Міністерство освіти і науки України
Національний університет водного господарства та природокористування

Навчально-науковий інститут права та гуманітарних наук
Кафедра правоохоронної діяльності та спеціальних юридичних дисциплін

08-01-05М

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять та самостійної роботи
з освітньої компоненти
«*Інформаційні системи та інформаційне забезпечення правоохоронної діяльності»*
для здобувачів вищої освіти другого (магістерського) рівня
за освітньо-професійною програмою «Правоохоронна діяльність» спеціальності К9 «Правоохоронна діяльність»
денної/заочної форми навчання

Рекомендовано
науково-методичною радою з якості
навчально-наукового інституту
права та гуманітарних наук
Протокол № 07 від 06.03.2026 р.

Рівне – 2026

Методичні вказівки до практичних занять та самостійної роботи з освітньої компоненти «*Інформаційні системи та інформаційне забезпечення правоохоронної діяльності*» для здобувачів вищої освіти другого (магістерського) рівня за освітньо-професійною програмою «Правоохоронна діяльність" спеціальності К9 "Правоохоронна діяльність» галузі знань К «Безпека та оборона» денної/заочної форми навчання [Електронне видання] / Цимбалюк В. І., Багатко А. С. – Рівне : НУВГП, 2026. – 48 с.

Укладачі: Цимбалюк В. І, .к.ю.н., професор кафедри правоохоронної діяльності та спеціальних юридичних дисциплін; Багатко А. С., асистент кафедри інформаційного права та юридичної журналістики.

Відповідальні за випуск: *Гришко Вікторія Іванівна*, к.пед.н., доцент, в.о. завідувача кафедри правоохоронної діяльності та спеціальних юридичних дисциплін.

Керівник групи забезпечення спеціальності К9
«Правоохоронна діяльність» Рогозіннікова К. С.

ЗМІСТ

Передмова

Шановні студенти!

Метою викладання навчальної дисципліни «Інформаційні системи та інформаційне забезпечення правоохоронної діяльності» є формування у здобувачів вищої освіти другого (магістерського) рівня системних знань про інформаційні системи правоохоронних органів, сучасні цифрові технології у кримінальному процесі та оперативно-службовій діяльності, а також набуття практичних навичок використання інформаційних ресурсів, баз даних і цифрових інструментів для забезпечення ефективного розслідування правопорушень, аналізу ризиків та прийняття обґрунтованих управлінських рішень.

Сьогодні правоохоронна діяльність нерозривно пов'язана з використанням сучасних цифрових технологій, автоматизованих баз даних, інформаційно-аналітичних ресурсів та електронного документообігу. Ефективність прийняття управлінських і процесуальних рішень значною мірою залежить від повноти, достовірності та своєчасності отриманої інформації, а також від уміння правильно її аналізувати й використовувати в межах чинного законодавства.

У процесі вивчення дисципліни студенти ознайомляться з принципами побудови та функціонування інформаційних систем, правовими засадами обігу інформації, особливостями інформаційно-аналітичного забезпечення правоохоронної діяльності, а також питаннями захисту інформації та забезпечення інформаційної безпеки. Значна увага приділяється практичним аспектам роботи з інформаційними ресурсами, формуванню навичок критичного аналізу даних та відповідального ставлення до використання інформації.

Методичні вказівки підготовлено з метою надання допомоги студентам у підготовці до практичних занять, виконанні індивідуальних завдань і самостійної роботи.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ТА ЇЇ СТРУКТУРА

1.1. **Опис навчальної дисципліни**

Мета навчальної дисципліни полягає у формуванні у здобувачів вищої освіти другого (магістерського) рівня системних знань про інформаційні системи правоохоронних органів, сучасні цифрові технології у кримінальному процесі та оперативно-службовій діяльності, а також у набутті практичних навичок використання інформаційних ресурсів, баз даних і цифрових інструментів для забезпечення ефективного розслідування правопорушень, здійснення аналітичної роботи, оцінки ризиків та прийняття обґрунтованих управлінських рішень в умовах цифрової трансформації суспільства.

Завдання навчальної дисципліни:

1. Ознайомлення здобувачів з організаційними та правовими засадами функціонування інформаційних систем МВС України та інших правоохоронних органів;
2. Формування знань щодо використання автоматизованих систем, спеціальних баз даних і міжвідомчих інформаційних ресурсів у кримінальному провадженні та оперативно-розшуковій діяльності;
3. Розвиток практичних умінь застосовувати OSINT-інструменти, цифрову криміналістику та методи роботи з електронними доказами;
4. Формування навичок забезпечення цілісності, допустимості та належного документування цифрової інформації відповідно до вимог процесуального законодавства;
5. Розвиток компетентностей щодо захисту персональних даних, безпечної роботи з інформаційними ресурсами, а також використання сучасних аналітичних підходів і технологій прогнозування у правоохоронній діяльності.

Компетентності:

ІК. Здатність розв’язувати складні задачі і проблеми у сфері правоохоронної діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК3. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК10. Здатність оцінювати та забезпечувати якість виконуваних робіт.
СК10. Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час рішення 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.

Програмні результати навчання (ПРН). Результати навчання (РН)

РН7. Давати короткий правовий висновок щодо окремих фактичних обставин з достатньою обґрунтованістю.
РН9. Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення.
РН10. 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.

РН13. Знати та розуміти особливості реалізації та застосування норм матеріального і процесуального права.
РН15. Вільно використовувати для правничої діяльності доступні інформаційні технології і бази даних.
РН16. Використовувати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань.
РН17. 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 оперативно-розшукової діяльності).
РН19. Аналізувати обстановку, рівень потенційних загроз та викликів, прогнозувати розвиток дій правопорушників, вживати заходів з метою запобігання, виявлення та припинення правопорушень

1.2. Тематика практичних занять

		Кількість годин

№ п\п	Назва теми	лекції		практичні	
		денна форма	заочна форма	денна форма	заочна форма
МОДУЛЬ 1. Інформаційні системи та інформаційно-пошукове забезпечення правоохоронної діяльності					
1.	Інформаційні системи МВС України та ЄІС: структура, функції, взаємодія.	2	1	2	1
2.	Автоматизовані системи та спеціальні бази даних у розслідуванні злочинів	2	-	2	-
3.	Єдина база розшуку осіб та міжвідомчий/міжнародний розшук	2	-	2	1
4.	OSINT у правоохоронній діяльності: технології, методика, правові межі	2	-	2	1
МОДУЛЬ 2. Технологічні та правові засади протидії кіберзлочинності в умовах цифрової трансформації					
5.	Кіберзлочинність і цифрова криміналістика: інструменти та методи розслідування	2	-	2	1
6.	Аналітика великих даних (Big Data) у прогнозуванні злочинності та управлінні безпекою	2	1	2	1
7.	Відеоспостереження, відеоаналітика та ГІС у профілактиці і реагуванні	2	-	1	-
8.	Захист персональних даних і штучний інтелект у правоохоронній діяльності: безпека, етика, прогнозування	2	-	1	1

1.3. Контрольні заходи та засоби діагностики

Поточний контроль знань здобувачів освіти з освітньої компоненти проводиться у формах:

- усного опитування на практичних заняттях;
- оцінки за написання есе та участь в обговоренні проблемних питань;
- аналіз та складання правових документів;
- оцінка виконання індивідуального науково-дослідного завдання.

1.4. Критерії та шкала оцінювання

Основними критеріями, що характеризують рівень компетентності здобувача вищої освіти при оцінюванні результатів поточного контролю з освітньої компоненти "Оперативно-розшукові заходи та негласні слідчі (розшукові) дії" є:

- повнота і вчасність виконання всіх видів навчальної роботи, передбачених силабусом освітньої компоненти;
- глибина і характер знань навчального матеріалу за змістом освітньої компоненти, що міститься в основних та додаткових рекомендованих літературних джерелах;
- вміння аналізувати явища, що вивчаються, у їх взаємозв'язку і розвитку;
- характер відповідей на поставленні питання (чіткість, логічність, лаконічність, послідовність тощо);
- вміння застосовувати теоретичні положення під час розв'язання практичних занять;
- вміння аналізувати достовірність одержаних результатів.

