кримінального аналізу та оперативного моніторингу).

АНАЛІТИЧНИЙ ДАЙДЖЕСТ – це періодичний огляд подій, який представляє собою вижимки подій за певний період з певної тематики у вигляді фрагментів текстів документів (цитати, витяги) та який знаходиться у сфері інтересів реальних або потенціальних замовників аналітичної діяльності.

АНАЛІТИЧНА ДІЯЛЬНІСТЬ – це інтелектуальна творча діяльність, спрямована на одержання та використання нових знань, що здійснюється із застосуванням наукових методів на основі процесу судження від конкретного до загального.

АНАЛІТИЧНІ ДОКУМЕНТИ (довідки, інформаційні зведення, аналітичні огляди) – аналітичні продукти, які готуються в залежності поставлених завдань та об'ємів інформації за усіма напрямами діяльності підрозділу.

АНАЛІТИЧНА КОМП'ЮТЕРНА МОДЕЛЬ – математична модель, що оперує нечисловими алгоритмами і реалізована на електронно-обчислювальній машині*;* інструмент*,* що використовується для оцінки працездатності системи фізичного захисту; розраховує ймовірність переривання послідовності дій правопорушника, виходячи з аналізу взаємодії факторів виявлення, затримки, реагування і встановлення зв'язку.

АНАЛІТИЧНА РОБОТА – підбір, узагальнення й аналіз (логічне дослідження) накопиченої інформації і підготовка на цій основі висновків, прогнозів і пропозицій для опрацювання аналітичних оглядів і прийняття рішень.

АНАЛІТИЧНА ТЕХНІКА – сукупність засобів, способів і прийомів, які використовуються у процесі аналізу й забезпечують досягнення та оформлення як окремих поточних результатів, так і здійснення аналізу в цілому. До аналітичної техніки відносять: статистичні зведення, карти, описи, письмові звіти, графіки (діаграми) зв'язків, руху товарів, подій, діяльності, переліки (зведення) прихованих (не оприлюднених) прибутків, систематичний пошук баз даних, перегляд звітів та повідомлень, порівняння збігів отриманих даних, визначення правдоподібності даних та збігів тощо.

АНАЛІТИЧНЕ ДОСЛІДЖЕННЯ – форма інформаційно-аналітичної діяльності, що полягає у найбільш поглибленому вивченні проблеми, під час якого здійснюється опис її структури, кількісних та якісних параметрів, а також чинники, що їх обумовлюють.

АНАЛІТИЧНИЙ ПРОДУКТ – це формалізовано-творчий результат роботи аналітика, який вміщує дані або знання, які встановлені під час проведення кримінального аналізу і, який в залежності від виду, може містити опис матеріалів, на основі якого виконано аналітичну діяльність, її перебіг, сформульований на основі засновків (передумов) умовивід (висновок), а також рекомендації. Для полегшення розуміння запропонованих висновків і рекомендацій у подальшому можуть додаватися схеми, діаграми і таблиці.

АНАЛІТИЧНА ЗАПИСКА – це детальний аналіз проблеми, висновки та у разі потреби практичні рекомендації. Іноді аналітична записка може бути підготовлена у формі ризиків – специфічного аналізу (в основному, короткострокового) основних загроз розвитку геокриміногенної ситуації.

АНАЛІТИЧНИЙ ЗВІТ – це аналітичний продукт, що містить обґрунтовані відповіді на запитання, поставлені замовником аналізу, які стали предметом аналітичного дослідження, та/або результати оцінки ризиків та загроз безпеки та свободи громадян, пропозиції щодо їх мінімізації та усунення.

АНАЛІТИЧНИЙ ПОШУК – планомірна цілеспрямована відповідна здійсненню оперативно-розшукових заходів, впорядкована за часом і регламентована законодавчими та іншими правовими актами сукупність етапів добування та подальшого аналізу за допомогою певних методик оперативних даних, що зафіксовані на матеріальних носіях.

АНАЛІТИЧНИЙ ОГЛЯД – це вторинний синтезований текст, в якому подано зведену характеристику певного питання чи проблеми, що базується на використанні інформації, отриманої з ряду першоджерел за певний проміжок часу.

