

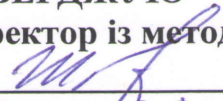
**ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»**

Факультет суспільних і прикладних наук

Кафедра права імені академіка УАН о. Івана Луцького

ЗАТВЕРДЖУЮ

Проректор із методичної роботи

 **Ярослав ШТАНЬКО**
«29» _____ 2025 р.

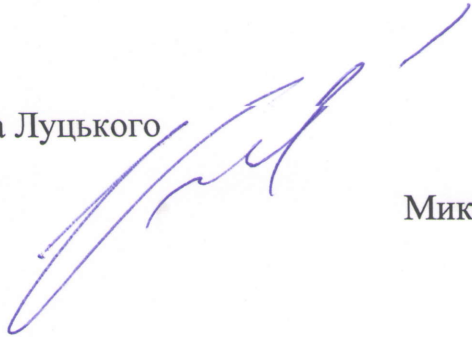
**ІНФОРМАЦІЙНО -АНАЛІТИЧНІ СИСТЕМИ ТА СИСТЕМИ ЗВ'ЯЗКУ В
ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ
СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

Галузь знань:	К Безпека та оборона
Спеціальність:	К 9 Правоохоронна діяльність
Освітньо-професійна програма:	«Правоохоронна діяльність»
Освітній рівень:	другий (магістерський)
Статус дисципліни:	обов'язкова
Мова викладання, навчання та оцінювання:	українська

**Івано-Франківськ
2025**

РОЗРОБНИК:

Професор кафедри права
імені академіка УАН о. Івана Луцького
доктор юридичних наук,
професор

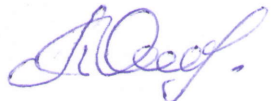


Микола КАРЧЕВСЬКИЙ

ЗАТВЕРДЖЕНО:

на засіданні кафедри права імені академіка УАН о. Івана Луцького,
протокол № 1 від 28.08 2025 р.

В.о. завідувача кафедри



Олександра ПТАШНИК

УЗГОДЖЕНО:

Гарант ОП



Сергій РЕПЕЦЬКИЙ

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 1 від 29 .08.2025 р.

Е-mail	<u>mykola.karchevskyi@ukd.edu.ua</u>
Номер аудиторії чи кафедри	<u>Кафедра права імені академіка УАН о. Івана Луцького, ауд. 201</u>
Посилання на сайт	<u>Микола Карчевський</u>
Сторінка курсу в СДО	Інформаційно -аналітичні системи та системи зв'язку в правоохоронній діяльності.

ВСТУП

Дисципліна «Інформаційно-аналітичні системи та системи зв'язку в правоохоронній діяльності» спрямована на підготовку магістрів правоохоронної сфери до ефективного використання сучасних інформаційних технологій, аналітичних методів і засобів зв'язку у професійній діяльності. Курс висвітлює концепцію поліцейської діяльності, керованої даними (data-driven policing), що ґрунтується на філософії Intelligence-Led Policing (ILP) – упровадженні аналізу даних та розвідки в управлінські рішення поліції. Студенти розглянуть теоретичні засади та практичні інструменти кримінального аналізу, ознайомляться з інформаційними системами Міністерства внутрішніх справ (МВС) України, сучасними засобами аналізу блокчейну і криптовалют для розслідувань, можливостями штучного інтелекту у прогнозуванні злочинності, а також європейськими стандартами щодо автоматизованої обробки персональних даних правоохоронними органами. Окрема увага приділяється опануванню базових аналітичних інструментів (Google Sheets, Looker Studio) для роботи з даними та вивченню систем зв'язку, які забезпечують діяльність правоохоронних органів.

Мета дисципліни – сформувати у здобувачів глибокі теоретичні знання та практичні навички використання інформаційно-аналітичних систем і засобів зв'язку в правоохоронній діяльності для підвищення ефективності попередження, розкриття та розслідування правопорушень.

Основні завдання навчальної дисципліни: опанувати концепції та методи, за допомогою яких дані та аналітика інтегруються в ухвалення управлінських рішень правоохоронних органів; навчитися застосовувати інструменти кримінального аналізу та інформаційні системи МВС у практичних ситуаціях; зрозуміти принципи роботи з блокчейн-аналітикою та використання криптовалютних транзакцій для розслідування злочинів; ознайомитися з технологіями штучного інтелекту для прогнозування ризиків і аналізу великих масивів правоохоронних даних; вивчити стандарти ЄС щодо захисту персональних даних при їх автоматизованому обробленні правоохоронними органами та відповідну європейську практику; набути навичок роботи з популярними хмарними інструментами аналізу даних (Google Sheets, Looker) для вирішення прикладних завдань; зрозуміти будову та принципи функціонування сучасних систем зв'язку правоохоронних органів (цифрові радіомережі, захищений зв'язок тощо).

В результаті успішного опанування дисципліни здобувач вищої освіти повинен знати:

- концепцію та ключові елементи підходу ILP (поліцейська діяльність, керована розвідкою та даними);
- основні методи кримінального аналізу (статистичний, геопросторовий, профайлінг, мережевий аналіз тощо) та їх інституційну реалізацію в діяльності поліції;

- структуру та призначення єдиної інформаційної системи МВС та її пріоритетних інформаційних ресурсів (реєстри, бази даних);
- можливості сучасних інструментів аналізу блокчейну (Chainalysis, Crystal) для відстеження криптовалютних транзакцій у розслідуваннях;
- сфери застосування штучного інтелекту в правоохоронній діяльності (прогностична аналітика, оцінка ризиків, розпізнавання образів та ін.) та пов'язані з цим етичні й правові ризики (алгоритмічна упередженість, прозорість, захист прав людини);
- вимоги директив ЄС щодо захисту персональних даних у кримінальному судочинстві (законність, цільове призначення, пропорційність, заборона повністю автоматизованих рішень без належного контролю людини);
- принципи роботи табличних інструментів та засобів візуалізації даних (Google Sheets, Looker Studio) для проведення правоохоронних аналізів;
- види та характеристики систем зв'язку, що використовуються правоохоронними органами (аналоговий та цифровий радіозв'язок, стандарти TETRA/P25, захищені канали тощо) та їх роль в координації дій підрозділів поліції.

Після завершення курсу здобувач повинен вміти:

- критично оцінювати дані кримінальної статистики та застосовувати їх для ухвалення управлінських рішень (виявлення crime hotspots, пріоритизація загроз);
- здійснювати базовий кримінальний аналіз – збирати, обробляти і візуалізувати дані про злочинність за допомогою електронних таблиць та ГІС-засобів;
- використовувати наявні інформаційні ресурси МВС (реєстри, бази даних) для перевірки інформації та отримання довідок у ході правоохоронної діяльності;
- аналізувати прості випадки руху криптовалютних коштів, застосовуючи логіку блокчейн-транзакцій (наприклад, за допомогою відкритих блокчейн-оглядачів) та розуміти висновки, які надають спеціалізовані аналітичні платформи;
- застосовувати інструменти штучного інтелекту на початковому рівні (наприклад, прогнозування ймовірності подій на основі наборів даних) з урахуванням обмежень щодо точності та упередженості таких систем;
- орієнтуватися в нормах європейського законодавства про захист даних і впроваджувати кращі практики захисту приватності при роботі з персональними даними громадян;
- створювати елементарні дашборди та звіти в Google Sheets та Looker Studio для представлення аналітичної інформації (діаграми динаміки злочинності, теплові карти правопорушень тощо);

– користуватися засобами службового зв'язку – портативними та автомобільними радіостанціями, засобами захищеного цифрового зв'язку – відповідно до встановлених протоколів, забезпечуючи безперервну комунікацію в оперативних умовах.