Оцінювання результатів поточного контролю проводиться у розрахунку від 0 до 100 балів.

Основними методами оцінювання є:

- аналіз усних відповідей;
- виконання практичних завдань;
- аналіз та складання процесуальних документів;
- написання есе та тез.

Оцінювання виконання завдань здійснюється за такими критеріями (у % від кількості балів, виділених на завдання із заокругленими до цілого числа):

0% - завдання не виконано;

40% - завдання виконано частково, висновки не аргументовані і не конкретні, звіт підготовлено недбало;

60% - завдання виконано повністю, висновки містять окремі недоліки, судження здобувача освіти не достатньо аргументовані, звіт підготовлено з незначним відхиленням від вимог;

80% - завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки несистемного характеру;

100% - завдання виконано правильно, вчасно і без зауважень.

2. ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

МОДУЛЬ І. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ІНФОРМАЦІЙНО-ПОШУКОВЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

ТЕМА № 1. Інформаційні системи МВС України та ЄІС: структура, функції, взаємодія.

План лекції:

1. Загальна характеристика інформаційних систем МВС України.
2. Єдина інформаційна система МВС: структура, складові та принципи взаємодії.
3. Призначення та функціональні можливості підсистем (реєстри, бази даних, облік).
4. Інтеграція інформаційних ресурсів МВС з Національною поліцією, ДПСУ, СБУ, ДБР, органами прокуратури та іншими суб'єктами.
5. Доступ до інформаційних систем: рівні, обмеження, службові повноваження та відповідальність.
6. Проблеми впровадження та перспективи розвитку ІТ у системі МВС України.

Питання для семінарського заняття:

1. Що розуміють під поняттям інформаційних систем у діяльності МВС України?
2. Які основні завдання та функції інформаційних систем у правоохоронних органах?
3. Які нормативно-правові документи регламентують створення та використання інформаційних систем МВС?

4. Хто відповідає за адміністрування та контроль роботи інформаційних систем у МВС?
5. Які принципи формування і ведення інформаційних ресурсів у системах МВС?
6. Яка структура Єдиної інформаційної системи МВС та які її основні підсистеми?
7. Які види даних накопичуються та обробляються у ЄІС?
8. Як забезпечується збереження, достовірність та конфіденційність інформації в ЄІС?
9. Які механізми взаємодії інформаційних систем МВС з іншими державними органами існують?
10. Як МВС взаємодіє з міжнародними організаціями щодо обміну інформацією про злочинність?
11. Які переваги використання інформаційних систем у оперативно-розшуковій діяльності?
12. Яким чином інформаційні системи сприяють підвищенню ефективності розслідування кримінальних правопорушень?
13. Які сучасні цифрові технології зараз впроваджуються у роботу МВС (аналітичні платформи, Big Data, ШІ)?
14. Які ризики та проблеми виникають при використанні цифрових технологій у правоохоронній діяльності?
15. Які перспективи розвитку інформаційних систем МВС в умовах цифрової трансформації держави?

Завдання № 1

Ознайомтеся з описом основних підсистем Єдиної інформаційної системи МВС України. Визначте, які види інформації та бази даних використовуються для оперативно-розшукової діяльності, розслідування кримінальних правопорушень та аналітичної роботи. Проаналізуйте порядок взаємодії інформаційних систем МВС з іншими державними органами та міжнародними

структурами. Складіть таблицю або схему, що відображає: підсистеми ЄІС; види інформації, що обробляються; цілі використання. Визначте можливі переваги та обмеження інформаційних систем МВС у практичній діяльності правоохоронних органів. Підготуйте короткий висновок щодо того, які сучасні цифрові технології (аналітичні платформи, OSINT, Big Data) можна ефективно інтегрувати для підвищення ефективності роботи систем.

Завдання № 2

Створіть кейс у програмі Excel, який відображає використання підсистем Єдиної інформаційної системи МВС. Використайте таблицю з колонками: «Підсистема», «Вид інформації», «Результат використання», «Ризики/обмеження». Для кожної підсистеми заповніть приклади конкретних даних, які вона обробляє, та як ці дані допомагають у розслідуванні. Додайте результати використання інформації, наприклад для розшуку осіб, перевірки транспортних засобів або аналітики кримінальних ризиків. У колонці «Ризики/обмеження» вкажіть можливі проблеми, такі як обмежений доступ, технічні збої або затримка оновлення даних. Застосуйте умовне форматування, щоб виділити успішне використання системи зеленим, а потенційні ризики – червоним кольором. Створена таблиця повинна наочно показувати взаємозв’язок між підсистемами, інформацією та результатами розслідування. Опишіть коротко, як дані з різних підсистем інтегруються для досягнення оперативних цілей. Додайте примітки щодо можливого вдосконалення роботи систем за допомогою сучасних цифрових технологій. Підготуйте короткий висновок про ефективність та обмеження використання інформаційних систем МВС у практичній діяльності правоохоронців

ТЕМА № 2. Автоматизовані системи та спеціальні бази даних у розслідуванні злочинів

План лекції:

1. Види автоматизованих систем, що застосовуються у кримінальному процесі та правоохоронній діяльності.
2. Системи обліку й аналізу злочинів (зокрема ІАС типу «Армор») та їх значення для оперативного реагування і розслідування.
3. Спеціальні бази даних: облік зброї, транспортних засобів, номерних знаків та інших об’єктів.
4. Біометричні системи ідентифікації: фотооблік, дактилоскопічні бази, ДНК-реєстри.
5. Методи пошуку, зіставлення та встановлення аналітичних зв’язків між інформаційними масивами.
6. Автоматизація процесів документування, аналізу та формування інформаційно-аналітичних матеріалів у кримінальних провадженнях.

Питання для семінарського заняття:

1. Що розуміють під поняттям автоматизованих систем у діяльності правоохоронних органів?
2. Які основні завдання автоматизованих систем у розслідуванні злочинів?
3. Які види спеціальних баз даних використовуються для збору та обробки інформації?
4. Як функціонують підсистеми для обліку осіб, транспортних засобів та речових доказів?
5. Яким чином автоматизовані системи допомагають у оперативно-розшуковій діяльності?
6. Які переваги використання спеціальних баз даних у порівнянні з традиційними методами обліку?

7. Як забезпечується достовірність та актуальність інформації у базах даних?
8. Які механізми взаємодії існують між автоматизованими системами та іншими державними органами?
9. Як міжнародні структури (INTERPOL, Europol) взаємодіють з автоматизованими системами МВС України?
10. Які технічні обмеження та ризики виникають при використанні автоматизованих систем?
11. Які правові та етичні аспекти слід враховувати під час роботи з базами даних?
12. Як сучасні цифрові технології (Big Data, OSINT, аналітичні платформи) можуть покращити роботу систем?
13. Наведіть приклади практичного застосування автоматизованих систем у розслідуванні кримінальних правопорушень.
14. Які проблеми можуть виникнути при інтеграції різних підсистем між собою?
15. Які перспективи розвитку та вдосконалення автоматизованих систем у діяльності МВС?

Завдання № 1

Створіть інтерактивний кейс розслідування злочину, наприклад, викрадення автомобіля або шахрайство онлайн. Використайте PowerPoint або Canva для побудови послідовності дій слідчого у вигляді слайдів або блок-схеми. На кожному кроці вкажіть, яку автоматизовану систему або базу даних використовує слідчий. Позначте, яку інформацію отримуєте від кожної системи та як вона допомагає просунути розслідування. Виділіть ризики та обмеження кожного етапу, наприклад, затримку оновлення даних або обмежений доступ. Додайте колонку або блок «Цифрові інструменти», де зазначте Big Data, OSINT, аналітичні платформи чи ГІС. Використайте кольорове кодування: зеленим – успішні дії, червоним – проблемні або ризикові моменти. Створіть гіперпосилання або навігацію між кроками, щоб демонструвати логіку розслідування у вигляді інтерактивної презентації.
Напишіть нотатки під кожним кроком: що зроблено, який результат

та можливі наслідки. Підготуйте висновок про ефективність автоматизованих систем і пропозиції щодо вдосконалення процесу розслідування.