АНАЛІТИЧНИЙ ПРОГНОЗ – містить аналіз інформації, яка відображає характер змін стану досліджуваного об'єкта (його структури, найважливіших показників і чинників, що визначають його розвиток), з метою виявлення закономірностей розвитку об'єкта, необхідних для проведення робіт з прогнозування.

АСОЦІАТИВНІ – дозволяють знаходити закономірності між пов'язаними подіями. Прикладом такої закономірності служить правило, яке вказує, що з події XX слід подія YY з певною ймовірністю. Встановлення таких залежностей дає можливість знаходити дуже прості і інтуїтивно зрозумілі правила.

– Б –

БАЗА ДАНИХ – сукупність даних, організованих за визначеними правилами, що передбачає загальні принципи опису, збереження і маніпулювання даними, незалежно від прикладних програм. В загальному випадку база даних містить схеми, таблиці, подання, збережені процедури та інші об'єкти.

БАЗА СТРАТЕГІЧНИХ ДАНИХ (БСД) – це стислий системний опис найсуттєвіших стратегічних елементів, що належать до зовнішнього середовища підприємства; вона (БСД) використовується для оцінки поточного становища, застосовується для визначення прояву процесів у майбутньому та для прийняття стратегічних рішень.

БЕЗПОСЕРЕДНІ ЗВ'ЯЗКИ – взаємовідношення предметів, явищ, процесів, їх властивостей без проміжних ланок.

– В –

ВЕРСІЯ – 1. Один із кількох різних переказів, викладів або одне з тлумачень якогось факту, події. 2. У слідчій та судовій діяльності – обґрунтоване припущення стосовно подій та окремих її обставин, які розслідуються, що пояснює їх походження і характер.

ВЗАЄМОЗВ'ЯЗОК – категорія, що відображає взаємовідношення та взаємодію предметів, явищ та процесів в їх розвитку, виникненні та зникненні.

ВИЗНАЧЕННЯ ПРІОРИТЕТІВ – сортування зібраної інформації та її організація залежно від важливості та актуальності.

ВИСНОВОК – логічний підсумок результатів аналітичного дослідження, зробленого на основі аналізу, певних фактів, даних, інформації тощо.

ВІЗУАЛІЗАЦІЯ *(від лат. Visualis)* **–** загальна назва прийомів уявлення числової інформації або фізичного явища у вигляді, зручному для зорового спостереження та аналізу.

– Г –

ГЕОГРАФІЧНІ ІНФОРМАЦІЙНІ СИСТЕМИ (ГІС) – це набір комп'ютерних інструментів, які дозволяють людині модифікувати, візуалізувати, запитувати та аналізувати географічні й табличні дані. ГІС-системи є потужним інструментом програмного забезпечення і дозволяють аналітикам кримінальної розвідки створювати все що завгодно, від простих пін-карт до тривимірної візуалізації просторових або тимчасових даних.

ГРАФІК – 1. Зображення за допомогою ліній різних моментів якогось процесу в їхній залежності. 2. План роботи з точними показниками норм і часу її виконання.

– Д –

ДАЙДЖЕСТ (англ. Digest- стислий виклад, резюме) – це документ, що становить добірку витягів із конкретного тексту, відібраних і згрупованих таким чином, щоб дати про нього загальне уявлення, чи добірку найцікавіших матеріалів, передрукованих з інших видань.

ДАНІ – факти або відомості, подані у формалізованому вигляді (наприклад, електронний або друкований документ), що забезпечує можливість їх зберігання, обробки та передачі.

ДЕКОМПОЗИЦІЯ – це метод аналітичного характеру, який дозволяє досліджувати процеси і явища, завдяки якому фахівці розбивають мету на кілька невеликих під задач, рішення яких призводить до очікуваного результату.

ДІАГРАМА ВЗАЄМОЗВ'ЯЗКІВ *(друга назва: релятивна, або асоціативна діаграма)* – техніка, за допомогою якої графічно, у впорядкований спосіб, можна представити інформацію на тему взаємовідносин між особами і організаціями. Діаграма взаємозв'язків придатна для визначення організаційної структури групи, оточення даної особи, її контактів, а також для пізнання механізмів керування даної групи.

