МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерної інженерії та інноваційних технологій

«ЗАТВЕРДЖУЮ»

Ректор Міжнародного гуманітарного університету д.ю.н., професор

Костянтин ГРОМОВЕНКО

«29» серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Основи цифрової криміналістики

Галузь знань	12 «Інформаційні технології»
Спеціальність	125 «Кібербезпека та захист інформації»
Назва освітньої програми	Кібербезпека
Рівень вищої освіти	перший (бакалаврський) рівень

Одеса – 2025 рік

Робоча програма затверджена на засіданні кафедри комп'ютерної інженерії та інноваційних технологій протокол № 1 від 29.08.2025 року.

Розробники і викладачі	Контактний тел.	E-mail
доцент кафедри комп'ютерної інженерії та інноваційних технологій, кандидат юридичних наук, доцент, **Ісмайлов Карен Юрійович**	+380997060070	0997060070@ukr.net

Завідувач кафедри комп'ютерної інженерії
та інноваційних технологій
к.т.н., доцент _____ Лариса ЙОНА

Гарант освітньої програми
к.т.н., доцент _____ Лариса ЙОНА

Узгоджено
Начальник навчального відділу _____ Лілія САЄНКО

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><th rowspan="2">Найменування показників</th><th rowspan="2">Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th colspan="2">Характеристика навчальної дисципліни</th></tr>
<tr><th>денна форма навчання</th><th>заочна форма навчання</th></tr>
<tr><td rowspan="10">Кількість кредитів – 4
Загальна кількість годин – 120</td><td>Галузь – 12 Інформаційні технології</td><td colspan="2">обов’язкова</td></tr>
<tr><td rowspan="9">Спеціальність – 125 Кібербезпека та захист інформації</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td colspan="2">2-й</td></tr>
<tr><td colspan="2">Семестр</td></tr>
<tr><td>3-й</td><td>3-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="8">Мова навчання – українська</td><td rowspan="8">Рівень вищої освіти – перший (бакалаврський) рівень</td><td>26 год.</td><td>6 год.</td></tr>
<tr><td colspan="2">Практичні, семінарські</td></tr>
<tr><td>26 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>0 год.</td><td>год.</td></tr>
<tr><td colspan="2">Самостійна робота та індивідуальні завдання</td></tr>
<tr><td>68 год.</td><td>110 год.</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>Залік</td><td>Залік</td></tr>
</table>

Основи цифрової криміналістики – це фундаментальна дисципліна, що вивчає теоретичні засади, методи та практичні інструменти виявлення, фіксації, збереження, аналізу та подання цифрових доказів у контексті розслідування кіберзлочинів та інших кіберінцидентів. Курс охоплює універсальні принципи роботи з цифровою інформацією як об'єктом судового дослідження, незалежно від типу носія, операційної системи чи програмного середовища. Особлива увага приділяється забезпеченню автентичності, цілісності та процесуальної допустимості цифрових доказів, а також дотриманню доказового ланцюжка (Chain of Custody) на всіх етапах роботи.

Знання, отримані в рамках цієї дисципліни, є критично важливими для майбутніх фахівців з кібербезпеки, оскільки ефективне розслідування інцидентів неможливе без належного документування та аналізу цифрових слідів. Розуміння природи волатильних і неволатильних даних, методів створення криміналістичних образів, особливостей роботи з логами, метаданими, мережевим трафіком та мобільними пристроями дозволяє фахівцю не лише виявляти факт компрометації, а й відтворювати хронологію подій, ідентифікувати джерела загроз та формувати обґрунтовані висновки для подальшого використання в правовому полі.

Метою дисципліни є формування у студентів системного розуміння ролі цифрової криміналістики в забезпеченні кібербезпеки, а також розвиток практичних навичок збору та аналізу цифрових доказів із дотриманням норм чинного законодавства України та міжнародних стандартів. Курс спрямований на інтеграцію технічних знань з юридичною складовою, що дозволяє випускникам ефективно взаємодіяти зі слідчими органами, експертними установами та підрозділами реагування на інциденти.