Завдання № 2

Створіть порівняльну інфографіку в Easel.ly. Розділіть її на три частини: ліва колонка – «Старі методи», права колонка – «Автоматизовані системи», а центр – ключова проблема. У лівій колонці покажіть традиційні способи роботи: картотеки, фототаблиці в альбомах, поштові запити.
У правій колонці відобразіть сучасні цифрові рішення: біометрична ідентифікація, хмарні бази даних, миттєвий обмін інформацією з Interpol. Підкресліть різницю у швидкості обробки інформації та доступності даних між старими та новими методами. У центрі вкажіть головну проблему, яку не вирішила навіть автоматизація, наприклад, людський фактор або кіберзлочинність. Додайте графічні елементи: іконки, стрілки, кольорові блоки, щоб порівняння було наочним. Використайте кольори для виділення: червоний – проблеми, зелений – переваги, синій – нейтральні дані.

ТЕМА № 3. Єдина база розшуку осіб та міжвідомчий/міжнародний розшук

План лекції:

1. Правова основа функціонування єдиної інформаційної бази розшуку осіб та її значення для забезпечення правоохоронної діяльності.
2. Підстави й критерії внесення особи до розшуку, порядок формування, ведення та актуалізації облікових даних.

3. Суб'єкти, відповідальні за наповнення та оновлення інформації, а також механізми міжвідомчої взаємодії й обміну даними.

4. Інтеграція національних ресурсів з міжнародними каналами розшуку (Інтерпол, Європол та ін.).

5. Порядок доступу до бази, отримання витягів, межі повноважень та юридична відповідальність за неправомірне використання інформації.

6. Проблемні питання: помилки, дублювання даних, ризики порушення прав людини та гарантії захисту персональної інформації.

Питання для семінарського заняття:

1. Що таке Єдина база розшуку осіб і для чого вона призначена?
2. Які основні завдання виконують правоохоронці за допомогою бази розшуку?
3. Які види розшуку передбачені в діяльності МВС (кримінальний, адміністративний, міжнародний)?
4. Який порядок внесення та актуалізації даних у базу?
5. Як підрозділи МВС взаємодіють між собою при використанні бази розшуку?
6. Які державні органи взаємодіють між собою у межах міжвідомчого розшуку?
7. Як відбувається обмін інформацією з міжнародними структурами, такими як INTERPOL і Europol?
8. Які правові та процедурні норми регулюють міжнародний обмін інформацією про розшук осіб?
9. Які цифрові інструменти використовуються для підвищення ефективності розшуку?
10. Як автоматизація скорочує час на пошук та підвищує точність даних?
11. Які обмеження та ризики пов'язані з використанням Єдиної бази розшуку?

12. Як інтеграція з Єдиною інформаційною системою МВС допомагає у комплексному аналізі даних?
13. Наведіть приклади практичного застосування бази у реальних розслідуваннях.
14. Які заходи забезпечують безпеку та конфіденційність інформації у базі?
15. Які перспективи розвитку та вдосконалення Єдиної бази розшуку можна передбачити в умовах цифровізації МВС?

Завдання № 1

Відкрийте Genially і оберіть шаблон для інтерактивного тесту або квізу, дайте назву «Єдина база розшуку осіб» створіть 10–12 запитань різного формату: вибір однієї або кількох правильних відповідей, відповідність, «так/ні», наприклад, призначення Єдиної бази розшуку, види розшуку (кримінальний, адміністративний, міжнародний), міжнародна взаємодія з INTERPOL та Europol, цифрові інструменти для прискорення розшуку (OSINT, аналітичні платформи), ризики та обмеження використання бази; додайте візуальні елементи: піктограми, графіки, ілюстрації комп'ютерів, глобуса чи документів; після вибору відповіді користувач отримує коротке пояснення, чому правильна відповідь вірна, а чому інші – ні; можна додати сценарії практичного застосування, наприклад: «що робити, якщо особу внесено до міжнародного розшуку»; використовуйте кольори для виділення результатів: зелений – правильна відповідь, червоний – неправильна, синій – додаткова інформація; наприкінці створіть підсумковий слайд, де будете бачити свій результат і короткий коментар про ефективність використання бази розшуку в практичній діяльності.

Завдання № 2

Відкрийте Google My Maps або ArcGIS Online і створіть нову карту, назвіть її «Єдина база розшуку: національні та міжнародні кейси», створіть точки на карті для різних категорій розшуку: кримінальний, адміністративний та міжнародний, для кожної точки додайте поп-ап з інформацією про тип розшуку, використані цифрові інструменти та приклад реальної або умовної справи, позначте міжнародні кейси синім кольором, національні – зеленим, проблемні – червоним, додайте лінії зв'язку між точками для демонстрації взаємодії підрозділів МВС та міжнародних структур (INTERPOL, Europol), використайте іконки та символи для наочності (людина – розшукана особа, глобус – міжнародний обмін інформацією, комп'ютер – цифрові інструменти), створіть легенду карти для розуміння кольорів та символів, додайте кнопку або шар «Висновки», де описані переваги та обмеження використання бази та цифрових інструментів, і підготуйте короткий звіт або презентацію, що пояснює логіку створення карти та як вона підвищує ефективність розшуку осіб.

ТЕМА № 4. OSINT у правоохоронній діяльності: технології, методика, правові межі

План лекції:

1. Поняття OSINT (Open Source Intelligence), його переваги та обмеження у правоохоронній діяльності.
2. Основні інструменти збору інформації: пошукові системи, соціальні мережі, відкриті реєстри та бази даних.
3. Методи збору, обробки та верифікації інформації для забезпечення достовірності та актуальності даних.

4. Законність і допустимість результатів OSINT у кримінальних провадженнях та оперативно-розшуковій діяльності.
5.Використання OSINT для протидії дезінформації, кіберзагрозам та інформаційній війні.

Питання для семінарського заняття:

1. Що таке OSINT і чим він відрізняється від інших методів збору інформації у правоохоронній діяльності?
2. Які основні види відкритих джерел інформації можна використовувати для розслідувань?
3. Яким чином пошукові системи та соціальні мережі допомагають у зборі доказів? Наведіть приклади.
4. Які переваги та обмеження використання OSINT у кримінальних і адміністративних справах?
5. Як OSINT може бути ефективним інструментом для виявлення кіберзагроз та злочинних схем?
6. Які основні етапи проведення OSINT-розслідування?
7. Як перевіряти достовірність та надійність інформації, отриманої з відкритих джерел?
8. Які законодавчі норми обмежують використання OSINT у правоохоронній практиці?
9. Як забезпечити баланс між ефективністю розслідування та дотриманням прав людини та конфіденційності?
10.Наведіть приклади ситуацій, коли неправомірне використання OSINT могло б призвести до відповідальності.

Завдання № 1

Проаналізуйте діяльність Instagram-магазину, підозрюваного у продажі неіснуючих товарів за передоплатою: встановіть зміни назв акаунту, використовуйте Google Lens для перевірки зображень на плагіат, проаналізуйте коментарі та знайдені номери банківських карток, перевірте телефон через GetContact, визначте автоматизовані позитивні відгуки, сформуйте цифрові сліди (скриншоти, посилання, номери рахунків) як первинну доказову базу, врахуйте правові та етичні обмеження,

запропонуйте подальші процесуальні дії та оформіть письмовий звіт із описом методів збору, перевірки достовірності та рекомендаціями щодо легалізації даних для суду.

