

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ**  
**ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ**  
**КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

**ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ  
ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ**

<b>Назва освітньо-професійної програми</b>	Правоохоронна діяльність
<b>Рівень вищої освіти</b>	другий (магістерський) рівень
<b>Галузь знань</b>	26 Цивільна безпека
<b>Спеціальність</b>	262 Правоохоронна діяльність
<b>Вид навчальної дисципліни</b>	обов'язкова
<b>Мова викладання</b>	українська
<b>Рік навчання</b>	перший (денна, заочна)

**ЗАТВЕРДЖЕНО**

Науково-методичною радою  
Дніпровського державного  
університету внутрішніх справ  
протокол від 30.08.2024 № 17

**ПОГОДЖЕНО**

Гарант освітньої програми «Правоохоронна діяльність»

\_\_\_\_\_  
(підпис) Володимир ШАБЛИСТИЙ |  
(ім'я та прізвище)

Розглянуто на засіданні кафедри Інформаційних технологій  
Протокол від 15.08.2024 № 1

Інформаційно-аналітичне забезпечення правоохоронної діяльності. Робоча програма навчальної дисципліни. Дніпро: Дніпровський державний університет внутрішніх справ, 2024 рік. кількість сторінок 16 с.

**РОЗРОБНИК:**

Доцент кафедри інформаційних технологій, кандидат технічних наук, доцент,  
Синиціна Юлія Петрівна

**РЕЦЕНЗЕНТИ:**

1. Доцент кафедри комп'ютерних інформаційних технологій Українського державного університету науки і технологій, кандидат технічних наук, доцент, Гришечкіна Тетяна Сергіївна;
2. Доцент кафедри прикладної математики Українського державного університету науки і технологій, кандидат фізико-математичних наук, доцент, Гасанов Закарія Муса огли.

**Лист оновлення та перезатвердження  
робочої програми навчальної дисципліни  
(додаток 1 до Робочої програми навчальної дисципліни)**

## 1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Характеристика навчальної дисципліни	
	денна форма здобуття вищої освіти	заочна форма здобуття вищої освіти
Кількість кредитів ЄКТС	3	3
Загальна кількість годин	90	90
Рік підготовки	перший	перший
Семестр	1	1
Лекції	2	2
Семінарські	-	-
Практичні	28	6
Самостійна робота	60	82
Індивідуальні завдання (курсова робота)		
Підсумковий семестровий контроль	залік	залік

## 2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» полягає у підготовці висококваліфікованих фахівців правоохоронної діяльності в сфері забезпечення охорони прав і свобод людини, інтересів суспільства і держави, захисту діяльності в правоохоронній галузі.

Очікувані результати навчання: у результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

*знати:*

- теоретичні основи інформаційно-аналітичного забезпечення в контексті правоохоронної діяльності;
- сучасні інструменти та технології для здійснення аналітичних операцій;
- нормативно-правову базу, що регулює інформаційно-аналітичну діяльність у правоохоронній сфері;
- специфіку кіберзагроз та методи їх виявлення та запобігання;
- основні принципи та можливості використання відкритих даних для аналізу та розслідування;

*вміти:*

- використовувати різноманітні аналітичні інструменти для обробки та інтерпретації інформації;
- виявляти та аналізувати потенційні правопорушення та інші загрози з використанням інформаційно-аналітичних методів;
- аналізувати потенційні загрози та вчасно реагувати на них;
- здійснювати пошук, збір та аналіз інформації з використанням відкритих

джерел.

Вивчення дисципліни забезпечує формування компетентностей за освітньою програмою: Правоохоронна діяльність.

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

**Загальні компетентності:**

ЗК1 – Здатність застосовувати знання у практичних ситуаціях.

ЗК4 – Здатність використовувати інформаційні та комунікаційні технології.

ЗК5 – Здатність вчитися і оволодівати сучасними знаннями.

ЗК8 – Здатність приймати обґрунтовані рішення.

ЗК9 – Здатність працювати в команді.

**Спеціальні компетентності:**

СК4 – Здатність до критичного та системного аналізу правових явищ і застосування набутих знань та навичок у професійній діяльності.

СК5 – Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК6 – Здатність аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації.