ПРЕРЕКВІЗИТИ. Передумовами є знання, уміння та навички, отримані при вивченні «Операційних систем» (ОК 20), «Безпеки програм та даних» (ОК 16), «Комплексних систем захисту інформації» (ОК 24), «Криптографії та криптоаналізу» (ОК 23), «Управління інформаційною та кібербезпекою» (ОК 30) та «Основ Web-безпеки» (ОК 22).

ПОСТРЕКВІЗИТИ. Знання методів цифрової криміналістики та розслідування інцидентів є корисними при паралельному вивченні «Управління інформаційною та кібербезпекою» (ОК 30), «Етичного хакінгу та тестування на проникнення» (ОК 18), а також при проходженні переддипломної практики (ОК 35) і підготовці та захисті кваліфікаційної роботи (ОК 36).

2. ОЧІКУВАНІ КОМПЕТЕНТНОСТІ, ЯКІ ПЛАНУЄТЬСЯ СФОРМУВАТИ ТА ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ

У процесі реалізації програми дисципліни «Криптографія та криптоаналіз» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

ІК. Здатність розв’язувати складні спеціалізовані задачі та практичні проблеми у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК)

ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями

Спеціальні (фахові, предметні) компетентності

СК 5. Здатність відновлювати функціонування інформаційних та інформаційно-комунікаційних систем після реалізації загроз, здійснення кібератак, збоїв і відмов різних класів та походження.

СК 10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Навчальна дисципліна «Основи цифрової криміналістики» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

РН 5. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення

РН 14. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційних та інформаційно-комунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки і забезпечувати функціонування спеціального програмного забезпечення щодо захисту та відновлення інформації.

РН 15. Збирати, обробляти зберігати, аналізувати критичні дані для доказу реалізації кіберзагроз, проводили аналіз та дослідження кіберінциденту з метою оперативного відновлення функціонування інформаційної системи.

РН 21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Вступ до цифрової криміналістики та її місце в системі кібербезпеки.
Поняття цифрової криміналістики. Роль у забезпеченні кібербезпеки. Основні напрями та завдання.

Тема 2. Правові та організаційні основи цифрової криміналістики. Законодавчі вимоги та міжнародні стандарти. Організація роботи експерта-криміналіста. Етичні та правові межі діяльності

Тема 3. Цифрові докази та сліди: види, властивості та фіксація. Класифікація цифрових доказів (файли, журнали, мережеві артефакти). Властивості цифрових слідів (автентичність, цілісність, повторюваність). Методи фіксації та документування.

Тема 4. Методи та засоби збору цифрових доказів. Інструменти збору даних (форензичні утиліти, open-source засоби). Процедури вилучення інформації з комп'ютерів, мобільних пристроїв, мереж. Забезпечення ланцюга збереження доказів.

Тема 5. Особливості розслідування окремих видів кіберзлочинів. Розслідування шахрайства, фішингу, атак типу DoS/DDoS. Аналіз шкідливого програмного забезпечення. Особливості роботи з інцидентами у соціальних мережах.

Тема 6. Цифрова криміналістика в системі реагування на інциденти (IR). Місце цифрової криміналістики у процесі Incident Response. Взаємодія з командами SOC та CERT. Практичні кейси реагування.

Тема 7. Аналіз доказів, звітність та етичні аспекти. Методи аналізу цифрових доказів. Підготовка експертних висновків та звітів. Етичні стандарти та професійна відповідальність.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин									
	денна форма					Заочна форма				
	усього	у тому числі				усього	у тому числі			
		лекц.	лаб.	практ.	сам. роб.		лекц.	лаб.	практ.	сам. роб.
Тема 1. Вступ до цифрової криміналістики та її місце в системі кібербезпеки	12	2		2	8	15				15
Тема 2. Правові та організаційні основи цифрової криміналістики	18	4		4	10	17	2			15
Тема 3. Цифрові докази та сліди: види, властивості та фіксація	18	4		4	10	17			2	15
Тема 4. Методи та засоби збору цифрових доказів	18	4		4	10	17	2			15
Тема 5. Особливості розслідування окремих видів кіберзлочинів	18	4		4	10	17			2	15
Тема 6. Цифрова криміналістика в системі реагування на інциденти (IR)	18	4		4	10	17	2			15
Тема 7. Аналіз доказів, звітність та етичні аспекти	18	4		4	10	20				20
Усього годин	**120**	**26**	**0**	**26**	**68**	**120**	**6**	**0**	**4**	**110**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЗАЛІК										