Завдання № 2

До вашого підрозділу надійшло повідомлення про акаунт у соціальній мережі, який пропонує інвестиційні послуги з високим прибутком, але викликає підозру на шахрайство. Використовуючи OSINT, виконайте наступні кроки:

1. Ідентифікуйте акаунт та пов'язані з ним сторінки або групи.
2. Проаналізуйте публікації, коментарі та взаємодію з іншими користувачами для виявлення підозрілих схем.
3. Перевірте наявність контактних даних (телефони, пошти, сайти) і оцініть їх достовірність за допомогою відкритих інструментів.
4. Визначте потенційні цифрові сліди: скриншоти публікацій, посилання на акаунти, доменні імена сайтів.
5. Оцініть ризики та законність подальших дій, враховуючи захист персональних даних та етичні обмеження.
6. Складіть звіт із описом методів збору та аналізу даних, оцінкою достовірності та рекомендаціями щодо можливих процесуальних дій.

Завдання № 3

До вашого підрозділу надійшло повідомлення про акаунт у соціальній мережі, який поширює інформацію про вигідні фінансові пропозиції, але ймовірно використовує фейкові відгуки та маніпуляції. Використовуючи OSINT, виконайте такі дії:

1. Визначте акаунти, пов'язані з підозрілою діяльністю, та перевірте наявність їхніх альтернативних профілів.
2. Проаналізуйте публікації, коментарі та взаємодії з іншими користувачами на наявність ознак автоматизованих ботів або фейкових відгуків.

3. Перевірте зображення та відео на плагіат, використовуючи інструменти перевірки (Google Lens, TinEye тощо).
4. Визначте цифрові сліди: посилання на акаунти, сайти, контактні дані, доменні імена.
5. Оцініть ризики і законність збору інформації, враховуючи захист персональних даних та етичні норми.
6. Складіть звіт із описом методів збору та перевірки інформації, результатами аналізу та рекомендаціями щодо подальших процесуальних дій.

ТЕМА №5. Кіберзлочинність і цифрова криміналістика: інструменти та методи розслідування

План лекції

1. Класифікація кіберзлочинів та сучасні тенденції розвитку у сфері цифрової злочинності.
2. Інструменти цифрової криміналістики, зокрема програмні продукти EnCase, FTK та інші, для збору, аналізу та документування цифрових доказів.
3. Методи аналізу електронної пошти, веб-браузера, соціальних мереж та месенджерів.
4. Виявлення шкідливого програмного забезпечення, лог-аналіз і трасування джерел загроз.
5. Процедури деанонімізації у цифровому середовищі, оцінка ризиків, межі та законність таких дій.
6. Забезпечення цілісності та допустимості цифрових доказів (chain of custody).
7. Взаємодія з CERT та міжнародними структурами, порядок реагування на інциденти кібербезпеки.

Питання для семінарського заняття:

1. Що таке кіберзлочинність? Наведіть приклади найпоширеніших видів кіберзлочинів та їх наслідків.
2. Яка відповідальність за кіберзлочини передбачена законодавством України? Порівняйте з міжнародними нормами (Будапештська конвенція).
3. У чому полягає відмінність між цифровою криміналістикою та традиційною криміналістикою?
4. Що таке «ланцюг зберігання доказів» (Chain of Custody) і чому він є критично важливим у цифрових розслідуваннях?
5. Опишіть основні етапи цифрового розслідування. Які помилки на кожному етапі можуть призвести до втрати доказів?
6. Які інструменти використовуються для аналізу дискових носіїв, мережевого трафіку та оперативної пам'яті? У чому їх відмінності?
7. Як шифрування та анонімізація (VPN, Tor, Dark Web) ускладнюють роботу слідчих?
8. Яку роль відіграє штучний інтелект у сучасній цифровій криміналістиці — як інструмент злочинців і як інструмент слідства?
9. Наведіть приклади успішної міжнародної співпраці у розслідуванні кіберзлочинів.
10. Які, на вашу думку, є найбільші виклики для цифрової криміналістики найближчими роками?

Завдання № 1

До відділу кіберполіції надійшло повідомлення від керівництва приватної компанії «ТехноБізнес». З корпоративних серверів було викрадено конфіденційну базу

даних клієнтів (понад 50 000 записів), а на сайті компанії розміщено повідомлення з вимогою викупу в криптовалюті. Слідчий отримує цифровий образ жорсткого диска сервера, логи мережевого трафіку та скріншоти листування зловмисника.

Завдання**:**

1. **Група 1:** опишіть покроково свої дії на місці інциденту. Як правильно зафіксувати та вилучити цифрові докази, не порушивши їх цілісність? Складіть протокол вилучення.
2. **Група 2:** використовуючи інструменти Autopsy або Wireshark (або їх демо-версії), проаналізуйте надані дані. Визначте: коли стався злом, який шлях пройшов зловмисник у системі, які файли були скопійовані.
3. **Група 3 :** на основі отриманих даних складіть план розслідування. Які запити потрібно направити провайдерам? Чи є підстави для міжнародного запиту (якщо IP-адреса іноземна)?
4. **Група 4 :** оцініть зібрані докази з правової точки зору. Які статті КК України можуть бути застосовані? Чи достатньо доказів для обвинувачення?

Кожна група презентує свої висновки, після чого відбувається спільне обговорення — чи вдалося розкрити справу.

Завдання № 2

Співробітник державної установи отримав електронний лист нібито від «Державної податкової служби України» з вимогою терміново підтвердити свої дані, перейшовши за посиланням. Він перейшов за посиланням і ввів свої логін та пароль. Наступного дня виявилось, що з його робочого акаунту були надіслані сотні фішингових листів колегам, а частина службових документів зникла з хмарного сховища.

Завдання**:**

1. Група 1: проаналізуйте «заголовки» фішингового листа (надаються роздруківки з прикладом на практичному занятті). Визначте: справжня IP-адреса відправника, домен-підробка, ознаки соціальної інженерії у тексті листа.
2. Група 2: складіть план термінових дій після виявлення інциденту. Що робити в перші 30 хвилин? Як мінімізувати збитки та зупинити поширення фішингу всередині установи?
3. Група 3 : визначте, які цифрові сліди залишив зловмисник. Які дані необхідно запросити у поштового провайдера та хостингу фішингового сайту? Складіть відповідний запит.
4. Група 4: розробіть коротку інструкцію для працівників установи «Як розпізнати фішинговий лист». Представте її у вигляді пам'ятки на 5-7 пунктів.

- Чи міг би цей інцидент статися, якби в установі було впроваджено двофакторну автентифікацію? Обґрунтуйте відповідь.

  Кожна група презентує свої рішення, після чого спільно визначається — які помилки були допущені на кожному етапі і як їх уникнути в майбутньому.

ТЕМА №6. Аналітика великих даних (Big Data) у прогнозуванні злочинності та управлінні безпекою

План лекції

1. Поняття електронних доказів та цифрової інформації, їх значення у кримінальному провадженні.
2. Основні джерела цифрових доказів: комп’ютерні та мобільні пристрої, хмарні сервіси, соціальні мережі та інші онлайн-ресурси.
3. Правила збирання, копіювання, вилучення та документування електронних доказів із забезпеченням цілісності та недоторканності даних.

4. Аналіз судової практики щодо прийнятності та допустимості електронних доказів, типові помилки сторін у процесі розгляду.
5. Перспективи розвитку нормативної бази щодо регулювання збору, зберігання та використання цифрових доказів.

Питання для семінарського заняття:

1. Що таке Big Data і які її ключові характеристики за моделлю «5V»? Наведіть приклади джерел великих даних у сфері безпеки.
2. Які методи аналізу даних застосовуються у правоохоронній діяльності? У чому різниця між описовою та предиктивною аналітикою?
3. Що таке Crime Mapping і як геопросторовий аналіз допомагає у запобіганні злочинності? Наведіть конкретні приклади.
4. Як працюють системи предиктивної поліції (PredPol, HunchLab, ShotSpotter)? Які результати їх застосування у світі?
5. Які переваги та ризики використання систем розпізнавання облич у публічних місцях?
6. Що таке «розумне місто» (Smart City) і як технології Big Data інтегруються в систему громадської безпеки?
7. Які алгоритмічні упередження (bias) можуть виникати у системах предиктивної поліції? Наведіть реальні приклади дискримінації.
8. Як GDPR регулює використання великих даних у правоохоронній діяльності? Яке законодавство діє в Україні?
9. Де проходить межа між забезпеченням безпеки та порушенням права на приватність? Обґрунтуйте свою позицію.