ДІАГРАМА ДІЯЛЬНОСТІ – блок-схема, яка показує, як потік управління переходить від однієї діяльності до іншої, при цьому увага фіксується на результаті діяльності.

ДІАГРАМА ПОДІЙ – є більш загальною версією схеми діяльності, а саме графічне представлення ходу подій на вісі часу.

– Е –

ЕКСПЕ́РТ *(лат. expertus – досвідчений, випробуваний)* – фахівець у будь-якій галузі, що проводить експертизу та здатний на підставі своїх знань та досвіду надавати кваліфіковану консультацію.

ЕКСПЕРТНЕ ОЦІНЮВАННЯ – процедура отримання оцінки проблеми на основі думки фахівця (експертів) з метою подальшого прийняття рішення (вибору).

Е́КСПОРТ ДАНИХ (від англ. *export*) – перетворення і запам'ятовування даних з початкового формату в інший формат, який буде зчитуватися певною програмою, призначеною для користувача. При цьому, звичайно, можлива сумісність з різними програмами.

ЕЛЕМЕНТ – це найпростіша неподільна частина системи, властивості якої визначаються конкретною задачею. 2. Елемент - це межа поділу системи з точок зору вирішення конкретного завдання і поставленої мети.

– З –

ЗБІР ІНФОРМАЦІЇ – діяльність суб'єкта, в ході якої він здійснює пошук і отримання відомостей про потрібний йому об'єкт.

ЗВІТНІ ДОКУМЕНТИ *(оперативно-розшукова діяльність)* – документи, що подаються у вищі, контрольні та/або наглядові органи і містять дані про результати оперативно-розшукової діяльності, зокрема результати кримінального аналізу.

ЗОВНІШНЄ СЕРЕДОВИЩЕ - це безліч існуючих поза системою елементів будь-якої природи, що впливають на систему і знаходяться під її впливом.

– І –

ІНТЕГРУВАННЯ *(як етап процесу кримінальної розвідки)* **–** полягає в об'єднанні інформації. На цьому етапі виконуються операції з масивами інформації, що полягають у її порівнянні, відборі, сортуванні, пошуку взаємозв'язків. Інтегрування може також полягати у візуальному представленні інформації у вигляді діаграм взаємозв'язків, діаграм руху, діаграм дій, матриці взаємозв'язків.

ІНТЕҐРОВАНИЙ БАНК ДАНИХ – це складна інформаційна система, яка являє собою сукупність окремих інформаційних систем (обліків, підсистем), що мають спільне застосування, високоорганізовану систему забезпечення й аналізу інформації з організацією доступу до інформації будь-якої його складової через одну адресу – ядро інтеґрованого банку даних.

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ (ІТ) – це комплекс методів і процедур, за допомогою яких реалізуються функції збирання, передавання, оброблення, зберігання та доведення до 3 користувача інформації в організаційно-управлінських системах з використанням обраного комплексу технічних засобів.

ІНФОРМАЦІЙНІ РЕСУРСИ *(англ. Information Resources)* – окремі документи і окремі масиви документів, документи і масиви документів в інформаційних системах, зафіксовані на відповідних носіях інформації, а також мовні засоби, що вживаються для опису конкретної предметної області і для доступу до даних і знань.

ІНФОРМАЦІЙНА СИСТЕМА – це організаційно впорядкована сукупність масивів інформації про певні об'єкти й інформаційні технології, у тому числі засоби сучасної

комп'ютерної техніки, програмного забезпечення та мереж зв'язку, що забезпечують процеси введення, опрацювання й видачі інформації користувачеві.

ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА - сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

ІНФОРМАЦІЯ - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

ІНФОРМАЦІЯ В АВТОМАТИЗОВАНИХ СИСТЕМАХ – сукупність усіх даних і програм, які використовуються в автоматизованих системах незалежно від засобу їх фізичного та логічного представлення.

– К –

КОНТЕНТ-МОНІТОРИНГ – систематичне, безперервне в часі сканування і контент-аналіз інформаційних ресурсів.