5. ПРАКТИЧНІ РОБОТИ

Назва теми	Кількість годин	
	Денна форма	Заочна форма
1. Ознайомлення з базовими поняттями цифрової криміналістики та її роллю у кібербезпеці (аналіз кейсів).	2	
2. Аналіз законодавчих вимог України та міжнародних стандартів (порівняльна таблиця).	2	
3. Розробка моделі організації роботи експерта-криміналіста (схема ролей та відповідальності).	2	2
4. Класифікація цифрових доказів (практичне завдання з групування артефактів).	2	
5. Фіксація та документування цифрових слідів (створення протоколу огляду).	2	2
6. Створення образу диска за допомогою open-source утиліт (Autopsy, FTK Imager).	2	
7. Вилучення даних з мобільного пристрою (демонстрація утиліт).	2	
8. Документування ланцюга збереження доказів (Chain of Custody)..	2	

9. Розслідування інциденту фішингу (аналіз електронних листів та заголовків).	2	
10. Аналіз DoS/DDoS-атаки за мережевими логами.	2	
11. Виявлення та дослідження шкідливого ПЗ (базовий статичний аналіз).	2	
12. Форензичний розбір інциденту (робота з журналами подій Windows/Linux).	2	
13. Моделювання взаємодії з SOC/CERT у процесі Incident Response.	2	
Всього	**26**	**4**

6. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни включаються:
1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до практичних занять.
4. Консультації з викладачем протягом семестру.
5. Самостійне опрацювання окремих питань навчальної дисципліни.
6. Підготовка та виконання контрольних робіт.
7. Підготовка до підсумкового контролю.

Тематика та питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1. Вступ до цифрової криміналістики та її місце в системі кібербезпеки** Поняття, мета та соціальне значення цифрової криміналістики (форензики) як прикладної судової науки. Історичні етапи становлення дисципліни: від комп'ютерної експертизи 1970-х до сучасних методів розслідування кіберінцидентів. Співвідношення понять «кібербезпека», «кіберрозслідування», «цифрова криміналістика» та «eDiscovery». Основні концепції та методологія: реактивний та проактивний підходи, принципи збереження цілісності доказів. Професійна діяльність цифрового криміналіста: необхідні технічні та юридичні компетенції, сфери працевлаштування. Місце дисципліни в системі наук: інтеграція IT-знань, криміналістики та процесуального права. Вплив технологічних трендів (хмарні обчислення, IoT, криптовалюти) на розвиток методів форензики.	8	15
2	**Тема 2. Правові та організаційні основи цифрової криміналістики** Нормативно-правова база України у сфері кібербезпеки та протидії кіберзлочинності: Кримінальний процесуальний кодекс, Закони «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах». Міжнародні стандарти: Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція), директиви ЄС. Поняття електронних (цифрових) доказів: вимоги до автентичності, цілісності, допустимості та належності. Процесуальні умови зняття інформації з каналів зв'язку, проведення	10	15