Компетентності та результати навчання, яких набувають здобувачі вищої освіти внаслідок вивчення навчальної дисципліни «Інформаційно-аналітичні системи та системи зв'язку в правоохоронній діяльності» (ОК9 відповідно до ОПП «Правоохоронна діяльність» другого (магістерського) рівня вищої освіти за спеціальністю К9 Правоохоронна діяльність) https://ukd.edu.ua/mahisterski-osvitni-prohramy	
Шифр та назва компетентності	Шифр та назва програмних результатів навчання
ЗК2. Здатність застосовувати знання у практичних ситуаціях.	ПРН2. Координувати діяльність суб'єктів забезпечення публічної безпеки і порядку, а також здійснювати взаємодію з представниками інших органів виконавчої влади та місцевого самоврядування, громадськістю з питань правоохоронної діяльності. ПРН3. Організовувати та керувати діяльністю підрозділів, які здійснюють правоохоронну діяльність. ПРН9. Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.	
СК10. Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час вирішення професійних завдань.	
СК12. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних, спеціальної техніки, оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності.	

спеціалізоване програмне забезпечення.

ПРН10. Користуватись державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку.

ПРН 13. Відшукувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію.

ПРН17. Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальних засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення

	оперативнорозшукової діяльності).
--	-----------------------------------

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	Перший (1)		
Семестр	Семестр (II)		
Кількість кредитів ЄКТС	3 (90 год)		
Аудиторні навчальні заняття		денна форма	заочна форма
	лекції	16 год.	4 год.
	семінари, практичні	14 год.	4 год.
Самостійна робота		60 год.	82 год.
Форма підсумкового контролю	Екзамен		

Структурно-логічна схема вивчення навчальної дисципліни:

Пререквізити	Постреквізити
	Особливості проведення та фіксації слідчих (розшукових) дій
	Аналіз, прогнозування та запобігання злочинності
	Міжнародні та національні механізми захисту і дотримання прав людини
	Правоохоронна практика

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Перелік тем лекційного матеріалу

Тема 1. Поліцейська діяльність, керована даними (2 год.)

Сутність підходу Data-Driven Policing: використання даних та доказів для ухвалення управлінських рішень, перехід від реактивної моделі до проактивної. Поняття інтелектуально-керованої поліції (Intelligence-Led Policing, ILP)

Модель ILP: цикл розвідки та аналізу, визначення пріоритетів та розвідувальних потреб, збір даних, їх обробка, аналіз і синтез аналітичних продуктів, доведення результатів до керівництва. Головна мета ILP – випереджаюче виявлення загроз і злочинних тенденцій, щоб запобігти злочинам до їх скоєння.

Практична реалізація керованої даними поліції: приклади впровадження ILP у світі (Велика Британія, США, ЄС). Роль підрозділів кримінального аналізу та fusion centers (центрів збору та аналізу розвідданих) у агрегуванні інформації та обміні нею між агенціями. Значення партнерства з іншими органами і приватним сектором у виявленні сучасних загроз.

Виклики впровадження data-driven підходів: кадрові (необхідність підготовки аналітиків), технічні (великі дані, сумісність систем), організаційні (культурні зміни від “традиційної” моделі до моделі, керованої даними). Питання етики: недопущення порушення прав громадян при масовому зборі та аналізі даних.

Тема 2. Кримінальний аналіз (2 год.)

Поняття кримінального аналізу: системна аналітична діяльність у правоохоронних органах, спрямована на отримання знань про злочинність і злочинців для підтримки прийняття рішень. Розвиток кримінального аналізу як професійної функції (міжнародний досвід становлення підрозділів аналізу в поліції).

Види та методи кримінального аналізу: стратегічний аналіз (довгострокові тенденції, прогнози злочинності), тактичний аналіз (оперативна підтримка розслідувань, профілі злочинців), адміністративний аналіз (оцінка ефективності підрозділів). Статистичні методи (коефіцієнти, тренди, кореляції), ГІС-аналіз для hotspots (географічна концентрація злочинів), соціальна мережна аналітика (виявлення зв'язків між правопорушниками), профайлінг та тимчасовий аналіз (добові/сезонні цикли злочинності).

Інструменти кримінального аналізу: спеціалізовані програмні продукти та бази даних. Використання електронних таблиць та СУБД для базового аналізу; програми візуалізації (IBM i2 Analyst's Notebook, GIS-програми, відкриті інструменти на зразок CrimeStat, R, CrimeDataLab). Сучасні trend analytics та

новітні інформаційно-аналітичні інновації, що впроваджуються аналітиками (елементи штучного інтелекту, автоматизація рутинних завдань).

Практичне застосування: аналіз кримінальної обстановки на основі відкритих даних (наприклад, публічних звітів поліції). Виявлення закономірностей: правило “80/20” (20% локацій генерують 80% злочинів) та повторна віктимізація. Представлення результатів аналізу у формі зрозумілих звітів для керівництва (діаграми, карти, аналітичні довідки). Значення кримінального аналізу у проєктах проблемно-орієнтованої поліції та превенції правопорушень.

Тема 3. Інформаційні системи Міністерства внутрішніх справ України (2 год.)

Єдина інформаційна система МВС (ЄІС МВС): призначення та архітектура. ЄІС МВС забезпечує автоматизований обмін даними між усіма суб'єктами системи МВС. Основні функціональні підсистеми ЄІС МВС: Національна система біометричної ідентифікації, інформаційно-пошукові системи Національної поліції, відомчі реєстри (транспортних засобів, зброї, осіб, зниклих безвісти тощо).

Ключові реєстри та бази даних: Єдиний реєстр досудових розслідувань (ЕРДР) – центральна база для обліку кримінальних проваджень, електронна система збору, зберігання та обробки інформації про хід досудового слідства. Інтегрована інформаційно-пошукова система Національної поліції (централізований банк даних про правопорушення, підозрюваних осіб, транспорт, зброю тощо). Реєстр адміністративних правопорушень у сфері безпеки дорожнього руху, Єдиний реєстр зброї, база даних розшукуваних осіб і предметів та інші ресурси, що входять до ЄІС.

Взаємодія та обмін даними: Інтеграція відомчих систем із національними та міжнародними базами. Обмін інформацією між МВС, судами (Єдиний держреєстр судових рішень), прикордонними та митними базами, Інтерполом. Проблеми сумісності форматів і захисту інформації при такому обміні.

Адміністрування та доступ: поняття суб'єктів ЄІС МВС та режимів доступу до даних (різні рівні користувачів). Забезпечення інформаційної безпеки – шифрування, розмежування доступу, резервування даних. Вимоги законодавства щодо захисту персональних даних у відомчих інформаційних системах.