КОНЦЕПТУАЛІЗАЦІЯ ПРОБЛЕМИ – етап аналітичного дослідження, що передбачає встановлення координат, правоохоронної проблеми, що аналізується в просторі наукового знання та соціального досвіду; досягнення найбільш загальної уяви щодо явищ та процесів, які аналізуються для вирішення правоохоронних проблем на основі вивчення теоретичних моделей, концепцій, прецедентів.

КОРЕЛЯЦІЯ ДАНИХ – це підхід до виявлення та ілюстрації взаємозв'язків між парою змінних – між рівнем злочинності і деяким чинником, який може зробити вплив на злочинність.

– Л –

ЛІНІЙНЕ ПРОГНОЗУВАННЯ – методи, що припускають буденну логіку причинно-наслідкових взаємозв'язків, що вкладається в класичну формулу лінійної регресії.

ЛОГІЧНИЙ ЛАНЦЮГ – безперервний, послідовний ряд подій, міркувань, суджень, знань та ін..

– М –

МЕТОД АНАЛІЗУ – досить загальна і широко застосовувана процедура вирішення проблем, розрахована на різні галузі дослідження (наприклад, метод візуалізації, метод прогнозування, метод оцінювання та ін.).

МЕТОД «КЛАСТЕРНИЙ АНАЛІЗ» - це сукупність математичних методів, призначених для формування «віддалених» один від одного груп «близьких» між собою об'єктів за інформацією про відстані або зв'язки (заходи близькості) між ними.

МЕТОД «КОРЕЛЯЦІЙНИЙ АНАЛІЗ» - полягає у визначенні характеру зв'язків між двома наборами елементів (змінних) – діяльності, умов, функцій, тощо, та будуванні на їх основі Scatter-діаграм (діаграм розсіювання), що відображають тренди (тенденції) у графічній формі, а не математично.

МЕТОД ОЦІНКИ ІНФОРМАЦІЇ 4х4 *(метод «чотири на чотири»)* – застосування для оцінки інформації сукупності критеріїв, за якими окремо визначається достовірність інформації та достовірність джерела, з якого інформація походить. За результатом оцінки інформації та джерела надається літерно-цифровий код. *(Див. критерії оцінки інформації та критерії оцінки джерела інформації).*

МЕТОД ОЦІНКИ РИЗИКІВ «HAZOP» - полягає в деталізації та ідентифікації проблем в організації та здійсненні досудового розслідування кримінальних проваджень, визначенні можливих причин їх виникнення та оцінки наслідків.

МЕТОД СЦЕНАРІЇВ – різновид прогнозування, що застосовується в ситуаціях, коли одна або більш значущих змінних володіє невизначеним значенням. Окремі сценарії можуть будуватися для кожного вірогідного значення змінної, для кожного діапазону значень або за схемою «песимістичний сценарій» - «найбільш вірогідний сценарій» - «оптимістичний сценарій».

МЕТОДИКА АНАЛІЗУ – відносно спеціалізована процедура або технічний прийом, що застосовуються аналітиками для вирішення конкретних видів проблем.

МЕТОДОЛОГІЯ *(грец. methodos – шлях. дослідження та logos - наука)* – 1. Вчення про науковий метод пізнання й перетворення світу; його філософська, теоретична основа. 2.

Сукупність методів дослідження, що застосовуються в будь-якій науці відповідно до специфіки об'єкта її пізнання. 3. *Кримінальний аналіз.* Система вихідних, основних принципів, що визначають спосіб підходу до аналізу й оцінки явищ або процесів, характер ставлення до них, спрямованість пізнавальної та практичної діяльності.

МЕТОДОЛОГІЯ АНАЛІЗУ – систематичне і критичне вивчення множинних методів і методик аналізу; має скоріше ставлення до процесу отримання значимого знання, до логіки дослідження проблем, ніж просто до застосування конкретних методів і методик.

МОНІТОРИНГ *(англ. monitoring – спостереження)* - спеціально організоване систематичне безперервне спостереження за яким-небудь процесом з метою виявлення його відповідності бажаному результату, а також прогнозування та запобігання критичним ситуаціям.