	огляду, обшуку, вилучення носіїв. Судова комп'ютерно-технічна експертиза: види, підстави призначення, права та обов'язки експерта. Організація взаємодії слідчих, експертів та ІТ-фахівців під час розслідування.		
3	**Тема 3. Цифрові докази та сліди: види, властивості та фіксація** Поняття цифрової інформації та слідів її створення, модифікації, транспортування, видалення. Класифікація цифрових доказів: волатильні (оперативна пам'ять, мережеві з'єднання) та неволатильні дані (дискові носії, логи, реєстр). Властивості цифрових доказів: автентичність, цілісність, допустимість, релевантність. Доказовий ланцюжок (Chain of Custody): правила документування переміщення та обробки доказів від вилучення до судового розгляду. Робота з метаданими, системними логами, файлами журналів подій. Методи фіксації слідів у протоколах огляду місця події: фото-, відеофіксація, хешування, створення біт-в-біт копій. Вплив порушення процедур фіксації на допустимість доказів у суді.	10	15
4	**Тема 4. Методи та засоби збору цифрових доказів** Алгоритм дій під час огляду місця події кіберзлочину: вилучення енергозалежних даних, робота з увімкненими/вимкненими пристроями, ізоляція від мережі. Створення криміналістичних образів носіїв: принципи біт-в-біт копіювання, верифікація через криптографічні хеш-функції (MD5, SHA-256). Спеціалізоване програмне забезпечення для цифрової криміналістики: огляд інструментів (Autopsy, FTK, Volatility, Wireshark), робота в середовищі Linux/Windows. OSINT-розвідка: аналіз відкритих джерел (реєстри, соціальні мережі, публічні бази) для збору доказової інформації. Відновлення видалених даних: методи роботи з файловими системами, аналіз нерозподіленого простору. Криптографічний захист доказів: забезпечення незмінності через хешування та цифрові підписи.	10	15
5	**Тема 5. Особливості розслідування окремих видів кіберзлочинів** Криміналістична характеристика кіберзлочинності: суб'єкт, об'єкт, спосіб вчинення, слідова картина. Розслідування фінансових злочинів: інтернет-шахрайства, крадіжки через системи дистанційного банківського обслуговування, кардшейрінг, аналіз транзакцій. Злочини проти власності та інтелектуальної прав: піратство, криптоджекінг, незаконне копіювання ПЗ. Кіберзлочини проти особистості: кіберсталкінг, кібербулінг, фішинг, крадіжка ідентичності – методи збору доказів у месенджерах та соціальних мережах. Розслідування злочинів у Dark Web: особливості роботи з анонімними мережами та криптовалютними гаманцями. Виявлення та фіксація дій інсайдерів, аналіз підробки електронних документів (податкові декларації, реєстри, «Дія»).	10	15
6	**Тема 6. Цифрова криміналістика в системі реагування на інциденти (IR)** Інтеграція цифрової криміналістики та Incident Response (IR): фази	10	15

	реагування, роль форензики на етапах containment, eradication, recovery. Кваліфікована фіксація слідів під час підозри на кібератаку: збереження волатильних даних, ізоляція зразків шкідливого ПЗ. Мережева криміналістика: аналіз трафіку (PCAP), виявлення вторгнень (IDS/IPS логи), реконструкція сесій, робота з логами фаєрволів та проксі. Криміналістика мобільних пристроїв (Mobile Forensics): вилучення даних зі смартфонів (Android/iOS), аналіз дзвінків, SMS, месенджерів, геолокації, хмарних синхронізацій. Відео-криміналістика: аналіз метаданих відео, покращення якості, ідентифікація об'єктів, верифікація автентичності записів. Запобігання повторенню інцидентів на основі результатів розслідування: формування рекомендацій із посилення захисту.		
7	**Тема 7. Аналіз доказів, звітність та етичні аспекти** Методика аналізу зібраних даних: кореляція подій, відтворення хронології (timeline analysis), побудова графів взаємодій. Підготовка звіту експерта/спеціаліста з цифрової криміналістики: структура, мова викладу, вимоги до об'єктивності та відтворюваності результатів. Презентація цифрових доказів у суді: особливості доведення, захист висновків від заперечень сторони захисту, демонстрація технічних аспектів нетехнічній аудиторії. Труднощі застосування цифрової криміналістики: швидка зміна технологій, шифрування, антифорензичні методи, міжюрисдикційні бар'єри. Етичні аспекти діяльності кіберкриміналіста: академічна доброчесність, конфіденційність, дотримання прав людини, уникнення конфлікту інтересів. e-Discovery: використання цифрових технологій у цивільних та господарських спорах, автоматизація пошуку релевантної інформації у великих масивах даних.	10	20
	Всього	**68**	**110**

7. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Види контролю	**Складові оцінювання**	
	Для екзамену	**Для заліку**
поточний контроль, який здійснюється у ході: проведення практичних (лабораторних) занять, виконання самостійної роботи, індивідуальних завдань, дослідна робота здобувача тощо.	**50%**	**100%**
підсумковий контроль	**50%**	

Методи діагностики знань (контролю)	фронтальне опитування; наукова доповідь, реферати, усне повідомлення, індивідуальне опитування; робота у групах; ділова гра, розв`язання ситуаційних завдань, кейсів, практичних завдань, екзамен