СК14 – Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних.

СК18 – Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.

**Пререквізити та постреквізити дисципліни:**

**Пререквізити:** «Інформаційні технології».

**Постреквізити:** «Кримінальний аналіз».

Здобувачі вищої освіти повинні продемонструвати такі **результати навчання:**

РН3 – Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.

РН4 – Формулювати і перевіряти гіпотези, аргументувати висновки.

РН8 – Здійснювати пошук інформації у доступних джерелах для повного та всебічного встановлення необхідних обставин.

РН9 – 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.

РН14 – Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності.

### **3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

#### **ТЕМА 1. ОСНОВНІ ПРИНЦИПИ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ.**

Поняття, предмет, мета та завдання навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності». Концепція та методологія інформаційно-аналітичного забезпечення правоохоронної діяльності. Роль підрозділів інформаційно-аналітичного забезпечення правоохоронної діяльності у визначенні стратегічних переваг.

#### **ТЕМА 2. ПОШУК ІНФОРМАЦІЇ З ВІДКРИТИХ ДЖЕРЕЛ МЕРЕЖІ ІНТЕРНЕТ.**

Історія розвитку та загальна характеристика пошукових систем. Пошук інформації за допомогою GOOGLE: сервіси, спеціальний пошук, апаратне забезпечення та інструменти. Мета-пошукові системи та системи анонімного пошуку інформації. Пошукові системи в соціальних мережах. Пошук оперативної інформації в соціальній мережі Facebook. Отримання оперативної інформації з соціальної мережі Вконтакте. Застосування правоохоронцями чат-ботів у месенджері Telegram. Інформаційні системи Міністерства юстиції України. Єдиний державний реєстр судових рішень.

#### **ТЕМА 3. ВИКОРИСТАННЯ OSINT-ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ.**

Аналіз OSINT-технологій у сучасному інформаційному середовищі. Методи та інструменти для збору, фільтрації та аналізу інформації з OSINT-джерел. Способи виявлення потенційних загроз, злочинних дій та ризиків за допомогою OSINT-технологій. Розробка стратегій та методів для оптимізації використання OSINT-технологій.

#### **ТЕМА 4. SWOT-АНАЛІЗ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ОЦІНКА СТРАТЕГІЧНИХ ФАКТОРІВ.**

Значення та роль SWOT-аналізу в оперативній діяльності. Використання SWOT-аналізу для стратегічного прийняття рішень. Важливість стратегічного планування. Розробка стратегій та дій на основі результатів SWOT-аналізу. Вплив технологічних інновацій, кібербезпеки та соціальних змін на SWOT-аналіз.

## **ТЕМА 5. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ: МЕТОДИ ТА СТРАТЕГІЇ КІБЕРБЕЗПЕКИ.**

Огляд сучасних викликів і загроз інформаційній безпеці в правоохоронній діяльності. Методи збору та аналізу конфіденційної інформації підрозділами стратегічних розслідувань. Стратегії захисту конфіденційної інформації від зовнішніх загроз правоохоронців. Аналіз інноваційних технологій та інструментів для захисту інформації. Розгляд методів та заходів для виявлення та запобігання соціальному інженерінгу та фішинг-атакам. Дослідження можливостей використання аналізу Big Data для виявлення кіберзагроз та підвищення рівня інформаційної безпеки.

## **ТЕМА 6. ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ (AI) ТА МАШИННОГО НАВЧАННЯ (ML) У ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ.**

Аналіз потенційного впливу технологій штучного інтелекту (AI) та машинного навчання (ML) в правоохоронній діяльності. Методи та інструменти використання штучного інтелекту (AI) та машинного навчання (ML) для аналізу великих обсягів даних. Важливість розробки інтелегентних алгоритмів для виявлення та прогнозування потенційних загроз та ризиків. Переваги та обмеження використання штучного інтелекту (AI) та машинного навчання (ML) в правоохоронній діяльності.