– Н –

НАДІЙНІСТЬ ДЖЕРЕЛА ІНФОРМАЦІЇ – здатність джерела об’єктивно відтворити обставини, які стали йому відомі (відносно особи) або в ньому (з його допомогою) відобразилися (відносно речових джерел).

НЕЗАЛЕЖНА ЗМІННА – зміна, яка впливає на значення інших змінних, змінюючи свої власні значення.

НЕОБХІДНІСТЬ – філософська категорія, що відображає внутрішні, стійкі, істотні зв'язки предметів, явищ, процесів і визначальна їх закономірне змінення і розвиток. Існує в природі та суспільстві у формі об'єктивних законів. Непізнані закони з'являються як «сліпа» необхідність.

НЕІСТОТНІ ЗВ'ЯЗКИ – тимчасові, нестійкі, не визначальні для даного явища або процесу зв'язки і відносини.

НОРМАТИВ МОЖЛИВОСТЕЙ (*стратегічний аналіз)* – коефіцієнт, що визначається діленням суми бальних оцінок ступеня відповідності факторів поточного і оптимального потенціалу організації на число оцінюваних чинників. Приймає значення від 0 до 1.

– О –

ОБ'ЄКТИВНІСТЬ – науковий принцип, який орієнтує дослідника на розуміння певної суб'єктивності тієї інформації, з якою йому доводиться працювати з метою отримання аргументованих результатів аналітичної роботи на підставі сучасних досягнень науки і ефективних інформаційно-аналітичних технологій. Він вимагає від аналітика мінімізувати вплив особистих і групових інтересів, установок, інших суб'єктивних чинників на процес і результати дослідження.

ОБ’ЄКТ АНАЛІТИЧНОЇ РОБОТИ – галузь практичної діяльності, на яку спрямований процес дослідження. Вибір об’єкту визначає межі застосування отриманих результатів.

ОПИС – спосіб дослідження, який полягає в зазначення ознак об’єкта. Це може бути усне або письмове перелічення кількісних чи якісних ознак, властивостей в певній послідовності.

ОПИС ЗАГРОЗ – опис, спрямований на ідентифікування та аналіз слабких пунктів, які можуть бути використані в рамках злочинної діяльності. Метою є достатньо раннє опрацювання пропозицій, які стосуються запобігання злочинності шляхом ліквідування слабких точок та заходи, спрямовані проти потенційних винуватців кримінальних діянь.

ОПИС ЯВИЩ – є аналізом злочинного явища, яке має місце на конкретній території відповідно до конкретного періоду часу. Метою є розпізнання певних зразків (щодо способу дії), часу та місця, яким надається перевага, причин) як вихідної бази для опрацювання широкої стратегії.

ОЦІНКА ІНФОРМАЦІЇ *(англ. Evaluation of information)* – це визначення цінності елементів інформації з точки зору достовірності, надійності, відповідності та точності.

ОЦІНКА РЕАКЦІЇ (*стратегічний аналіз)* – аналіз реакції правоохоронного суб'єкта на вплив зовнішнього середовища через «вхід» - виклики, загрози, проблеми, можливості, вимоги, ресурси.

ОЦІНКА РИЗИКІВ (*стратегічний аналіз)* – це дослідження та визначення (пошук і встановлення) слабких елементів системи охорони кордону. Сферами, в яких здійснюється оцінка, а потім аналіз ризиків, зокрема є: система (модель) управління; дислокація технічних і людських ресурсів; рівень підготовленості персоналу до виконання визначених завдань;

результати службової діяльності у співставленні з обсягом і рівнем складності завдань; логістика та інші чинники, які зумовлюють ефективність виконання завдань.

П

ПРОГРАМНІ АНАЛІТИЧНІ ІНСТРУМЕНТИ – це сучасне програмне забезпечення (сервіси) дослідження, які дозволяють швидко та ефективно проводити аналіз системи взаємопов'язаних об'єктів і динаміки послідовних подій, відображаючи результати дослідження у вигляді зручних для розуміння схем, діаграм тощо.