10. Чи може Україна впровадити системи предиктивної аналітики злочинності? Які перешкоди та можливості для цього існують?

Завдання № 1

Аналітичний відділ Національної поліції України отримав масив даних за останні 2 роки з різних джерел: статистика викликів 102, дані з камер відеоспостереження, інформація з соціальних мереж, звіти патрульних. Завдання — виявити приховані закономірності та підготувати аналітичну доповідь для керівництва.

Завдання:

1. Група 1: визначте, які з наданих джерел даних є найціннішими і чому. Які дані є «брудними» (неповними, суперечливими) і як їх очистити? Застосуйте модель «5V» до кожного джерела.
2. Група 2: використовуючи надані таблиці з даними, знайдіть часові та географічні закономірності злочинів. Побудуйте графік динаміки злочинності по місяцях. Які фактори (погода, свята, події) впливають на сплески злочинності?
3. Група 3: проаналізуйте надані приклади публікацій з відкритих джерел. Які сигнали в соціальних мережах можуть вказувати на підготовку злочину? Де межа між моніторингом і стеженням?
4. Група 4: на основі висновків інших груп підготуйте коротку аналітичну доповідь для керівництва (5-7 слайдів або тез). Які рекомендації ви надасте щодо розподілу ресурсів поліції?

- Які ризики виникають, якщо алгоритм навчений на історичних даних, що відображають упереджене ставлення до певних соціальних груп?

Кожна група презентує свої висновки, після чого спільно обговорюється — наскільки Big Data може замінити традиційну оперативну роботу поліцейського.

Завдання № 2

Поліція великого міста планує встановити систему розпізнавання облич на 50 камерах у центрі міста та на вокзалах. База даних міститиме фото осіб, що перебувають у розшуку. Мер міста просить правоохоронців підготувати аналітичну доповідь — чи варто впроваджувати систему?

Завдання:

1. Група 1: опишіть як працює система розпізнавання облич. Який відсоток похибок є прийнятним?
2. Група 2: підготуйте аргументи «за» впровадження системи. Які злочини вона допоможе розкрити або попередити? Наведіть реальні приклади зі світової практики успішного застосування.
3. Група 3: підготуйте аргументи «проти». Які права громадян можуть бути порушені? Що показує досвід країн, де від таких систем відмовились або обмежили їх використання?
4. Група 4: чи відповідає впровадження такої системи вимогам GDPR та законодавству України? Які умови мають бути виконані для законного використання? Чи потрібна окрема законодавча база?

- Де проходить межа між безпекою та тотальним стеженням? Чи готове суспільство платити за безпеку своєю приватністю?

Усі групи беруть участь в голосуванні з обговоренням: впроваджувати систему чи ні, і за яких умов.

ТЕМА № 7. Відеоспостереження, відеоаналітика та ГІС у профілактиці і реагуванні

План лекції

1. Історія розвитку відеоспостереження, типи камер та їх технічні характеристики, аналогові vs IP-системи, принципи побудови міських систем відеоспостереження.
2. Типи систем відеоспостереження, їх призначення та особливості використання: стаціонарні, мобільні та дрони.
3. Методи розпізнавання облич і номерних знаків, принципи роботи систем та потенційні ризики при застосуванні.
4. Централізовані міські системи відеоконтролю та їх роль у забезпеченні громадської безпеки.
5. Використання геоінформаційних систем (ГІС) для аналізу злочинності, картографування «hot spots» та планування патрулювання.
6. Інтеграція ГІС із іншими інформаційними системами для ефективного розгортання сил поліції.
7. Питання конфіденційності, можливості витоків даних та правові обмеження при застосуванні систем відеоспостереження і ГІС.

Питання для семінарського заняття:

1. Які ключові етапи розвитку систем відеоспостереження та чим відрізняються аналогові системи від IP-систем?
2. Які типи камер використовуються у міських системах відеоспостереження та які їхні технічні характеристики впливають на ефективність моніторингу?
3. Що таке відеоаналітика та які завдання вона вирішує у забезпеченні громадської безпеки
4. Як працює автоматичне розпізнавання облич (FRT) та розпізнавання номерних знаків (LPR/ANPR), і в яких ситуаціях ці технології є найбільш корисними?
5. Яким чином аналіз натовпу та виявлення аномальної поведінки допомагає у профілактиці правопорушень?

6. Що таке ГІС і геопросторовий аналіз, і як їх використовують для картування злочинності (Crime Mapping)?
7. Як інтеграція ГІС з базами даних поліції покращує прийняття оперативних рішень?
8. Які переваги дають єдині ситуаційні центри (Command & Control Centers) та системи «розумного міста» у контексті безпеки?

9. Які виклики та обмеження існують при впровадженні відеоспостереження та відеоаналітики у великих містах?
10. Наведіть приклади використання ArcGIS або Google Maps Platform для моніторингу безпеки та аналізу криміногенної ситуації.

Завдання № 1

Ви — команда експертів, яку запросило керівництво середнього українського міста (300 000 мешканців). Місто отримало грант ЄС на розбудову інтегрованої системи безпеки. Бюджет — 5 млн євро. Завдання — розробити концепцію «розумної безпеки міста» з інтеграцією відеоспостереження, відеоаналітики та ГІС.

Завдання:

1. Група 1: розробіть схему розміщення камер відеоспостереження у місті. Скільки камер потрібно? Де пріоритетно розмістити — вокзали, ринки, парки, школи? Які технічні характеристики камер обрати для різних локацій? Скільки це коштує з бюджету?
2. Група 2: визначте, які модулі відеоаналітики необхідні місту. Чи потрібне розпізнавання облич? Система LPR/ANPR на в'їздах до міста? Виявлення аномальної поведінки на вокзалі? Обґрунтуйте вибір і вкажіть вартість.
3. Група 3: розробіть концепцію інтерактивної карти безпеки міста. Які шари даних вона має містити? Як інтегрувати дані з

камер, патрульних екіпажів та бази злочинів в єдину картину? Покажіть макет на схемі.
4. Група 4: опишіть як має працювати єдиний Command & Control Center міста. Скільки операторів потрібно? Як система реагує на виявлену загрозу в автоматичному режимі? Який протокол дій чергової зміни?

- Кожна група презентує свою частину, після чого всі разом збирають єдину концепцію та відповідають на питання— викладача та представників інших груп.

1. Що робити, якщо хакери зламають систему відеоспостереження?
2. Як система поводитиметься під час масових заворушень?
3. Чи не перевищує вартість обслуговування системи початковий бюджет через 3 роки?
4. Як захистити персональні дані мешканців міста?

Завдання № 2

О 14:47 у центрі міста скоєно збройний напад на інкасаторський автомобіль. Двоє озброєних осіб у масках вкрали 2 млн гривень і зникли. Очевидці повідомляють різні описи — плутанина, паніка. У вашому розпорядженні: записи з 12 міських камер відеоспостереження, система розпізнавання номерних знаків (LPR), ГІС-карта міста з маршрутами патрульних екіпажів та дані мобільних операторів про активні SIM-карти в радіусі 200 метрів від місця події.

Завдання:

1. Група 1: вам надано схему розташування 12 камер навколо місця події та часові мітки. Побудуйте «відеомаршрут» підозрюваних — де вони з'явились у кадрі, куди рухались, на якому транспорті втекли. Визначте «сліпі зони» — де камер не вистачає.

2. Група 2: система зафіксувала 847 автомобілів у зоні події між 14:30 і 15:10. Використовуючи надані фільтри (викрадені авто, авто в розшуку, підозріла поведінка — в'їзд і виїзд без зупинки), звузьте список до 5-7 підозрілих транспортних засобів. Обґрунтуйте вибір.
3. Група 3: на карті міста позначте місце події, відомі маршрути втечі, розташування патрульних екіпажів на момент інциденту та можливі місця переховування. Визначте оптимальні точки блокування доріг — де і коли їх треба було виставити щоб перехопити злочинців?
4. **Група 4:** на основі даних усіх груп складіть єдиний оперативний план переслідування. Які ресурси задіяти? Які запити направити негайно — до мобільних операторів, банків, сусідніх міст? Як організувати взаємодію між підрозділами в реальному часі?