### **4. СТРУКТУРА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ**

#### **ДЕННА ФОРМА НАВЧАННЯ**

##### **Теми та план лекційних занять**

<b>Назва теми лекційного заняття</b>	<b>План лекційного заняття</b>	<b>Кількість годин</b>
<b>Тема 1.</b> Основні принципи інформаційно-аналітичного забезпечення	1. Поняття, предмет, мета та завдання навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності».	2

правоохоронної діяльності.	2. Концепція та методологія інформаційно-аналітичного забезпечення правоохоронної діяльності. 3. Роль підрозділів інформаційно-аналітичного забезпечення правоохоронної діяльності у визначенні стратегічних переваг.	
----------------------------	--	--

### Теми практичних занять

Назва теми практичного заняття	Кількість годин
<b>Тема 1.</b> Основні принципи інформаційно-аналітичного забезпечення правоохоронної діяльності.	4
<b>Тема 2.</b> Пошук інформації з відкритих джерел мережі інтернет.	6
<b>Тема 3.</b> Використання OSINT-технологій для підвищення ефективності правоохоронної діяльності.	2
<b>Тема 4.</b> SWOT-аналіз в правоохоронній діяльності: оцінка стратегічних факторів	12
<b>Тема 5.</b> Забезпечення інформаційної безпеки правоохоронної діяльності: методи та стратегії кібербезпеки.	2
<b>Тема 6.</b> Використання технологій штучного інтелекту (AI) та машинного навчання (ml) у правоохоронній діяльності.	2

### Теми для самостійної роботи

Назва теми	Кількість годин
<b>Тема 1.</b> Основні принципи інформаційно-аналітичного забезпечення правоохоронної діяльності.	12
<b>Тема 2.</b> Пошук інформації з відкритих джерел мережі інтернет.	8
<b>Тема 3.</b> Використання OSINT-технологій для підвищення ефективності правоохоронної діяльності.	12
<b>Тема 4.</b> SWOT-аналіз в правоохоронній діяльності: оцінка стратегічних факторів	8
<b>Тема 5.</b> Забезпечення інформаційної безпеки правоохоронної діяльності: методи та стратегії кібербезпеки.	12
<b>Тема 6.</b> Використання технологій штучного інтелекту (AI) та машинного навчання (ml) у правоохоронній діяльності.	8

## ЗАОЧНА ФОРМА НАВЧАННЯ

### Теми та план лекційних занять

Назва теми лекційного заняття	План лекційного заняття	Кількість годин
<b>Тема 1.</b> Основні принципи інформаційно-аналітичного забезпечення правоохоронної діяльності.	1. Поняття, предмет, мета та завдання навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності». 2. Концепція та методологія інформаційно-аналітичного забезпечення правоохоронної діяльності.	2

	3. Роль підрозділів інформаційно-аналітичного забезпечення правоохоронної діяльності у визначенні стратегічних переваг.	
--	---	--

### Теми практичних занять

Назва теми практичного заняття	Кількість годин
<b>Тема 2.</b> Пошук інформації з відкритих джерел мережі інтернет.	2
<b>Тема 3.</b> Використання OSINT-технологій для підвищення ефективності правоохоронної діяльності.	2
<b>Тема 4.</b> SWOT-аналіз в правоохоронній діяльності: оцінка стратегічних факторів	2

### Теми для самостійної роботи

Назва теми	Кількість годин
<b>Тема 1.</b> Основні принципи інформаційно-аналітичного забезпечення правоохоронної діяльності.	20
<b>Тема 2.</b> Пошук інформації з відкритих джерел мережі інтернет.	24
<b>Тема 3.</b> Використання OSINT-технологій для підвищення ефективності правоохоронної діяльності.	18
<b>Тема 4.</b> SWOT-аналіз в правоохоронній діяльності: оцінка стратегічних факторів	20