-ПРОФІЛЬ – аналітичний продукт, який вміщує типові або, встановлені у ході аналізу ознаки, критерії, які дозволяють за комплексом цих ознак охарактеризувати та встановити потенційну жертву, злочинців подію.

ПРОФІЛЮВАННЯ РИЗИКІВ – встановлення суб'єктів, з боку яких існує висока ймовірність протизаконних дій, та їх селекція з метою проведення заходів, що виходять за сферу звичайного контролю, з метою запобігання вчиненню правопорушення або для встановлення доказів у разі його вчинення.

ПРОЦЕС АНАЛІТИЧНОЇ РОБОТИ – сукупність уявних операцій, які здійснюються в певній послідовності з використанням аналітичних засобів.

-Р-

РЕЛЕВАНТНІСТЬ ІНФОРМАЦІЇ – наявність зв'язку з проблемою (відповідність нашим інтересам) і здатність інформації вести вклад в процес розуміння проблеми.

РИЗИК – потенційна можливість реалізації загрози; числове значення ризику отримують перемноженням ймовірності виникнення події на ймовірність її конкретного наслідку.

РІШЕННЯ – вибір одного з можливих альтернативних варіантів, що здійснюється особою, яка приймає рішення і спрямований на досягнення визначеної мети. Рішення може розглядатися і як організаційний акт, і як один із основних етапів управління.

– С –

СИНТЕЗ – 1. Метод наукового дослідження предметів, явищ дійсності в цілісності, єдності та взаємозв'язку їх частин; прот. аналіз. 2. Єдність, цілісність певних сполучених, пов'язаних між собою явищ, предметів дійсності. 3. *книж.* Узагальнення, висновок із чого-небудь. 4. *хім.* Одержання або утворення складних хімічних речовин шляхом сполучання простіших речовин або елементів.

СИСТЕМА АНАЛІЗУ РИЗИКІВ – це сукупність підрозділів, утворених на всіх рівнях управління, що функціонують у сфері збору, обробки, систематизації, оцінки та аналізу інформації щодо загроз у сфері безпеки, а також систематичний оборот і використання результатів аналізу ризиків у службовій діяльності компетентних державних органів.

СИСТЕМНИЙ ПІДХІД – спосіб теоретичного та практичного дослідження, при якому кожний об'єкт розглядається як система.

СИТУАЦІЙНИЙ АНАЛІЗ – вивчається конкретна ситуації, відхилення від штатних ситуацій з метою попередження виникнення подібних в майбутньому.

СПОСТЕРЕЖЕННЯ – спосіб дослідження, який полягає в навмисному, систематичному і цілеспрямованому сприйнятті об'єктів, явищ з метою вивчення їх специфічних змін у певних умовах і відшукування смислу цих явищ.

СТРУКТУРНО-ФУНКЦІОНАЛЬНИЙ АНАЛІЗ – один з основних принципів системного дослідження соціальних явищ та процесів як структурно роздробленої цілісності, в якій кожен елемент структури має визначене функціональне призначення.

– Т –

ТЕХНОЛОГІЇ – під поняттям технології ми розуміємо загальні знання та опанування засобами,

– У –

УМОВИВІД – це найбільш складна форма мислення. Вона встановлює нові зв'язки між предметами і явищами на основі вже відомих. Умовивід - цілісне розумове утворення і має структуру: посилка (засновок) - судження, яке віддзеркалює вже відомі зв'язки; заключення (висновок) - судження, яке віддзеркалює нові зв'язки.

– Ф –

ФАКТ – відповідне дійсності явище, процес, подія, що має місце в об'єктивній реальності та є об'єктом вивчення.

ФАЗА ПРОЦЕСУ ОПРАЦЮВАННЯ ІНФОРМАЦІЇ – етап інформаційної обробки отриманих даних. Процес опрацювання інформації складається з наступних фаз: 1. Постановка цілей; 2. Пошук / збір інформації; 3. Реєстрування інформації; 4. Впорядкування інформації; 5. Накопичення / зберігання інформації; 6. Аналіз / оцінка інформації (у вузькому значенні), абстракція, компресування, порівняння / погодження, агрегація, відбір, поєднання; 7. Оцінка інформації / висновки / прогнозування; 8. Представлення результатів; 9. Візуалізація; 10. Звітування; 11. Передача результатів (усна, письмова); 12. Реалізація результатів; 13. Розробка стратегії; 14. Підсумкова оцінка і зворотна інформація.