Перспективи розвитку: впровадження нових модулів (наприклад, система електронного документообігу МВС, аналітичні панелі для керівництва на основі даних ЄІС), інтеграція з демографічним реєстром, системами відеоспостереження (проєкт «Безпечне місто»), використання хмарних технологій для зберігання й обробки великих даних правоохоронної сфери.

Тема 4. Blockchain-аналітика у правоохоронній діяльності. Crystal, Chainalysis (2 год.)

Роль криптовалют у сучасній злочинності: використання Bitcoin та інших криптовалют у кіберзлочинах, відмиванні коштів, торгівлі наркотиками та іншій протиправній діяльності (Darknet-ринки, програми-вимагачі тощо). Виклики, які стоять перед правоохоронцями: псевдоанонімність блокчейну, глобальний характер транзакцій, відсутність регуляторних кордонів.

Основи блокчейн-аналізу: прозорість публічних блокчейнів. Можливості відстеження “шляхів грошей” у блокчейні через аналіз графів транзакцій. Поняття біткойн-адреси та гаманця, кластери адрес, які належать одному користувачу. Евристики для об’єднання адрес (напр., спільні виходи транзакцій).

Спеціалізовані інструменти: огляд провідних платформ Blockchain Intelligence. Chainalysis – комерційний сервіс аналізу криптовалют, що надає інструменти для виявлення підозрілих транзакцій, зіставлення адрес з реальними сервісами та побудови зв’язків між ними.

Crystal – інструмент, розроблений для правоохоронців і фінансових установ, який дозволяє відстежувати біткойн-транзакції до реальних суб’єктів. Принципи роботи Crystal: скрейпінг даних з відкритих джерел про приналежність адрес, автоматизоване “ризикове скорингування” транзакцій та гаманців. Інші рішення: CipherTrace, Elliptic, Bitquery тощо – їх можливості та обмеження.

Практичне застосування в розслідуваннях: реальні кейси, коли за допомогою блокчейн-аналізу було ідентифіковано злочинців (наприклад, відстеження платежів у справі Silk Road, викриття хакерських груп, що переводили криптовалюту у фіат). Використання аналітичних звітів Chainalysis у судових справах. Обмеження: складність аналізу coinjoin-транзакцій, використання міксерів, а також перехід злочинців на криптовалюту з підвищеною анонімністю (Monero тощо). Необхідність міжнародної співпраці для закріплення доказової бази (через біржі, платформи).

Нормативні аспекти: правові підстави для відстеження криптовалютних транзакцій в Україні та світі. Включення аналітичних звітів по блокчейну до матеріалів кримінального провадження (експертні висновки). Тенденція до регулювання ринків віртуальних активів (Регламент ЄС MiCA та ін.)

Тема 5. Штучний інтелект для прогнозування та аналітики у правоохоронній сфері (2 год.)

Загальні відомості про ШІ: ключові концепції – машинне навчання, нейронні мережі, алгоритми класифікації та прогнозування. Сфери застосування AI/ML у правоохоронній діяльності: прогнозування локацій і часу скоєння злочинів (predictive policing), оцінка ризику рецидиву або небезпеки підозрюваного (інструменти типу COMPAS), аналіз відео- та аудіоданих (розпізнавання облич, номерних знаків, голосу), обробка великих масивів тексту (наприклад, соцмереж) для виявлення загроз тероризму тощо.

Прогностичне поліцейське патрулювання: алгоритми location-based (на основі статистики злочинів передбачають “гарячі точки” і вікна часу

підвищеного ризику) та person-based підходи (оцінюють індивідів за ймовірністю стати злочинцем чи жертвою). Вдалі кейси: проект Crime Nabi в Японії (покращення виявлення hotspots більш ніж на 50%); використання ШІ-аналітики для пошуку зниклих осіб (Marinus Analytics, США).

ШІ у слідстві та судочинстві: автоматизований аналіз доказів (наприклад, класифікація величезних обсягів цифрових доказів – фото, переписок), допомога в проходженні відеоматеріалів (проекти типу Axon AI для перегляду записів нагрудних камер). У судах – системи підтримки прийняття рішень щодо запобіжних заходів та умовно-дострокового звільнення (алгоритмічні оцінки ризиків).

Ризики та етичні проблеми: алгоритмічна упередженість, проблема прозорості. Міжнародна дискусія щодо правових обмежень.

Регулювання ШІ та найкращі практики: Європейський Акт про ШІ – класифікація систем для правоохоронців як “високого ризику” з обов’язковими вимогами до прозорості та оцінки впливу. Рекомендації щодо відповідального використання ШІ: підзвітність розробників та користувачів алгоритмів, незалежний аудит на упередженість, залучення громади до обговорення (концепція Ethics by Design). Баланс між інноваціями та дотриманням прав людини у сфері правоохоронного застосування штучного інтелекту.

Тема 6. Стандарти ЄС щодо автоматизованої обробки персональних даних правоохоронними органами. Практика ЄС (2 год.)

Загальна характеристика правового режиму: Директива (ЄС) 2016/680 (так звана Law Enforcement Directive, LED). Принципи обробки даних згідно з європейськими стандартами: законність і справедливість; збирання даних для визначених, чітких і законних цілей; пропорційність – дані мають бути релевантними та не надмірними для мети обробки; точність та актуальність; зберігання не довше, ніж необхідно; цільове призначення – заборона використовувати дані несумісно з початковою метою збору. Забезпечення належного захисту і безпеки даних (технічними і організаційними заходами) – шифрування, контроль доступу, журналювання дій тощо.

Спеціальні вимоги LED: розмежування даних різних категорій суб’єктів – підозрюваних, засуджених, потерпілих, свідків – для уникнення надмірного втручання. Встановлення строків зберігання і періодичний перегляд необхідності зберігання персональних даних.

Права суб’єктів даних: право осіб отримувати інформацію про обробку їхніх даних правоохоронним органом, право на доступ до своїх даних, виправлення або видалення неточних даних, право на оскарження до незалежного наглядового органу (уповноваженого із захисту даних). Обмеження прав суб’єктів. Заборона певних видів обробки

Практика ЄС та кейси: огляд рішень Суду ЄС та національних практик щодо використання технологій спостереження і аналізу даних поліцією.

Реалізація стандартів в Україні: огляд стану імплементації європейських підходів у національному законодавстві (Закон України «Про захист персональних даних», окремі положення про інформаційні системи правоохоронних органів).

Плани адаптації LED в межах євроінтеграції. Значення рішень Європейського суду з прав людини (наприклад, щодо зберігання DNA-профілів, прослуховування) для практики правоохоронних органів.

Тема 7. Аналітичні можливості Google Sheets та Looker Studio у правоохоронній діяльності (2 год.)

Google Sheets як інструмент аналізу даних: хмарна електронна таблиця, що дозволяє працювати спільно з даними в реальному часі. Можливості Sheets для правоохоронців: імпорт даних (CSV, XLS) з різних джерел, використання формул і функцій для обчислення показників (середні, проценти змін, ранжування), застосування функцій пошуку та фільтрів для вибіркового аналізу. Побудова зведених таблиць (Pivot Table) для агрегування статистики злочинності за категоріями (тип злочину, час, локація). Візуалізація в Sheets: швидке створення діаграм (лінійних графіків динаміки, гістограм розподілу, секторних діаграм структури).