ТЕМА №8 Захист персональних даних і штучний інтелект у правоохоронній діяльності: безпека, етика, прогнозування

План лекції

1. Принципи захисту персональних даних у правоохоронній діяльності та роль штучного інтелекту у забезпеченні безпеки й прогнозуванні криміногенних ситуацій.
2. Внутрішні політики та контроль доступу в правоохоронних органах, методи шифрування, резервного копіювання та аудиту доступу до інформаційних ресурсів.
3. Predictive policing: моделі, алгоритми та логіка прогнозування злочинності.
4. Використання Big Data для аналізу криміногенних ситуацій і прийняття рішень.
5. Проблеми дискримінації та упереджених алгоритмів, етичні виклики та законодавче регулювання застосування штучного інтелекту у сфері правоохоронної діяльності.

Питання для семінарського заняття:

1. Що таке персональні дані і які їх категорії існують у контексті правоохоронної діяльності? Які принципи їх законної обробки?
2. Яка різниця між загальним регулюванням GDPR та спеціальною Директивою ЄС 2016/680 щодо обробки даних поліцією? Як це впливає на Україну?
3. У яких сферах правоохоронної діяльності штучний інтелект вже застосовується сьогодні? Наведіть конкретні приклади з України та світу.
4. Що таке «упередженість алгоритму» (algorithmic bias) і як вона може призвести до дискримінації у правоохоронній практиці?
5. Які вимоги висуває EU AI Act до систем штучного інтелекту високого ризику у сфері правоохоронної діяльності?
6. Як забезпечити безпечне зберігання та обробку великих масивів персональних даних у системах ШІ? Які технічні та організаційні заходи необхідні?
7. Що таке «чорна скринька» (black box) у контексті ШІ і чому це є проблемою для кримінального судочинства?
8. Чи може алгоритм бути упередженим, якщо його розробники не мали дискримінаційних намірів? Обґрунтуйте відповідь на прикладі системи COMPAS.
9. Де проходить межа між законним використанням ШІ для забезпечення безпеки та порушенням права на приватність і презумпцію невинуватості?
10. Які механізми громадського та незалежного контролю за використанням ШІ у правоохоронній діяльності існують у світі і чи потрібні вони Україні?

Завдання № 1

Ваш підрозділ планує впровадити систему штучного інтелекту для прогнозування місць підвищеного ризику злочинності у місті. Система аналізує дані з камер відеоспостереження, соціальних мереж та державних баз даних.

Завдання:

1. Визначте, які типи персональних даних будуть оброблятися у системі (наприклад, обличчя, номери автомобілів, геолокація, контактні дані).
2. Оцініть потенційні ризики порушення конфіденційності та безпеки цих даних.
3. Запропонуйте методи захисту персональних даних (шифрування, обмеження доступу, анонімізація, аудит дій користувачів).

1. Розгляньте етичні питання використання ШІ: упередженість алгоритмів, дискримінація, баланс між ефективністю розслідування та правами людини.
2. Підготуйте звіт із описом ризиків, запропонованих заходів та рекомендаціями щодо безпечного і етичного використання системи ШІ у правоохоронній діяльності.

Завдання № 2

Ваш відділ бере участь у пілотному проєкті “розумного міста”, де ШІ аналізує дані з камер відеоспостереження, сенсорів, мобільних додатків та соціальних мереж для прогнозування ризиків злочинності та надзвичайних ситуацій.

Завдання:

1. Ідентифікуйте типи персональних даних, які будуть оброблятися системою (геолокація, відео, контактна інформація, дані про транспорт).
2. Визначте потенційні загрози конфіденційності та безпеки для мешканців міста.
3. Пропишіть правила та обмеження для використання ШІ: хто має доступ до даних, як обробляються результати, які дії заборонені.

4. Проведіть аналіз етичних аспектів: чи може алгоритм створювати упередження щодо окремих районів чи груп населення? Як уникнути дискримінації?
5. Сформуйте короткий план дій у разі виявлення критичних ризиків або порушення конфіденційності.
6. Оформіть звіт із описом аналізу даних, ризиків, запропонованих правил безпеки та рекомендацій щодо етичного застосування системи.

3. САМОСТІЙНА РОБОТА ЗДОБУВАЧІВ ОСВІТИ

Підготовка до семінарських занять допомагає глибше опанувати ключові теми освітньої компоненти «Інформаційні системи та інформаційне забезпечення правоохоронної діяльності», сформувати цілісне розуміння теоретичних положень і механізмів їх практичного застосування. У процесі обговорення навчального матеріалу здобувачі освіти мають можливість розвивати аналітичне мислення, навички аргументації, роботи з нормативно-правовими актами та спеціальними джерелами.

Самостійна робота сприяє кращому засвоєнню навчального матеріалу, поглибленню знань з окремих проблемних питань, формуванню вмінь здійснювати пошук, аналіз і систематизацію інформації, а також застосовувати сучасні інформаційні технології у сфері правоохоронної діяльності. Вона забезпечує розвиток професійної самостійності, відповідальності та готовності до практичної діяльності в умовах цифровізації суспільства.

Самостійна робота здійснюється у таких формах:

– опрацювання лекційного матеріалу та рекомендованої навчальної і наукової літератури;

– вивчення та аналіз нормативно-правових актів, що регулюють питання функціонування інформаційних систем у сфері правоохоронної діяльності;

– підготовка до семінарських занять, участь у дискусіях та обговоренні проблемних питань;

– виконання індивідуальних завдань, підготовка рефератів, аналітичних доповідей і презентацій;

– розв’язання практичних ситуаційних завдань (кейсів), пов’язаних із використанням інформаційних технологій у правоохоронній сфері;

– підготовка до модульного контролю та інших форм підсумкового оцінювання;

– робота з електронними ресурсами, інформаційно-пошуковими системами та спеціалізованими базами даних.

Підготовка до семінарських занять передбачає вирішення ситуаційних задач з відповідної теми. Вирішення ситуаційних задач передбачає ретельне вивчення всіх питань семінарського заняття, ознайомлення з рекомендованою літературою, опрацювання та детальний аналіз нормативних джерел з відповідної теми.

Розглядаючи конкретне завдання, необхідно дослідити всі обставини казусу і чітко відповісти на поставлені після завдання питання. Відповіді мають носити розширений та обґрунтований характер, обов'язково із посиланням на норми того чи іншого нормативного акту, а також на монографічне або навчально-методичне джерело, яке використовувалося.

Складаючи схеми чи таблиці, необхідно ознайомитися зі всіма метеріалами відповідної теми, опрацювати нормативно-правові акти та іншу спеціалізованулітературу. Виклад матеріалу у схемах і таблцях повинен бути стислим, максимально інформованим. Текстову інформацію, що подано в схемах та таблицях, потрібно ретельно перевірити на відсутність орфографічних, граматичних чи стилістичних помилок. Схеми, таблиці мають бути подані на електронному носії та у роздрукованому вигляді, а також можуть бути у письмовій формі.

4. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Однією з форм організації навчального процесу в умовах кредитно-модульної системи є індивідуальна робота здобувачів освіти.

Індивідуальна робота студентів з навчальної дисципліни «*Інформаційні системи та інформаційне забезпечення правоохоронної діяльності*» може включати:

– написання наукових статей, тез доповідей, рефератів з актуальних проблем інформаційного забезпечення правоохоронної діяльності та їх презентацію на семінарських заняттях;

– участь у студентських конференціях, конкурсах наукових робіт, олімпіадах, наукових засіданнях, науково-практичних семінарах, круглих столах, колоквіумах тощо;

– анотування додаткових джерел з навчальної дисципліни, складання бібліографічних описів відповідно до встановлених стандартів;

– підготовку аналітичних оглядів судової практики щодо використання інформаційних систем і цифрових доказів у кримінальному провадженні;

– виконання індивідуальних дослідницьких завдань, пов’язаних з аналізом функціонування державних інформаційних ресурсів та відомчих інформаційних систем;

– підготовку проєктів нормативних або аналітичних документів з питань удосконалення інформаційного забезпечення правоохоронної діяльності;

– розроблення презентаційних матеріалів, схем, алгоритмів роботи інформаційно-пошукових систем;

– підготовку до участі у фахових дискусіях з питань захисту інформації, цифрової трансформації правоохоронних органів та забезпечення інформаційної безпеки держави.