## 5. ПЕРЕЛІК ПИТАНЬ ТА ЗАВДАНЬ, ЩО ВІНОСЯТЬСЯ НА ПІДСУМКОВИЙ КОНТРОЛЬ

1. Основні виклики інформаційно-аналітичного забезпечення в умовах розширення цифрового середовища та зростання обсягів інформації.
2. Методи та підходи, які використовуються для перевірки та підтвердження достовірності інформації, що використовується в аналізі.
3. Впровадження технологій та інструментів для оптимізації інформаційно-аналітичного процесу.
4. Як підрозділи стратегічних розслідувань ведуть моніторинг і аналіз суспільних мереж та медіа для виявлення публічних настроїв та думок? Як вони реагують на екстрені ситуації і кризові ситуації через інформаційно-аналітичне забезпечення?
5. Роль SWOT-аналізу в оперативній діяльності правоохоронних органів.
6. Методи та заходи для виявлення та запобігання соціальному інженерингу та фішинг-атакам в контексті інформаційної безпеки.
7. Виклики і загрози інформаційній безпеці в діяльності підрозділів стратегічних розслідувань і чому ця тема важлива
8. Методи збору та аналізу конфіденційної інформації, які використовують підрозділами стратегічних розслідувань.
9. Найбільш ефективні стратегії захисту конфіденційної інформації від зовнішніх загроз.
10. Інноваційні технології та інструменти для захисту інформації в сучасних



підрозділах стратегічних розслідувань.

11. Можливості ГІС для моніторингу та аналізу розвитку інфраструктури та транспортних мереж у контексті національної безпеки.

12. Як технології VR/AR можуть посилити використання геоінформаційних технологій для стратегічних розслідувань?

13. Наведіть практичні приклади використання ГІС для аналізу демографічних та соціальних тенденцій, які можуть бути важливими для стратегічних розслідувань.

14. Яким чином ГІС можуть підтримувати вирішення екологічних завдань та прогнозування екологічних криз?

15. Наведіть можливості для використання ГІС у сфері боротьби з кіберзагрозами та кібербезпекою.

16. Як ГІС можуть сприяти впровадженню інтегрованих систем моніторингу та управління кризовими ситуаціями?

17. Виклики при використанні ГІС для аналізу геополітичних факторів у стратегічних розслідуваннях.

18. Можливості для використання ГІС у контексті прогнозування та реагування на природні катастрофи.

19. Історія розвитку OSINT-технологій.

20. Роль OSINT-технологій в сучасному інформаційному середовищі та як вони можуть покращити діяльність підрозділів стратегічних розслідувань.

21. Методи та інструменти для збору інформації з OSINT-джерел. Які є основні відмінності між ними?

22. Можливі способи виявлення потенційних загроз, злочинних дій та ризиків за допомогою OSINT-технологій.

23. Приклади успішного використання OSINT-технологій у діяльності підрозділів стратегічних розслідувань ви можете навести? Як це вплинуло на їхню ефективність та результативність?

24. Як OSINT-технології можуть сприяти підвищенню громадської та національної безпеки? Які переваги вони мають у цьому контексті?

25. Які можливості ви бачите для подальшого розвитку та вдосконалення використання OSINT-технологій в стратегічних розслідуваннях? Які тренди в цій галузі ви враховуєте?

26. Основні виклики та завдання перед підрозділами стратегічних розслідувань у зв'язку з використанням OSINT-технологій. Як вони можуть підготувати персонал для роботи з цими технологіями?

27. Наведіть приклади можливих використань OSINT-технологій для виявлення та аналізу терористичних загроз та інших форм злочинності.

28. Основні поняття технологій штучного інтелекту (AI) та машинного навчання (ML).

29. Використання технологій штучного інтелекту (AI) та машинного навчання (ML) у діяльності підрозділів стратегічних розслідувань.

30. Аналіз потенційного впливу технологій штучного інтелекту (AI) та машинного навчання (ML) в діяльності підрозділів стратегічних розслідувань.

31. Методи та інструменти використання штучного інтелекту (AI) та машинного

навчання (ML) для аналізу великих обсягів даних.

32. Важливість розробки інтелегентних алгоритмів для виявлення та прогнозування потенційних загроз та ризиків.

33. Переваги та обмеження використання штучного інтелекту (AI) та машинного навчання (ML) в діяльності підрозділів стратегічних розслідувань.

34. Приклади успішного використання штучного інтелекту (AI) та машинного навчання (ML) в діяльності підрозділів стратегічних розслідувань та їх вплив на громадську та національну безпеку.

35. Безпека та захист конфіденційної інформації при використанні цих технологій у діяльності підрозділів стратегічних розслідувань.