Looker Studio (Google Data Studio): безкоштовна веб-платформа для створення інтерактивних аналітичних дашбордів і звітів із різних джерел даних. Інтеграція з Google Sheets. Переваги Looker Studio для потреб правоохоронців: наочне відображення складної інформації (карти злочинності, показники ефективності) у вигляді зрозумілих графіків і карт; інтерактивність.

Приклади використання: створення панелі показників діяльності поліції (кількість зареєстрованих злочинів, розкриття, середній час реагування) – з відображенням цілей та фактичних значень. Побудова географічної карти в Looker Studio з нанесенням точок злочинів або зон концентрації правопорушень.

Обмеження та безпека: при роботі з реальними даними правоохоронних органів у хмарних сервісах необхідно враховувати вимоги інформаційної безпеки – можливо, потрібні закриті мережі або анонімізація даних перед завантаженням. Обмеження Google Sheets – продуктивність при дуже великих обсягах даних (десятки тисяч рядків і більше).

Тема 8. Системи зв'язку у правоохоронній діяльності (2 год.)

Еволюція засобів зв'язку поліції: від аналогових УКХ-радіостанцій до сучасних цифрових мереж. Вимоги до зв'язку в правоохоронних органах: надійність (зв'язок не повинен перериватися у критичний момент), захищеність (неможливість перехоплення переговорів сторонніми), швидкість з'єднання і групового виклику (між підрозділами, штабом та ін.).

Цифрові trunked-radio системи стандарту TETRA (Terrestrial Trunked Radio) – європейський стандарт професійного мобільного радіозв'язку, спеціально

розроблений для екстрених служб. Характеристики TETRA: використання часових слотів TDMA (4 канали на частоті 25 кГц), шифрування ефіру та за потреби end-to-end, можливість як прямих викликів, так і через інфраструктуру (ретранслятори). Проект 25 (P25) – північноамериканський аналог цифрового стандартизованого зв'язку, сумісний для різних агентств. Приклади впровадження

Поступовий перехід на цифрові засоби в Україні (система «Кордон» для ДПСУ, проекти цифрового зв'язку для Нацполіції).

Спеціальні можливості зв'язку: режим DMO (Direct Mode) – прямий зв'язок між радіостанціями без інфраструктури на випадок виходу з ладу мережі або роботи поза зоною покриття (із можливістю ретрансляції сигналу через інші радіостанції). Екстрений виклик. Інтеграція голосового зв'язку з передачею даних.

Безпечний зв'язок і новітні технології: впровадження LTE/5G мереж для потреб публічної безпеки (наприклад, американська мережа FirstNet) – забезпечення широкосмугової передачі даних (відео з місця події, доступ до баз даних з планшетів у патрульних машинах) разом із гарантованим пріоритетованим доступом для екстрених служб.

Використання захищених мобільних месенджерів (із шифруванням і контролем ІТ-відділу) як доповнення до радіозв'язку. Супутниковий зв'язок для ситуацій, коли наземна інфраструктура відсутня (спеціальні портативні термінали, якими користуються підрозділи в місії або прикордонники у важкодоступних районах).

Кібербезпека систем зв'язку. Захист конфіденційності переговорів – обов'язкове наскрізне шифрування для оперативних каналів. Організація зв'язку під час надзвичайних ситуацій (резервні канали, мобільні ретранслятори на випадок відмови стаціонарної мережі).

Державна система урядового зв'язку як складовий єдиної системи зв'язку органів державної влади, що забезпечує захищені канали для вищого керівництва держави та критичних державних інституцій.

Національна система конфіденційного зв'язку, яка інтегрує урядовий, спеціальний і захищений корпоративний зв'язок, а також гарантує інформаційну безпеку у сфері державного управління.

Формування та реалізація державної політики у сферах: кіберзахисту критичної інформаційної інфраструктури; безпеки державних інформаційних ресурсів та інформації з обмеженим доступом; криптографічного та технічного захисту інформації; телекомунікацій і користування радіочастотним ресурсом України.

Поштовий зв'язок спеціального призначення та урядовий фельд'єгерський зв'язок як складові спеціальних каналів комунікації правоохоронних та державних органів.

Перелік тем семінарських занять

Тема 1. Поліцейська діяльність, керована даними (2 год.)

Семінарського заняття не передбачено

Зміст самостійної роботи здобувачів:

Базова самостійна робота: опрацювання лекційного матеріалу та основної літератури, підбір прикладів практичного застосування технології ухвалення рішень керованих даними у практичній діяльності поліції для подальшого обговорення під час семінарів.

Додаткова самостійна робота: аналіз призначення функцій та можливостей навчальних інформаційно-аналітичних систем CrimeDataLab та IFSafeLab

Тема 2. Кримінальний аналіз – семінарське заняття (2 год.)

Обговорення поняття та ролі кримінального аналізу: які нові можливості отримують правоохоронні органи завдяки впровадженню аналітичних підрозділів (приклади з інших країн, досвід Національної поліції України).

Види кримінального аналізу та відповідні завдання: приклади стратегічного, тактичного й адміністративного аналізу зі своєї практики або відомих кейсів. Чим відрізняється аналіз для профілактики злочинності від аналізу для розкриття конкретного злочину?

Які інструменти (Excel/Sheets, GIS) використовувалися б для такого аналізу?

Проблемні питання: що обмежує ефективність кримінального аналізу в наших реаліях? (недостатність даних, їх якість, опір змінам з боку персоналу). Які кроки потрібно здійснити для розвитку цієї функції (тренінги, ПЗ, регламентація роботи аналітиків)?

Зміст самостійної роботи здобувачів:

Базова самостійна робота: опрацювання лекційного матеріалу та основної літератури до теми 2; аналіз офіційної кримінальної статистики за останні кілька років (за даними МВС чи ін. відкритими джерелами) – виявлення загальної тенденції (зростання/спад злочинності) і формулювання питань для обговорення на основі цих даних (наприклад: які види злочинів демонструють найбільшу зміну і чому?).

Додаткова самостійна робота: підготовка короткої доповіді про досвід впровадження інформаційно-аналітичної системи або підрозділу кримінального аналізу в одній із країн ЄС/НАТО (на вибір студента – наприклад, “Поліцейська аналізна платформа Нідерландів” чи аналітичні підрозділи ФБР); виконання міні-дослідження з використанням CrimeDataLab: зібрати з відкритих джерел дані про певну категорію злочинів (наприклад, кількість шахрайства по областях) і побудувати просту візуалізацію (діаграму, карту), надати інтерпретацію знайденим тенденціям.

Тема 3. Інформаційні системи МВС – семінарське заняття (2 год.)

Структура Єдиної інформаційної системи МВС: скласти схему (блок-схему) ЄІС МВС із основними підсистемами. Обговорення: які з цих підсистем є найбільш значущими для повсякденної роботи слідчого/дільничного?