Вибір виду індивідуальної роботи здійснюється студентом з урахуванням власних наукових інтересів за попереднім погодженням з викладачем. Тематика та конкретна форма виконання завдання визначаються на початку навчального року, а виконана робота подається у встановлені строки. Організацію,

методичний супровід, контроль та оцінювання якості виконання індивідуальної роботи здійснює викладач (науковий керівник). Індивідуальна робота подається на кафедру для перевірки до початку екзаменаційної сесії.

Теми для написання рефератів

(есе, наукових статей, тез наукових доповідей, презентацій)

1. Єдина інформаційна система МВС України: сучасний стан та перспективи розвитку в умовах євроінтеграції.
2. Порівняльний аналіз інформаційних систем правоохоронних органів України та країн ЄС.
3. Проблеми інтероперабельності інформаційних систем МВС України та шляхи їх вирішення.
4. Цифрова трансформація МВС України: виклики впровадження єдиного інформаційного простору.
5. Правові засади функціонування ЄІС: відповідність стандартам ЄС та міжнародним вимогам.
6. Автоматизовані криміналістичні обліки в Україні: ефективність та напрями модернізації.
7. Використання біометричних баз даних у розслідуванні злочинів: досвід України та світу.
8. Єдиний реєстр досудових розслідувань (ЄРДР) як інструмент управління кримінальним провадженням.
9. Спеціальні бази даних ДНК-профілів у розкритті тяжких злочинів: правові та етичні аспекти.
10. Автоматизовані дактилоскопічні системи (АДІС) у криміналістичній практиці України.
11. Механізми міжвідомчої взаємодії в системі розшуку осіб в Україні: проблеми та шляхи вдосконалення.
12. Співпраця України з Інтерполом: використання баз даних I-24/7 у розшуку злочинців.
13. Шенгенська інформаційна система (SIS) як інструмент міжнародного розшуку: перспективи для України.
14. Правові механізми міжнародного розшуку та екстрадиції в умовах воєнного стану.
15. Цифровізація системи розшуку осіб: досвід впровадження та оцінка ефективності.
16. OSINT як інструмент досудового розслідування: правові межі та процесуальний статус отриманих даних.

17. Розвідка на основі відкритих джерел (OSINT) у протидії організованій злочинності.
18. Соціальні мережі як джерело оперативної інформації: методика збору та аналізу даних.
19. Правові та етичні межі використання OSINT у правоохоронній діяльності України.
20. Інструменти OSINT (Maltego, Shodan, SpiderFoot) у розслідуванні кіберзлочинів.
21. Цифрова криміналістика як новий напрям судової експертизи: становлення та перспективи в Україні.
22. Особливості збирання та дослідження цифрових доказів у кримінальному провадженні України.
23. Ransomware-атаки на об'єкти критичної інфраструктури: методи розслідування та протидії.
24. Ланцюг зберігання цифрових доказів (Chain of Custody): правові вимоги та практика забезпечення.
25. Інструменти цифрової криміналістики (Autopsy, EnCase, Volatility): порівняльний аналіз та практика застосування.
26. Розслідування злочинів у Dark Web: технологічні можливості та правові обмеження.
27. Фішинг як інструмент кіберзлочинності: методи виявлення, розслідування та запобігання.
28. Big Data у предиктивній поліцейській діяльності: світовий досвід та перспективи для України.
29. Алгоритмічна упередженість у системах предиктивної поліції: виявлення, вимірювання та усунення.
30. Геопросторовий аналіз злочинності (Crime Mapping) як інструмент управління поліцейськими ресурсами.
31. Аналіз соціальних мереж (SNA) у виявленні злочинних угруповань: методологія та практика.
32. Правові межі використання Big Data у правоохоронній діяльності: баланс між ефективністю та правами людини.
33. Предиктивна поліція в умовах воєнного стану: досвід України та міжнародні паралелі.
34. Інтелектуальні системи відеоспостереження у профілактиці злочинності: ефективність та правові обмеження.

35. Автоматичне розпізнавання номерних знаків (LPR/ANPR) у розслідуванні злочинів: практика та перспективи.
36. ГІС-технології в управлінні патрульною поліцією: оптимізація маршрутів та розподіл ресурсів.
37. Системи «розумного міста» (Smart City) у забезпеченні громадської безпеки: досвід впровадження.
38. Єдині ситуаційні центри (Command & Control Centers) як інструмент координації правоохоронних органів.
39. Правові засади використання систем відеоспостереження у публічних місцях: стандарти ЄС та Україна.
40. Штучний інтелект у кримінальному судочинстві: алгоритмічне правосуддя чи загроза справедливому суду?
41. EU AI Act та його вплив на використання штучного інтелекту у правоохоронній діяльності України.
42. Система оцінки ризику рецидиву COMPAS: правові та етичні проблеми алгоритмічного прогнозування.
43. Захист персональних даних в інформаційних системах правоохоронних органів: відповідність вимогам GDPR.
44. Право на пояснення алгоритмічного рішення (Explainable AI) у контексті кримінального провадження.
45. Перспективи етичного регулювання штучного інтелекту у правоохоронній діяльності України в умовах євроінтеграції.

Тези доповіді повинні бути обсягом 2-5 сторінок тексту та набрані у редакторі Microsoft Word (LibreOffice Writer) шрифтом Times New Roman, розмір шрифта 14, інтервал між рядками одинарний. Формат аркуша - А4. Параметри сторінки: ліве поле - 2.0 см, праве - 2.0 см, верхнє - 2.0 см, нижнє - 2.0 см. Сторінки без нумерації. Назва доповіді друкується великими літерами, шрифт жирний, без нахилу та підкреслювань, по центру аркуша, без переносів, відокремлюється від тексту одним вільним рядком зверху та знизу.

5. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

1. Конституція України : Закон України від 28 черв. 1996 р. № 254к/96-ВР (чинна редакція станом на 2026 р.). *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. *Відомості Верховної Ради України*. 1994. № 16. Ст. 93.
3. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.
4. Про захист персональних даних : Закон України від 01 черв. 2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
5. Про звернення громадян : Закон України від 02 жовт. 1996 р. № 393/96-ВР. *Відомості Верховної Ради України*. 1996. № 47. Ст. 256.
6. Про Національну поліцію : Закон України від 02 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.
7. Про Національну програму інформатизації : Закон України від 01 груд. 2022 р. № 2807-IX. *Відомості Верховної Ради України*. 2022. № 27–28. Ст. 181.
8. Про електронні комунікації : Закон України від 16 груд. 2020 р. № 1089-IX. *Відомості Верховної Ради України*. 2020. № 25–26. Ст. 170.
9. Про публічні електронні реєстри : Закон України від 18 листоп. 2021 р. № 1907-IX. *Відомості Верховної Ради України*. 2022. № 6. Ст. 41.
10. Про хмарні послуги : Закон України від 17 лют. 2022 р. № 2075-IX. *Відомості Верховної Ради України*. 2022. № 31. Ст. 233.
11. Про основні засади забезпечення кібербезпеки України : Закон України (чинна редакція 2023 р.). *Відомості Верховної Ради України*. 2023. № 11. Ст. 88.