ФОРМУЛЮВАННЯ ВИСНОВКІВ *(як етап процесу кримінальної розвідки)* – це кінцевий етап кожного аналізу. Висновки формулюються, виходячи з логіки, на підставі інформації та передумов. У випадку, якщо після перевірки висновки будуть відкинуті, цикл кримінальної розвідки вимагає повторення, починаючи від етапу накопичення інформації до етапу повторного формулювання нових висновків.

– Х –

ХАРАКТЕРИСТИКА – 1. Опис, визначення істотних, характерних особливостей, ознак кого-, чого-небудь. 2. Офіційний документ, в якому міститься відгук, висновок про чию-небудь трудову й громадську діяльність. 3. *спец.* Графічне зображення властивостей чого-небудь за допомогою кривої; який-небудь основний графічний показник чогось.

ХРОНОЛОГІЯ – як загальне поняття: послідовність історичних подій у часі; часослів'я, опис і вивчення того, як саме відбувалися певні події в часі (історично). *Астрономічна хронологія* - встановлення точного астрономічного часу на базі вивчення закономірностей руху небесних тіл. *Історична хронологія* - відносно самостійна («допоміжна») історична дисципліна, що вивчає різноманітні системи літочислення та їхній розвиток, допомагає встановлювати точні дати історичних подій і джерел шляхом переведення на сучасне літочислення дат інших літочислень і календарів.

ХРОНОЛОГІЯ ПОДІЙ (*кримінальний аналіз)* – будь-яка версія розвитку тих чи інших подій, що явно чи неявно враховує їх відносне і абсолютне розташування у часі і просторі.

– Ч –

ЧАСТОТА *(англ. frequency)* – фізична величина, що дорівнює кількості однакових подій за одиницю часу. Вона є характеристикою будь-яких процесів, які регулярно повторюються (кількість подій за одиницю часу) або величиною, що виражає: кількість рухів, коливань, повторень за одиницю часу тощо.

– Я –

ЯВИЩЕ – категорія для позначення в предметі, процесі того, що безпосередньо виявляється, виникає перед нами. Явище є зовнішньою, мінливішою і рухливішою стороною предмета, процесу.

7. ПЕРЕЛІК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Базова:

1. Конституція України від 28 червня 1996 року № 254к/96. URL: https://zakon.rada.gov.ua
2. Кримінальний кодекс України від 05.04.2001 № 2341-14. URL: http://zakon.rada.gov.ua/laws
3. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI URL: https://zakon.rada.gov.ua/laws
4. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 01.08.2016 № 80/94-ВР. URL:https://zakon.rada.gov.ua/laws
5. Закон України «Про інформацію» від 02.10.1992 № 2657-12. URL: http://zakon.rada.gov.ua/laws
6. Закон України « Про хмарні послуги» від 17.02.2022 **№** 2075-IX**.** URL: https://zakon.rada.gov.ua/laws

7. Закон України «Про захист персональних даних» від 01.06.2010 № 742297-17. URL: http://zakon.rada.gov.ua/laws
8. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. № 2163- VIII. URL: http://zakon.rada.gov.ua/laws
9. Указ Президента України «Про рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України» від 27 січня 2016 р., № 96/2016. URL: http://zakon.rada.gov.ua.
10. Указ Президента України «Про Національний координаційний центр кібербезпеки» від 07.06.2016 № 242/2016. URL: http://zakon.rada.gov.ua.
11. Ланде Д.В. OSINT у кібербезпеці : навч. пос. / Ланде Д.В. Київ: ТОВ «Інжиніринг», 2024. 522 с. ISBN 978-966-2344-97-4
12. Використання інструментів та методов OSINT для отримання пошукової інформації : практ. порадник / Д. С. Зоренко [та ін.] ; СБУ, Ін-т підгот. юрид. кадрів для СБУ НЮУ ім. Ярослава Мудрого. -4-е вид. - Харків : ІПЮК для СБ України, 2023. - 36 с.
13. Мірошніченко І.О., Ланде Д.В. Роль методів OSINT в кібербезпеці та їх застосування під час воєнних конфліктів. *Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених*. С. 282-284
14. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник / О. О. Торбас. Одеса : Юридика, 2024. 180 с. - Режим доступу: https://doi.org/10.32837/11300.27740
15. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.
16. Користін О.Є., Тімошин А.С. Інформаційні технології в кримінальному аналізі (практична частина): Навчальний посібник. 2022, 102 с.