Робота з реєстрами: моделювання ситуації – слідчий отримав інформацію про виявлений автомобіль без номерів, і є підозра, що він може бути у розшуку. Які дії щодо перевірки по наявних базах даних він має здійснити? Аналогічно, ситуація: особа без документів – які інформаційні ресурси допоможуть встановити особу.

Захист персональних даних в інформаційних системах: обговорення вимог законодавства (ст. 10 Закону України “Про захист персональних даних”, принципів LED) у контексті роботи з ЄІС МВС. Що означає “цільове призначення” даних? Чи може інформація з реєстрів МВС використовуватися для дослідницьких чи статистичних цілей – за яких умов?

Сучасні тенденції: які нові інформаційні системи чи модулі були запроваджені останнім часом? Дискусія: як цифровізація процесів (електронні протоколи, електронний документообіг) впливає на ефективність правоохоронної діяльності і які ризики несе.

Зміст самостійної роботи здобувачів:

Базова самостійна робота: детальне вивчення структурно-функціональних схем ЄІС МВС з лекційних матеріалів і нормативних актів (положення про ЄІС МВС) – складання переліку основних інформаційних ресурсів (реєстрів) із коротким описом їхнього призначення; опрацювання інструкцій/наказів МВС щодо порядку доступу до цих реєстрів (хто і як може отримувати інформацію).

Додаткова самостійна робота: підготовка короткого есе або аналітичної довідки на тему “Порівняння інформаційних систем поліції України та однієї з країн ЄС” – наприклад, зіставити ЄІС МВС з відповідною системою в Польщі чи Німеччині (які є спільні риси, що відмінного, які успішні рішення можна запозичити); виконання практичного завдання – за допомогою демоверсії або опису інтерфейсу будь-якого поліцейського реєстру (наприклад, ЄРДР) описати послідовність дій для внесення інформації про нове кримінальне провадження; ознайомлення з доповідями/звітами міжнародних проєктів (EUAM, ICITAP) щодо розвитку інформаційних систем МВС України та підготовка питань для обговорення на наступному занятті.

Тема 4. Blockchain-аналітика – семінарське заняття (2 год.)

Криптовалюти і правоохоронна діяльність: спільне обговорення – чому криптовалюти стали популярними серед злочинців? Які типи злочинів найчастіше їх використовують? Чи означає псевдонімність біткойну, що злочинця неможливо знайти?

Принципи аналізу блокчейну. Огляд інструментів: студентам пропонується відвідати веб-сайт (демонстраційний) Chainalysis або Crystal та ознайомитися з

прикладом інтерфейсу. Обговорення функціоналу: які види даних показує система?

Кейс-стаді: розбір публічного кейсу (наприклад, Colonial Pipeline ransomware attack 2021 – коли ФБР відстежило й вилучило частину викупу в біткойнах). Хто бажає, готує стислий виклад кейсу: як саме вдалося дізнатися, куди пішли гроші; яку роль відіграли біржі або KYC (верифікація) у встановленні особи. Обговорення правових моментів: як отримали приватний ключ (ордер, оперативні заходи?), у якій юрисдикції це відбувалося.

Дебати: “Чи повинна держава мати можливість повністю deanonymize транзакції у блокчейні?”. Одна частина групи аргументує, що так (для ефективної боротьби зі злочинністю, сурто не повинно бути “тихою гаванню”). Інша – що повний контроль неможливий та небажаний (приватність, технічні складнощі).

Резюме: блокчейн – не анонімний, значна частина злочинної активності може бути відстежена завдяки доступності реєстру. Правоохоронцям потрібні і навички, і міжнародна співпраця, щоб успішно використовувати ці можливості.

Зміст самостійної роботи здобувачів:

Базова самостійна робота: опрацювання лекційного матеріалу; ознайомлення зі статтею/розділом з рекомендованої літератури про принципи розслідування злочинів, пов'язаних із криптовалютами; практична вправа – використовуючи відкритий блокчейн-оглядач (наприклад, Blockchain.com Explorer), знайти та проаналізувати просту транзакцію: визначити її хеш, кількість входів/виходів, суму, комісію, висновки щодо того, чи була вона “простою” чи “комбінованою” (з багатьма входами, що може вказувати на змішування коштів).

Додаткова самостійна робота: підготовка презентації про один із спеціалізованих інструментів блокчейн-аналітики – описати його можливості, які типи криптовалют підтримує, які кейси успішно розкривалися з його допомогою (наприклад, Chainalysis і справа Silk Road, Crystal і операція по викриттю дитячої порнографії та ін.); написання короткого аналітичного огляду “Використання криптовалют українською оргзлочинністю: ризики та протидія” (зі спробою оцінити масштаб проблеми і наявні в Україні можливості її вирішення).

Тема 5. Штучний інтелект у правоохоронній аналітиці – семінарське заняття (2 год.)

Обговорення очікувань і реальності: студенти діляться своїм розумінням, що таке “штучний інтелект” і які приклади його роботи вони знають (не лише в поліції, а й загалом). Потім – які очікування від використання ШІ в поліції. Висновок про існуючі технології та їх межі.

Predictive policing: розбір прикладу алгоритму прогнозування. Відомі експерименти: Лос-Анджелес (PredPol) – як алгоритм виявив патерни, непомітні людині, і чи справді це дало ефект.

Системи оцінки ризиків (Risk assessment): наприклад, COMPAS – алгоритм, що оцінює ризик рецидиву. Група ділиться на дві частини для рольової гри:

“комісія з умовно-дострокового звільнення”. Одній половині дають умовний профайл особи + результат COMPAS (високий ризик), іншій – тільки профайл без алгоритму. Питаємо: кого б ви відпустили? Обговорення: чи схильні люди довіряти алгоритму більше за власні оцінки, якщо так – добре це чи погано? Згадуємо відомий випадок із COMPAS, коли алгоритм виявився упередженим щодо афроамериканців.

АІ для відеоспостереження: системи розпізнавання обличчя в натовпі, системи “розумного” відеонагляду, що визначає підозрілу поведінку. Обговорення правових і етичних аспектів: чи погоджуються студенти з розгорненням таких систем у своєму місті? Де межа між безпекою і приватністю? Згадати, що в ЄС схиляються до заборони розпізнавання обличчя правоохоронцями у реальному часі.

Нові загрози, пов’язані з ІІІ: обговорення поняття deepfake, приклади, коли злочинці вже використовували ІІІ (фейкові відео з вимогою викупу, voice spoofing для шахрайства з банками).

Кейс для аналізу: проєкт “Х” (вигаданий) – поліція планує впровадити систему, що автоматично аналізує всі виклики 102 і класифікує їх за рівнем пріоритету з використанням ML-моделі. Запитання для груп: які потенційні вигоди, які ризики? Студенти оформлюють “резолюцію” – впроваджувати чи ні, і які запобіжні заходи потрібні.

Завершення: ІІІ – потужний інструмент, який може підвищити ефективність правоохоронних органів, але його впровадження повинно бути поступовим, з урахуванням правових норм і громадського контролю.

Зміст самостійної роботи здобувачів:

Базова самостійна робота: опрацювання лекційного матеріалу і рекомендованих статей по темі 5; аналіз одного з реальних прикладів використання АІ в поліції (наприклад, PredPol або Palantir в поліції Лос-Анджелеса); ознайомлення зі змістом Закону ЄС про ІІІ (розділ про правоохоронну діяльність) – коротко викласти, які системи ІІІ вважаються “високоризиковими” і що це означає.