12. Про Бюро економічної безпеки України : Закон України від 28 січ. 2021 р. № 1150-IX. *Відомості Верховної Ради України*. 2021. № 23. Ст. 197.
13. Про Національне антикорупційне бюро України : Закон України (чинна редакція станом на 2024–2025 рр.). *Відомості Верховної Ради України*.
14. Про запобігання корупції : Закон України (чинна редакція). *Відомості Верховної Ради України*. 2022. № 49. Ст. 2056.
15. Про електронні довірчі послуги : Закон України (чинна редакція). *Відомості Верховної Ради України*. 2021.
16. Стратегія кібербезпеки України : Указ Президента України від 26 серп. 2021 р. № 447/2021.
17. Про кіберзахист критичної інфраструктури : Закон України від 07 жовт. 2022 р. № 2659-IX. *Відомості Верховної Ради України*. 2022. № 42. Ст. 207.
18. Про електронний документообіг в державних органах : Закон України від 15 груд. 2021 р. № 1941-IX. *Відомості Верховної Ради України*. 2022. № 10. Ст. 66.
19. Про електронну ідентифікацію та е-підпис : Закон України від 17 бер. 2022 р. № 2137-IX. *Відомості Верховної Ради України*. 2022. № 14. Ст. 88.
20. Про електронну комерцію : Закон України від 01 лип. 2023 р. № 2845-IX. *Відомості Верховної Ради України*. 2023. № 25. Ст. 102.
21. Про відкриті дані та відкриті реєстри : Закон України від 12 трав. 2021 р. № 1410-IX. *Відомості Верховної Ради України*. 2021. № 20. Ст. 78.
22. Про електронні публічні послуги в сфері публічної адміністрації : Постанова Кабінету Міністрів України від 10 серп. 2022 р. № 847. *Офіційний вісник України*. 2022. № 60. Ст. 44.
23. Про інформаційні системи та кіберзахист у правоохоронних органах : Наказ МВС України від 05 квіт. 2023 р. № 200. *Офіційний вісник МВС України*. 2023. № 12. Ст. 15.
24. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229 XII. *База даних «Законодавство України» / Верховна Рада України*. URL: https://zakon.rada.gov.ua/go/2229-12

25. Про прокуратуру України : Закон України від 14 жовт. 2014 р. № 1697 VII. *База даних «Законодавство України» / Верховна Рада України*. URL: https://zakon.rada.gov.ua/laws/main/l433079z1
26. Про захист інформації та кіберзахист державних інформаційних ресурсів : Закон України від 17 квіт. 2025 р. № 4336 IX. *Відомості Верховної Ради України*. 2025.
27. Про інформацію : Закон України від 02 жовт. 1992 р. № 2657 XII. *Відомості Верховної Ради України*.
28. Про внесення змін до деяких законів України щодо захисту інформації в інформаційно-телекомунікаційних системах : Закон України (чинна редакція). *Відомості Верховної Ради України*.
29. Про основи національної безпеки України : Закон України (чинна редакція). *Відомості Верховної Ради України*.
30. Цимбалюк В. І., Багатко А. С. Правове регулювання кібербезпеки в Україні: сучасні виклики та перспективи розвитку. *Український політико-правовий дискурс*. 2025. № 18. С. 1–17.
31. Цимбалюк В. І., Багатко А. С. Міжнародне співробітництво у сфері кібербезпеки: роль України в умовах гібридної війни. *Науковий вісник УжНУ. Серія «Право»*. Вип. 92. С. 34–42.
32. Цимбалюк В. І., Багатко А. С. Кібербезпека об'єктів критичної інфраструктури України: актуальні проблеми та шляхи вирішення. *Наукові інновації та передові технології. Серія «Право»*. 2026. № 2 (54). С. 3490–3498.

Допоміжна:

1. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності : навч.-практ. посіб. Київ : Нац. акад. внутр. справ, 2024. 120 с.
2. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков та ін. Дніпро : Дніпров. держ. ун-т внутр. справ, 2024. 180 с.

3. Використання сучасних інформаційних технологій і діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару (28 листоп. 2019 р., м. Дніпро). Дніпро : Дніпропетровський державний університет внутрішніх справ, 2019. 124 с.
4. Інформаційне забезпечення юридичної діяльності : підручник / ред. В. Б. Вишня. Дніпро : Дніпропетровський державний університет внутрішніх справ, 2018. 245 с.
5. Бондар В. С., Рибалкін А. О. Інформаційне забезпечення досудового розслідування колабораційної діяльності. *Науковий вісник Ужгородського університету. Серія: Право*. 2023. Т. 2. Вип. 79. С. 225–231.
6. Вареник О. С. Тенденції міжнародного співробітництва у сфері кібербезпеки. *Юридичний науковий електронний журнал*. 2024. № 11. С. 591–593.
7. Кононенко В. П. Інформаційна безпека як стан. *Науковий вісник Ужгородського університету*. 2023. Т. 2. Вип. 76. С. 244–250.
8. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.
9. Тарасюк А. В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник*. 2020. Вип. 1. С. 133–136.
10. Тєтєвін М. С. Досвід України в галузі міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського національного університету*. 2024. Вип. 82. Ч. 3. С. 263–266.
11. Черниш Р. В. Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник кримінального правосуддя*. 2023. № 3–4. С. 112–121.
12. Бєлкін Л. М. та ін. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law»*. 2022. № 3 (64). С. 78–86.

13. Колосовський Є. Ю. Сучасний стан кібербезпеки в Україні в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402–405.
14. Ширяєв Д. О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів*. 2023. С. 600–602.
15. Синиціна Ю. Актуальні питання підготовки фахівців у галузі інформаційних технологій для органів Національної поліції України. *Сучасні інформаційні технології в діяльності Національної поліції :* матеріали Всеукр. наук.-практ. конференції (м. Дніпро, 02 листоп. 2023 р.). Дніпро : ДДУВС, 2024. С. 171–174.
16. Биков І. О. Інформаційно-аналітичне забезпечення діяльності слідчих та оперативних підрозділів у боротьбі з економічними злочинами. *Право і суспільство*. 2024. № 1. Т. 2. С. 392–396.
17. Старостін О. Ю. Забезпечення інформаційної безпеки як складової національної безпеки України. *Вісник кримінологічної асоціації України*. 2024. № 1 (31). С. 446–474.
18. Паращук Л. Я., Паращук С. М. Рекомендації стосовно використання інформаційних систем для покращення ситуаційної обізнаності органів військового управління. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2025. № 1. С. 46–54.
19. Зоренко Д. До питання процедури фіксації результатів OSINT в контексті розслідування воєнних злочинів. *Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд в майбутнє :* матеріали панельної дискусії VII Харківського Міжнародного юридичного форуму (25 верес. 2023 р.). Київ : Алерта, 2023. 146 с.
20. Латковська Т., Марущак А. Інтеграція штучного інтелекту у діяльність правоохоронних органів: ризики в контексті кібербезпеки. *Право та державне управління*. 2025. № 1. С. 355–361.
21. Глиняний І. В., Марчук В. В. Електронні сервіси в правоохоронній діяльності як елемент протидії корупції. *Правові новели*. 2025. № 25. С. 206–212.

22. Інформаційна безпека : навч. вид. / за ред. Ю. Я. Бобала, І. В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 590 с.
23. Присяжнюк М. М. Інформаційна безпека та кібербезпека держави. Київ : Ліра-К, 2024. 224 с.
24. ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements. International Organization for Standardization. Geneva, 2013.
25. ISO/IEC 27002:2022. Information technology — Security techniques — Code of practice for information security controls. International Organization for Standardization. Geneva, 2022.
26. NIST Cybersecurity Framework (CSF). Version 1.1. National Institute of Standards and Technology. Gaithersburg, 2018.
27. Scientific Working Group on Digital Evidence (SWGDE). Best Practices for Digital Evidence. USA, 2022.
28. McCarthy J. et al. Data in Policing: An Integrative Review. *International Journal of Police Science & Management*. 2024. Vol. 26, № 1. P. 45–67.
29. Schmitt M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.
30. Open-Source Intelligence (OSINT) Tools for Law Enforcement. *Journal of Policing, Intelligence and Counter Terrorism*. 2023. Vol. 18, № 3. P. 201–220.
31. Challenges and Solutions in Law Enforcement in the Digital Era. *International Conference on Law Enforcement Technologies*. 2022. P. 88–102.