Додаткова:

1. Жмур Н. В., Землянікін М. П. Історія становлення та сучасний стан технології пошуку інформації OSINT. *Юридичний вісник* № 3 (64) 2022. С. 95- 101. DOI: 10.18372/2307-9061.64.16895.
2. Щурат Т. Г. Напрями використання OSINT в оперативно- розшуковій діяльності. Роль та місце правоохоронних органів у розбудові демократичної правової держави: *матеріали XIV міжнар. наук.-практ. інтернетконф.,* м. Одеса, 31 жовтня 2022 р. С.144-146.
3. Кожушко О. О. Розвідка відкритих джерел інформації (OSINT) у розвідувальній практиці США. URL: http://jrnl.nau.edu.ua/index.php/ IMV/article/viewFile/3264/3217.
4. Розвідка на основі відкритих джерел. URL:https://www.wikidata.uk-ua.nina.az/OSINT.html
5. NATO Open Source Intelligence Handbook. URL: https://archive.org/details/NATOOSINTHandbookV1.2/mode/2u
6. Ржевська Н.Ф., Кожушко О.О. Розвідка відкритих джерел (OPEN SOURCE NTELLIGENCE) URL: https://ena.lpnu.ua:8443/server/api/ core/bitstreams/ a964dfbb-a16d-4e8a-b621-9aa6cb277197/content
7. Прощаєв В.В. Принципи розвідувальної діяльності за законодавством країн пострадянського простору: порівняльний аналіз. *Науковий вісник публічного та приватного права.* Випуск 1, том 1, 2019. С. 96-100.
8. Мартинюк С.О. Характеристика принципів функціонування OSINT у сфері національної безпеки. *Юридичний науковий електронний журнал.* № 9/2021. С. 332-334. URL: http://www.lsej.org.ua/9_2021/85.pdf
9. Zosym Maxym. Розвідка з відкритих джерел (Open-source intelligence – OSINT). URL: https://www.maxzosim.com/rozvidka-z-vidkritikh-dzherel- osint/
10. Розробка та програмна реалізація методики цифрової розвідки на основі відкритих джерел. Всеукраїнський конкурс на кращу студентську наукову роботу 2020/2021 навчального року. Секція: «Кібербезпека». URL: https://lpnu.ua/sites/default/files/2021/pages/12564/rozvidka.pdf
11. Bellingcat опублікував мапу зруйнованих Росією цивільних об'єктів в Україні. Радіо свобода. URL: https://www.radiosvoboda.org/a/news- bellingcat-karta-ruynuvan/31760116.html InformNapalm. URL https://informnapalm.org/ua/about-us/
12. The New York Times. URL: https://www.nytimes.com/ interactive/2022/12/21/

world/europe/bucha-ukraine- massacre-victims.html .
13. Щербань В.Д. Система гарантій функціонування OSINT у сфері антикорупційної діяльності в правоохоронних органах. *Часопис Київського університету права.* 2019/4 С.137-141. URL: file:///C:/Users/Lenovo/Downloads/127D0%A2%D0%B5%D0%BA%D1%81%D1%82%20%D1%81%D1%82%D0%B%D1%82%D1%82%D1%96-240-1-10- 20200319.pdf .

Інформаційні ресурси

1. www.rada.gov.ua – Офіційний сайт Верховної Ради України.
2. http://ippi.org.ua/ - науково-дослідний центр правової інформатики.
3. http://textbooks.net.ua – електронна бібліотека.
4. http://radnuk.info – український юридичний портал «Радник»