Додаткова самостійна робота: дослідження випадку судового оскарження алгоритму (наприклад, справа State v. Loomis щодо використання COMPAS у Вісконсині) – підготувати міні-бриф, як суд обґрунтував рішення, чи дозволив враховувати алгоритм при винесенні вироку; написання есе на тему “Алгоритми прогнозування злочинності: чи є майбутнє в Україні?” – де обґрунтувати власну позицію з посиланням на досвід інших країн.

Тема 6. ЄС стандарти захисту даних – семінарське заняття (2 год.)

Дискусія: «Що важливіше – безпека чи приватність?».

Розбір принципів LED: студенти об’єднуються в малі групи, кожна отримує один з принципів (законність, мінімізація, обмеження строку зберігання,

точність, безпека). Група готує коротке пояснення принципу своїми словами з прикладом його значення на практиці.

Кейс-стаді «База ДНК vs права людини»: ситуація – поліція прагне створити базу ДНК усіх громадян “для швидкого розкриття злочинів”. Обговорення з посиланням на практику ЄСПЛ (справа *S. and Marper v. UK*, де зберігання ДНК невинуватих осіб визнано порушенням ст.8 ЄКПЛ). Студенти висловлюються, чи згодні з рішенням: які ризики у тотальному зберіганні ДНК-профілів? Які альтернативи?

Автоматизовані рішення: обговорення прикладів, коли рішення приймає комп’ютер. Чи стикалися студенти з цим? Чи було б прийнятним, щоб система сама вирішувала, кого арештувати, без участі слідчого? Студенти обговорюють, як забезпечити “значну участь людини”.

Практика забезпечення прав суб’єктів: моделювання ситуації – громадянин запитує у поліції, чи є в них його персональні дані і вимагає надати копію. Як повинен діяти відповідальний підрозділ? Обговорення українського контексту: на практиці такі запити рідкі, але за законом поліція мусить відповідати

Реальні кейси у ЄС: обговорення коротких повідомлень про те, як у конкретній країні адаптували LED.

Підсумкова вправа: кожен студент називає один практичний крок, який, на його думку, повинна зробити Національна поліція України, щоб краще захищати персональні дані громадян. Група формує спільний список рекомендацій.

Зміст самостійної роботи здобувачів:

Базова самостійна робота: опрацювання тексту Директиви (ЄС) 2016/680 або її стислого викладу українською/англійською; складання таблиці відповідності: принципи захисту даних (LED) – положення українського закону “Про захист персональних даних”.

Додаткова самостійна робота: написання есе на тему “Співвідношення безпеки і приватності: як знайти баланс?” – аргументувати, спираючись на європейські стандарти, власну позицію щодо використання інструментів масового стеження або збору даних.

Тема 7. Інструменти Google Sheets та Looker Studio – семінарське заняття (2 год.)

Практичне завдання: студенти заздалегідь отримують невеликий набір даних (наприклад, 100 записів про злочини: дата, район, тип злочину). На семінарі – спільна робота: відкрити цей файл у Google Sheets (поширений доступ) і виконати кілька завдань: порахувати кількість злочинів по кожному району (використовуючи функцію зведеної таблиці або фільтри), визначити середню кількість злочинів на день тощо.

Візуалізація даних: на основі отриманих у першій частині результатів (кількість злочинів по районах) студенти будують діаграму в Sheets (стовпчикову чи кругову) – хто справився, демонструє через спільний екран або описує кроки.

Обговорення: яка діаграма краще підходить для представлених даних і чому.

Знайомство з Looker Studio: створити новий звіт у Looker Studio, підключивши той самий Google Sheet як джерело.

Обговорення: чим такий інтерактивний звіт корисніший за статичні графіки?

Використання аналітичних інструментів у реальній роботі: дискусія – чи доводилося комусь зі студентів застосовувати Excel/Sheets у службових завданнях? Якщо так, поділитися досвідом. Якщо ні, то придумати разом 2-3 ситуації, де це могло б стати в пригоді.

Інші функції Sheets/Looker для правоохоронців: можливість імпорту даних із зовнішніх джерел (імпорт XML/JSON через скрипти, Google Public Data), використання Google Forms + Sheets для опитувань (наприклад, опитати місцевих мешканців щодо їх відчуття безпеки і автоматично отримати таблицю результатів). Обговорення, як такі інструменти полегшують дослідницьку роботу підрозділам превенції чи кадрового забезпечення (анкетування).

Підбиття підсумків вправи: студенти формулюють, які нові навички вони здобули.

Зміст самостійної роботи здобувачів:

Базова самостійна робота: повторення матеріалу – самостійне виконання аналогічних завдань із іншим набором даних (підготовано викладачем або знайдено студентом у відкритих джерелах, наприклад, статистика ДТП чи адміністративних правопорушень); складання інструкції (у вигляді алгоритму дій) “Як побудувати зведену таблицю в Google Sheets”; аналіз декількох шаблонів звітів Looker Studio (Google надає галерею шаблонів) – вибрати один, який міг би бути корисним поліції (наприклад, шаблон аналізу інцидентів) і коротко описати, чим.

Додаткова самостійна робота: підготовка міні-проєкту – знайти у відкритому доступі реальний датасет, пов’язаний із кримінальною юстицією (наприклад, відкриті дані поліції про злочини певного місяця, або дані соціопитування щодо довіри до поліції), завантажити його в Google Sheets і виконати аналіз (описати дані, побудувати 1–2 діаграми, зробити короткі висновки). Оформити результати або у вигляді скріншотів з поясненнями, або надати доступ до створеного дашборду Looker Studio; ознайомлення з довідковими матеріалами Google (онлайн-документацією або уроками на YouTube) щодо додаткових можливостей Sheets, Looker.

Тема 8. Системи зв’язку – семінарське заняття (2 год.)

Основи організації зв’язку: які засоби радіозв’язку використовуються в підрозділах, де служать студенти (якщо є практичний досвід у групі, обговорення проблем аналогового зв’язку).

Цифровий радіозв’язок: які переваги згадані?

Чи може месенджер замінити рацію? Обговорення: плюси, мінуси.

Безпека зв’язку: студенти наводять потенційні загрози та засоби захисту.

Аналіз кейсу: моделювання ситуації відключення звичайних каналів зв'язку. Як Національна поліція, СБУ чи МВС можуть забезпечити взаємодію через систему урядового чи конфіденційного зв'язку?

Дискусія: «Чи є доцільним поширення урядового зв'язку на органи місцевого самоврядування у кризових ситуаціях?» Аргументи «за» і «проти».

Практичне завдання: скласти схему взаємодії між поліцією, кіберцентром Держспецзв'язку та урядовим фельд'єгерським зв'язком у випадку кібератаки на критичну інфраструктуру (наприклад, енергосистему).

Обговорення: які обмеження та виклики пов'язані з користуванням радіочастотним ресурсом України правоохоронними органами (приклади – втручання сторонніх осіб, потреба у резервуванні каналів)?