## 6. КРИТЕРІЇ ТА ЗАСОБИ ОЦІНЮВАННЯ УСПІШНОСТІ НАВЧАННЯ

ДЛЯ ДЕННОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		Підсумковий контроль
Аудиторна робота	Самостійна робота/ Індивідуальна робота	Залік (3)
≤ 40	≤ 10	
≤ 50		≤ 50
<b>Підсумкова оцінка у випадку заліку (П) = ПК + З ≤ 100</b>		

ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		Підсумковий контроль
Аудиторна робота	Самостійна робота/ Індивідуальна робота	Залік (3)
≤ 20	≤ 30	
≤ 50		≤ 50
<b>Підсумкова оцінка у випадку заліку (П) = ПК + З ≤ 100</b>		

Критерієм успішного проходження Здобувачем підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Мінімальний пороговий рівень оцінки визначається за допомогою якісних критеріїв і трансформується в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали.

Здобувач допускається до складання підсумкового контролю, якщо ним виконані всі передбачені РПНД поточні завдання та сума балів поточного контролю не менше ніж 34. Якщо сума балів поточного контролю менше ніж 34, здобувач не допускається до підсумкового контролю і зобов'язаний доопрацювати завдання та набрати необхідну кількість балів.

За результатами аудиторної роботи здобувач денної форми навчання має отримати максимальну кількість 40 балів (кожне заняття оцінюється за п'ятибальною шкалою); за результатами самостійної роботи – 10 балів. Таким чином бали за поточний контроль (34-50 балів).

За результатами аудиторної роботи здобувач заочної форми навчання має отримати максимальну кількість 20 балів (кожне заняття оцінюється за п'ятибальною шкалою); за результатами самостійної роботи – 30 балів. Таким чином бали за поточний контроль (34-50 балів).

Розрахунок підсумкової оцінки з навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» здійснюється відповідно до формули:

$$П = ПК + З \leq 100,$$

де ПК – бали за поточний контроль (34-50 балів),

З – бали за результатами складання заліку

### Критерії оцінювання аудиторної роботи здобувачів вищої освіти (денна та заочна форми навчання)

БАЛИ	ПОЯСНЕННЯ
5	<b>Високий рівень</b> компетентностей. Питання по практичним роботам, винесені на розгляд, засвоєні у повному обсязі; на високому рівні сформовані необхідні практичні навички та вміння; всі навчальні завдання, передбачені планом заняття, виконані в повному обсязі. Під час заняття продемонстрована стабільна активність та ініціативність. Відповіді на теоретичні питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань ґрунтується на глибокому знанні навчального матеріалу дисципліни.
4	<b>Невисокий рівень</b> компетентностей. Питання по практичним роботам, винесені на розгляд, засвоєні у повному обсязі; в основному сформовані необхідні практичні навички та вміння; всі передбачені планом заняття навчальні завдання виконані в повному обсязі з неістотними неточностями. Під час заняття продемонстрована ініціативність. Відповіді на питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань переважно ґрунтується на знанні навчального матеріалу дисципліни.
3	<b>Достатній рівень</b> компетентностей. Питання по практичним роботам, винесені на розгляд, у цілому засвоєні; практичні навички та вміння мають поверхневий характер, потребують подальшого напрацювання та закріплення; навчальні завдання, передбачені планом заняття, виконані, деякі види завдань виконані з помилками.
2	<b>Недостатній рівень</b> компетентностей. Питання по практичним роботам, винесені на розгляд, засвоєні частково, прогалини у знаннях не носять істотного характеру; практичні навички та вміння сформовані недостатньо; більшість навчальних завдань виконано, деякі з виконаних завдань містять істотні помилки, які потребують подальшого усунення.
1	<b>Мінімальний рівень</b> компетентностей. Студент не готовий до заняття, не знає більшої частини програмного матеріалу, з труднощами виконує завдання, невпевнено відтворює терміни і поняття, що розглядалися під час заняття, допускає змістовні помилки, не володіє відповідними вміннями і навичками, необхідними для розв'язання професійних завдань.
0	<b>Незадовільний рівень</b> компетентностей. Відсутність на занятті.