Зміст самостійної роботи здобувачів:

Базова самостійна робота: вивчення матеріалів лекції і додаткових джерел про системи зв'язку; складання словника основних термінів (не менше 10) з коротким поясненням своїми словами – наприклад, “Транкінгова система – ...; Повнодуплексний зв'язок – ...; Енд-то-енд шифрування – ...”; ознайомлення з національними нормативами щодо організації зв'язку в підрозділах (накази чи інструкції МВС, якщо доступні публічно) – законспектувати структуру позивних, канали, порядок ведення переговорів.

Додаткова самостійна робота: підготовка повідомлення про міжнародний досвід організації системи зв'язку поліції; “Як працює американська мережа FirstNet” – знайти інформацію в інтернеті (статті, офіційні сайти) і зробити короткий огляд основних характеристик, акцентуючи, як вирішено питання пріоритетів і стійкості; проведення малого дослідження у формі інтерв'ю (якщо є знайомі поліцейські зв'язківці чи диспетчери) – розпитати про їх роботу, які проблеми зі зв'язком виникають найчастіше, як вони їх вирішують

Актуальні проблеми кримінального права та процесу»:

Найменування видів робіт	Розподіл годин за формами навчання	
	денна	заочна
Самостійна робота, год, зокрема:	60	82
Опрацювання матеріалу, викладеного на лекціях	10	10
Підготовка до практичних занять та контрольних заходів	10	15
Виконання індивідуальних практичних робіт	10	15
Підготовка до поточного контролю	15	17
Опрацювання матеріалу, винесеного на самостійне вивчення	15	25

ПОЛІТИКА КУРСУ

1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з «Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти». Ознайомитись з документом можна за [покликанням](#).



2) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за [покликанням](#).



3) щодо відпрацювання пропущених занять

Згідно “Положення про організацію освітнього процесу” здобувач допускається до семестрового контролю з конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом / робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥ 35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за [покликанням](#).



4) щодо дотримання академічної доброчесності

“Положення про академічну доброчесність” закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за [покликанням](#).



5) щодо використання штучного інтелекту

“Положення про академічну доброчесність” визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за [покликанням](#). “Положення про систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів” містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за [покликанням](#).



6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анулюється без права перескладання.

Ознайомитись з відповідним документом можна за [посиланням](#).

Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.



7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за [покликанням](#).



МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця.

Програмний результат навчання	Метод навчання	Метод оцінювання
Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефахівців; зокрема, під час публічних виступів, дискусій, проведення занять.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний	іспит, поточний контроль, усний контроль,

	методи, метод самостійної роботи вдома, робота під керівництвом викладача	письмовий контроль, тестовий контроль
Оцінювати та забезпечувати якість виконуваних робіт у процесі управління правоохоронним підрозділом в різних умовах обстановки, а також розробляти відповідні аналітичні та інформаційні матеріали, робити усні та письмові звіти та доповіді.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Розробляти та кваліфіковано застосовувати нормативно-правові акти в різних сферах юридичної діяльності, реалізовувати норми матеріального й процесуального	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль

права в професійній діяльності.		
Надавати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль
Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію.	словесні, наочні, практичні методи, індуктивний, дедуктивний, аналітичний, порівняння, узагальнення, конкретизація, дослідницький, інтерактивний методи, метод самостійної роботи вдома, робота під керівництвом викладача	іспит, поточний контроль, усний контроль, письмовий контроль, тестовий контроль

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Вид контрольного заходу	Зміст	% від загальної оцінки	Бал	
			min	max
Поточні контрольні заходи	опитування, поточні контрольні роботи, практичні завдання, результати виконання індивідуальної роботи	60	35	60
Підсумкові контрольні заходи	екзамен	40	24	40
Усього:		100	60	100

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів.

Фіксація **поточного** контролю здійснюється в електронному журналі обліку успішності академічної групи на підставі чотирибальної шкали («2»; «3»; «4»; «5»). У разі відсутності студента на занятті виставляється «н». За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Усі пропущені заняття, а також негативні оцінки здобувачі зобов'язані відпрацювати впродовж трьох наступних тижнів. У разі недотримання цієї норми, замість «н» у журналі виставляється «0» (нуль балів), без права перескладання. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».

Порядок оцінювання. До підсумкового контролю допускаються студенти, які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен / диференційований залік і повинні йти на перездачу.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно зі Шкалою оцінювання знань за ЄКТС) і є сумою балів отриманих під час поточного та підсумкового контролю.

Шкала оцінювання знань за ЄКТС

Оцінка за національною шкалою	Рівень досягнень, %	Шкала ECTS
Національна диференційована шкала		
Відмінно	90 – 100	A
Добре	83 – 89	B
	75 – 82	C
Задовільно	67 – 74	D
	60 – 66	E
Незадовільно	35 – 59	FX
	0 – 34	F
Національна недиференційована шкала		
Зараховано	60 – 100	-
Не зараховано	0 – 59	-

Студенти, які не з'явилися на заліки / екзамени без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основні джерела

1. Користін О.Є., Швець Д.В., Бутко Б.О. та ін. Реалізація філософії “Intelligence-Led Policing” в системі кримінального аналізу Національної поліції України: монографія / за заг. ред. О.Є. Користіна. – Київ: ВАІТЕ, 2024. – 444 с. – ISBN 978-966-2310-66-5. – DOI: 10.36486/978-966-2310-66-5. – URL: https://vaite.kiev.ua/doi/ilp/INTELLIGENCE-LED_POLICING_sfs.pdf .
2. Huber N. D. Intelligence-Led Policing for Law Enforcement Managers // FBI Law Enforcement Bulletin, October 10, 2019. – URL: <https://leb.fbi.gov/articles/featured-articles/intelligence-led-policing-for-law-enforcement-managers> .
3. Clarke R. V., Eck J. E. Crime Analysis for Problem Solvers in 60 Small Steps. – Washington, DC: Office of Community Oriented Policing Services, U.S. DOJ, 2005. – 148 p. – URL: <https://popcenter.asu.edu/content/crime-analysis-problem-solvers-60-small-steps>
4. Карчевський М.В. CrimeDataLab – інформаційно-аналітична платформа відкритих даних щодо протидії злочинності в Україні. <https://crimedatalab.org/>
5. Карчевський М.В. IFSafeLab – інтерактивна карта концентрації ДТП на дорогах Прикарпаття. <https://crimedatalab.shinyapps.io/IFSafeLab/>

Додаткові джерела

До теми 1. Поліцейська діяльність, керована даними

1. Удо Моллер. Правоохоронна діяльність, керована аналітикою: передова методика сучасної правоохоронної діяльності. EUAM Ukraine, 23.02.2017. URL: <https://www.euam-ukraine.eu/ua/news/opinion/intelligence-led-policing-the-cutting-edge-of-modern-law-enforcement/>
2. Міськів Д.М., Федчак І.А. Щодо взаємозв'язку моделі Problem-Oriented Policing з іншими проактивними моделями правоохоронної діяльності. Галицькі студії: юридичні науки. 2024. № 6. С. 33–40. DOI: 10.32782/galician_studies/law-2024-6-4. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/8201>

До теми 2. Кримінальний аналіз

1. Шинкаренко І.Р. Проблеми запровадження кримінального аналізу в діяльність підрозділів кримінальної поліції: теоретико-історичне підґрунтя. Науковий вісник ДДУВС. 2017. № 1. С. 233–242. URL: <https://er.dduvs.edu.ua/handle/123456789/125>

2. Гончарук О.М. Основні компоненти забезпечення ефективної діяльності підрозділів кримінального аналізу Національної поліції України. Науковий вісник УжНУ. Серія «Право». 2025. Вип. 88, ч. 2. С. 355–363. DOI: 10.24144/2307-3322.2025.88.2.48. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/05/50-1.pdf>

До теми 3. Інформаційні системи МВС

1. Фещенко І. ARMOR, «Оберіг» і «Гарпун»: що треба знати про інформаційні бази МВС. Informator.ua, 15.04.2024. URL: <https://informator.ua/uk/armor-oberig-i-garpun-shcho-treba-znati-pro-informaiyni-bazi-mvs-i-chi-mozhna-samostiyno-pereviriti-svoji-dani-v-nih>

2. Корнієнко М.В. Кримінальний аналіз у діяльності Національної поліції України. Право і суспільство. 2024. № 1(2). С. 397–402. URL: http://pravoisuspilstvo.org.ua/archive/2024/1_2024/part_2/62.pdf

До теми 4. Blockchain-аналітика у правоохоронній діяльності

1. Носов В.В., Манжай І.А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. Право і безпека. 2021. № 1(80). С. 93–100. URL: <https://dspace.univd.edu.ua/entities/publication/e6c8c349-e12d-4f26-a4fc-9b424db639e8>

2. Кіберполіція України. Співпраця з компанією Crystal Blockchain для протидії шахрайству з віртуальними активами. 2022. URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-u-spivpraczi-z-kompaniyeyu-crystal-blockchain-efektyvno-protydiye-shaxrajstvu-z-vykorystannyam-virtualnyx-aktyviv-205/>

3. Chainalysis Team. 2023 Crypto Crime Trends: Illicit Cryptocurrency Volumes Reach All-Time Highs. – Chainalysis Blog, 12.01.2023. – URL: <https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/> (дата звернення: 22.09.2025).

4. Bitfury Group. Bitfury Launches Crystal – A Blockchain Investigative Tool for Law Enforcement and Financial Institutions (Press Release). – 30.01.2018. – URL: https://bitfury.com/content/downloads/1_30_2018_bitfury_releases_crystal.pdf

До теми 5. ІІІ для прогнозів та аналітики

1. Зачек О.І., Дмитрик Ю.І., Сеник В.В. Роль штучного інтелекту в підвищенні ефективності правоохоронної діяльності. Науковий вісник ЛьвДУВС. 2023. № 3. С. 148–156. DOI: 10.32782/2311-8040/2023-3-19. URL: <http://journals.lvduvs.lviv.ua/index.php/law/article/view/637>

2. Баловсяк Н. Алгоритми правосуддя: як поліцейські та слідчі використовують штучний інтелект. DSnews.ua, 30.11.2024. URL: <https://www.dsnews.ua/ukr/society/algoritmi-pravosuddya-yak-policeyski-ta-slidchi-vikoristovuyut-shtuchniy-intelekt-30112024-512565>

3. Карчевський М. В., Куковинець Д. О. Використання технологій штучного інтелекту правоохоронними та судовими органами: світовий досвід та напрями розвитку національного законодавства. Питання боротьби зі злочинністю: зб. наук. пр. / редкол.: В. С. Батиргарєєва (голов. ред.) та ін. Харків: Право. 2023. Вип. 46. С. 21-31. <http://pbz.nlu.edu.ua/article/view/301290/293453>

4. Карчевський М. В. Штучний інтелект та протидія злочинності // Використання технологій штучного інтелекту у протидії злочинності : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). – Харків : Право, 2020. С.32-44 https://ivpz.kh.ua/wp-content/uploads/2020/12/%D0%9C%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D0%B8-%D1%81%D0%B5%D0%BC%D1%96%D0%BD%D0%B0%D1%80%D1%83_%D0%92%D0%B8%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-%D1%82%D0%B5%D1%85%D0%BD-%D1%88%D1%82%D1%83%D1%87%D0%BD%D0%BE%D0%B3%D0%BE-%D1%96%D0%BD%D1%82%D0%B5%D0%BB_5.11.2020.pdf

5. Osborne Clarke LLP. Facial recognition and data protection: new guidelines in the EU. – Osborne Clarke Insights, 21.06.2021. – URL: <https://www.osborneclarke.com/insights/facial-recognition-and-data-protection-new-guidelines-european-union> (дата звернення: 22.09.2025).

6. Tang J., Hiebert K. The Promises and Perils of Predictive Policing. – Centre for International Governance Innovation (CIGI), 22 May 2025. – URL: <https://www.cigionline.org/articles/the-promises-and-perils-of-predictive-policing/>

До теми 6. Стандарти ЄС щодо персональних даних

1. Різенко О.В. Європейські правові стандарти захисту персональних даних. Актуальні проблеми правознавства. 2024. № 6. С. 105–112. DOI: 10.24144/2788-6018.2024.06.105. URL: <https://app-journal.in.ua/wp-content/uploads/2024/12/107.pdf>

2. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities... – EUR-Lex, 2016. – URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680&qid=1758566580875> : .

До теми 7. Аналітичні можливості Google Sheets та Looker

1. Старк С. Як імпортувати та обробляти дані за допомогою Google Spreadsheets. Inweb, 12.11.2024. URL: <https://theinweb.media/google-spreadsheets-import-parse-data/>
2. Netpeak Blog. Як об'єднати декілька джерел даних у Google Looker Studio. 2022.URL: <https://netpeak.net/uk/blog/yak-ob-ednati-dzherela-danikh-u-google-looker-studio/>

До теми 8. Системи зв'язку у правоохоронній діяльності

1. Мирошниченко В.О., Прокопов С.О., Рижков Е.В. Впровадження сучасних систем цифрового радіозв'язку у підрозділах Національної поліції: наук.-практ. рекомендації. Дніпро: ДДУВС, 2021. 28 с. URL: <https://er.dduvs.edu.ua/handle/123456789/6956>
2. Міністерство внутрішніх справ України. Єдина багатозонава система цифрового радіозв'язку (ЄБСЦР). 2021. URL: <https://mvs.gov.ua/informatizaciia-sistemi-mvs/jedina-bagatozonova-sistema-cifrovogo-radiozviazku>
3. Фокус.ua. «Секретний» зв'язок для армії і поліції зламали за хвилину. Фокус, 27.07.2023. URL: https://focus.ua/uk/digital/581147-shpionazh-ne-budet-prezhnim-sverhsekretnuyu-svyaz-dlya-voennyh-i-politikov-vzломali-za-minutu#goog_rewarded
4. Sierra Wireless (Semtech). European Police Organization Consolidates Emergency Communications System on TETRA Network (Danish National Police Case Study). – Customer Stories, [б.п.]. – URL: <https://www.sierrawireless.com/resources/customer-stories/danish-national-police/>