Для навчальної дисципліни «Інформаційно-аналітичне забезпечення правоохоронної діяльності» засобами діагностики знань (успішності навчання) виступають: стандартизовані тести, тези, есе, презентації результатів виконаних завдань та досліджень, презентації та виступи на наукових заходах, інші види індивідуальних та групових завдань.

### **Критерії оцінювання самостійної роботи (денна форма навчання)**

Пропонується наступне оцінювання самостійної роботи студентів за виконання 1 завдання за вибором здобувача та узгодженням з викладачем:

1. Написання та участь у конкурсі творчих та/або наукових робіт серед студентів, (МОН, ДДУВС) (написання робіт, есе, доповідь, творча публікація, творча візуалізація, відеоролик) - 10 балів.
2. Підготовка презентацій-доповідей участі в роботі науковому студентську гуртку кафедри (надати презентація та фото виступу) – 10 балів.
3. Підготовка тези доповідей на міжнародну (всеукраїнську) науково-практичну конференцію за умови надання PrinScrin перевірки на плагіат за результатом не менше 70% оригінального тексту. Тези повинні бути підготовленні відповідно «Методичних вказівок з написання тез» – 10 балів.
4. Отримання сертифікату після проходження он-лайн тесту Цифрограм 1.0 для громадян на освітній платформі ДІЯ: Освіта <https://osvita.diia.gov.ua/digigram> - 10 балів.
5. Підготовка презентації у редакторі Гугл презентації (завантаження презентації та надання посилання у коментарях на СУДН «Moodle») за темою зі списку у додатковому файлі «Методичні вказівки до виконання презентації у редакторі Гугл презентація» – 10 балів.
6. Виконання індивідуальної роботи згідно завдання викладача (до 10 балів: Кросворд – 3 балів; Реферат – 3 балів; Есе – 4 балів).
7. Проходження тесту з самостійної роботи 40 питань відповідно 10 балів

### **Критерії оцінювання самостійної роботи (заочна форма навчання)**

Пропонується наступне оцінювання самостійної роботи курсантів за виконання 1 завдання за вибором здобувача та узгодженням з викладачем для отримання максимальної кількості балів - 30:

1. Написання та участь у конкурсі творчих та/або наукових робіт серед студентів, (МОН, ДДУВС) (написання робіт, есе, доповідь, творча публікація, творча візуалізація, відеоролик) - 30 балів.
2. Підготовка презентацій-доповідей участі в роботі науковому студентську гуртку кафедри (надати презентація та фото виступу) – 10 балів.
3. Підготовка тези доповідей на міжнародну (всеукраїнську) науково-практичну конференцію за умови надання PrinScrin перевірки на плагіат за результатом не менше 70% оригінального тексту. Тези повинні бути підготовленні відповідно «Методичних вказівок з написання тез» – 10 балів.
4. Отримання сертифікату після проходження он-лайн тесту Цифрограм 1.0 для громадян на освітній платформі ДІЯ: Освіта <https://osvita.diia.gov.ua/digigram> - 30 балів.
5. Підготовка презентації у редакторі Гугл презентації (завантаження презентації та надання посилання у коментарях на СУДН «Moodle») за темою зі

списку у додатковому файлі «Методичні вказівки до виконання презентації у редакторі Гугл презентація» – 10 балів.

6. Проходження тесту з самостійної роботи 40 питань відповідно 30 балів.

### Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ECTS	
	Залік	Екзамен/ диференційований залік	Оцінка	Пояснення
90-100	зараховано	Відмінно	A	« <b>Відмінно</b> » - теоретичний зміст курсу засвоєний у повному обсязі; сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані в повному обсязі.
83-89		Добре	B	« <b>Дуже добре</b> » - теоретичний зміст курсу засвоєний в повному обсязі; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання більшості з них оцінена кількістю балів, близько до максимальної.
75-82			C	« <b>Добре</b> » - теоретичний зміст курсу засвоєний цілком; в основному сформовані практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання жодного з них не оцінена мінімальною кількістю балів, деякі види завдань виконані з помилками.
68-74		Задовільно	D	« <b>Задовільно</b> » - теоретичний зміст курсу засвоєний не повністю; але прогалини не носять істотного характеру; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; більшість передбачених РПНД навчальних завдань виконано, деякі з виконаних завдань містять помилки.
60-67			E	« <b>Достатньо</b> » - теоретичний зміст курсу засвоєний частково; не сформовано деякі практичні навички роботи; частина передбачених РПНД навчальних завдань не виконані або якість виконання деяких з них оцінено числом балів, близьким до мінімального.
35-59	не зараховано	Не задовільно	Fx	« <b>Умовно незадовільно</b> » - теоретичний зміст курсу засвоєний частково; не сформовані необхідні практичні навички роботи; більшість навчальних завдань не виконано або якість їх виконання оцінено кількістю балів, близько до мінімальної; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю повторного складання).
1-34			F	« <b>Безумовно незадовільно</b> » - теоретичний зміст курсу не засвоєний; не сформовані необхідні практичні навички роботи; всі виконані навчальні завдання містять грубі помилки або не виконані взагалі; додаткова самостійна робота над матеріалом курсу не призведе до значного підвищення якості виконання навчальних завдань.

### 7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧЕНО НАВЧАЛЬНОЮ ДИСЦИПЛІНОЮ

1. Комп'ютерна техніка, відповідне програмне забезпечення.
2. Наявність доступу до Інтернет.
3. Мультимедійне обладнання.

## **8. ІНФОРМАЦІЙНЕ ТА МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ (рекомендовані джерела інформації)**

### **Основні нормативні акти:**

- закони:

1. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ.  
URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення 20.07.2024);
2. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI.  
URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення 20.07.2024).

- постанови, інші рішення, роз'яснення суддів (Конституційного, Верховного):

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова КМУ від 8 лютого 2021 року № 92. URL: <https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text>;

### **Підручники:**

1. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. д.т.н., проф. В.Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с.  
URI: <https://er.dduvs.in.ua/handle/123456789/7110>;
2. Інформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижій, С.О. Прокопов, Е.В. Рижков. Дніпро: Дніпроп. держ. ун-т внутр.справ, 2021. 492с. URI: <http://er.dduvs.in.ua/handle/123456789/6820>

### **Монографії та інші наукові видання:**

1. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: Львівський державний університет внутрішніх справ, 2020. 256 с.
2. Габорець О. А., Лунгол О. М. Основи кібербезпеки: методичні рекомендації до практичних занять. Кропивницький: Book Creator, 2023. 76 с. URL: <https://read.bookcreator.com/fQ6a2RCUdGO8pRyIJCh2iAlj1bt2/v0qCTrYoRnGfe3g3qIgfHQ/axo1DK1pTdulxaUM4L81Q>
3. Лунгол О. М., Габорець О. А. OSINT-технології в правоохоронній діяльності: навчальний посібник. Мультимедійне видання. Кропивницький: Book Creator, 2023. URL:

<https://read.bookcreator.com/fQ6a2RCUdGO8pRyIJCh2iAlj1bt2/sWY11xVJRKymMSKpkHe4TQ/izsvJPMuS4uLPTsQxI8LvQ>

4. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: Львівський державний університет внутрішніх справ, 2017. 244 с.

#### **Інтернет-ресурси:**

1. Офіційний сайт Президента України: [www.president.gov.ua](http://www.president.gov.ua)
2. Офіційний сайт Верховної Ради України: [www.kmu.gov.ua](http://www.kmu.gov.ua)
3. Офіційний сайт Кабінету Міністрів України: [www.kmu.gov.ua](http://www.kmu.gov.ua)
4. Офіційний сайт Верховного Суду: <https://supreme.court.gov.ua/supreme/>
5. Офіційний сайт Міністерства внутрішніх справ України: <https://mvs.gov.ua/>
6. Офіційний сайт Національної поліції України: <https://www.npu.gov.ua/>
7. Головне управління державної служби України: <http://www.guds.gov.ua>
8. Сайт Ради національної безпеки і оборони України: <http://www.raibow.gov.ua>
9. OSINT Framework: <https://osintframework.com/>
10. Національна бібліотека України імені В.І. Вернадського: [www.nbuv.gov.ua](http://www.nbuv.gov.ua)

**Завідувач кафедри  
економічної та інформаційної  
безпеки**

**Андрій ГРЕБЕНЮК**