8. ОЦІНЮВАННЯ ЗДОБУВАЧІВ ВИЩОЇ ТА ФАХОВОЇ ПЕРДВИЩОЇ ОСВІТИ ЗА НАВЧАЛЬНУ ДИСЦИПЛІНУ У МІЖНАРОДНОМУ ГУМАНІТАРНОМУ УНІВЕРСИТЕТІ

(*поточний контроль, підсумковий контроль, загальний результат оцінювання)*

ЗАЛІК

Поточний контроль		
Види роботи	**Планові терміни виконання**	**Форми контролю та з**
Систематичність і активність роботи на практичних (лабораторних) з		
1.1. Підготовка до практичних (лабораторних) занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоє час практичних (лабораторних) за
Виконання завдань для самостійного опрацювання		
1.2. Індивідуальне тестування, завдання, підготовка реферату (есе) за заданою тематикою	Відповідно до робочої програми та розкладу занять	Розгляд відповідного матеріалу пі занять або ІКР[1], перевірка конспе текстів тощо
Виконання індивідуальних завдань, дослідна робота здобувача		
1.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	Відповідно до робочої програми та розкладу занять	Обговорення результатів проведен аудиторних занять, наукових конф круглих столів.
Разом балів за поточний контроль		
Загальний результат оцінювання		

Поточний контроль знань здобувачів освіти при формі контролю **залік** (максимум 100 балів) оцінюється за шкалою *(«2», «3», «4», «5»)*, з обов'язковим переведенням балів за кожний вид роботи таким чином:

- за підготовку до аудиторних занять (максимум 60 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості практичних (лабораторних) занять, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 12;
- за виконання завдань для самостійного опрацювання (тестування, завдання, підготовка реферату (есе) за заданою тематикою) (максимум 20 балів) здобувачу освіти необхідно мати не менше 1/2 оцінок від загальної кількості програмного матеріалу, що виноситься на самостійне вивчення, для переводу зазначених балів середньоарифметична оцінка множиться на коефіцієнт 4;
- за інші види індивідуальних завдань, в т.ч. підготовку наукових публікацій, участь у роботі круглих столів, конференцій тощо (максимум 20- балів) здобувачу освіти необхідно мати не

[1] Індивідуально-консультативна робота викладача зі здобувачами

менше 1/2 оцінок від загальної кількості інших видів індивідуальних завдань, для переводу балів за підготовку до аудиторних занять середньоарифметична оцінка множиться на коефіцієнт 4.

КРИТЕРІЇ ОЦІНЮВАННЯ ЗА ПОТОЧНИЙ КОНТРОЛЬ

- «2»- виставляється за неправильну відповідь (письмову роботу), яка не відповідає змісту теми та свідчить про нерозуміння її основних положень;
- «3» -виставляється за відповідь (письмову роботу), яка відповідає змісту теми, але є неповною і неточною у визначенні понять, свідчить про неповне розуміння основних положень навчального матеріалу, свідчить про те, що знання студента мають фрагментарний, поверховий характер;
- «4» - оцінюється правильна і обґрунтована відповідь (письмова робота), з якої видно, що студент знає й розуміє теоретичний матеріал в обсязі навчальної теми, володіє необхідними навичками, не допускає суттєвих помилок.

«5» - оцінюється повна, правильна, ґрунтовна відповідь (письмова робота) на запитання теми, що передбачає логічність і послідовність викладу матеріалу, володіння термінологією, показує вміння повно й глибоко використовувати

9. КРИТЕРІЇ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ (для іспиту / заліку)

Рівень знань оцінюється:

- «відмінно» / «зараховано» A - від 90 до 100 балів. Студент виявляє особливі творчі здібності, вміє самостійно знаходити та опрацьовувати необхідну інформацію, демонструє знання матеріалу, проводить узагальнення і висновки. Був присутній на лекціях та семінарських заняттях, під час яких давав вичерпні, обґрунтовані, теоретично і практично правильні відповіді, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» B - від 82 до 89 балів. Студент володіє знаннями матеріалу, але допускає незначні помилки у формуванні термінів, категорій, проте за допомогою викладача швидко орієнтується і знаходить правильні відповіді. Був присутній на лекціях та семінарських заняттях, має конспект з виконаними завданнями до самостійної роботи, презентував реферат (есе) за заданою тематикою, проявляє активність і творчість у науково-дослідній роботі;
- «добре» / «зараховано» C - від 74 до 81 балів. Студент відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, з допомогою викладача може аналізувати навчальний матеріал, але дає недостатньо обґрунтовані, невичерпні відповіді, допускає помилки. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, реферату та активність у науково-дослідній роботі;
- «задовільно» / «зараховано» D - від 64 до 73 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на середньому рівні, допускає помилки, серед яких є значна кількість суттєвих. При цьому враховується наявність конспекту з виконаними завданнями до самостійної роботи, рефератів (есе);
- «задовільно» / «зараховано» E - від 60 до 63 балів. Студент був присутній не на всіх лекціях та семінарських заняттях, володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні, на всі запитання дає необґрунтовані, невичерпні відповіді, допускає помилки, має неповний конспект з завданнями до самостійної роботи.
- «незадовільно з можливістю повторного складання» / «не зараховано» FX – від 35 до 59 балів. Студент володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.
- «незадовільно з обов'язковим повторним вивченням дисципліни» / «не зараховано» F – від 0 до 34 балів. Студент не володіє навчальним матеріалом.

ТАБЛИЦЯ ВІДПОВІДНОСТІ ЗАГАЛЬНИХ РЕЗУЛЬТАТІВ ОЦІНЮВАННЯ ЗНАНЬ ЗА РІЗНИМИ ШКАЛАМИ

100-бальною шкалою	Шкала за ECTS	За національною шкалою	
		екзамен	залік
90-100	A	Відмінно	Зараховано
82-89	B	Добре	
74-81	C		
64-73	D	Задовільно	
60-63	E		
35-59	FX	Незадовільно	Не зараховано
1-34	F		

10. ДОТРИМАННЯ ВИМОГ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Викладання та засвоєння навчальної дисципліни передбачає неухильне дотримання вимог академічної доброчесності, яка регулюється Законом України "Про освіту" (Відомості Верховної Ради (ВВР), 2014, № 37-38, ст.2004), «Методичними рекомендаціями для закладів вищої освіти з підтримки принципів академічної доброчесності» (Лист МОН № 1/9-650 від 23.10.18 року), іншими нормативними документами. Зокрема, основні засади дотримання академічної доброчесності визначено у «Положенні про академічну доброчесність у Міжнародному гуманітарному університеті», «Кодексі академічної доброчесності Міжнародного гуманітарного університету» та «Інструкції щодо процедури технічної перевірки на наявність текстових запозичень (академічного плагіату)», затвердженої наказом МГУ від 03.05.2024 р., № 708а.

Відповідно до ст.42 Закону України "Про освіту" академічна доброчесність - це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна
Основна

1. Вступ до цифрової криміналістики : навч. посіб. / [В. Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова] ; за ред. В. Ю. Шепітька ; Нац. юрид. ун-т ім. Ярослава Мудрого. Харків : Право, 2025. 124 с
2. Основи кримінального аналізу: підручник / Бабенко А.М., Заєць О.М., Некрасов В.А., **Ісмайлов К.Ю.,** Пефтієв Д.О. та ін.; за заг. ред. Користіна О.Є., 2019. Одеса. 296 с.

3. Навчальний посібник Тактичний кримінальний аналіз: теорія і практика / Н.П. Свиридюк, О.М. Цильмак, Заєць О.М., Ісмайлов К.Ю., Некрасов В.А. за заг. ред. Користіна О.Є.; МВС України, ДНДІ, ОДУВС. Одеса: РВВ ОДУВС, 2019. 216 с.
4. Реалізація філософії «Intelligence-led Policing» в системі кримінального аналізу Національної поліції України: монографія / Користін О., Бутко Р., Денисенко Б., **Ісмайлов К.Ю**. та ін., за заг. ред. Користіна О.Є. Київ: «ВАІТЕ»,
5. 2024. 444 с.
6. Інноваційні методи та цифрові технології в криміналістиці й судовій експертизі : монографія / [В. Ю. Шепітько, Г. К. Авдєєва, В. М. Шевчук та ін.] ; за заг. ред. В. Ю. Шепітька ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 208 с.
7. Шепітько В. Ю. Цифрова криміналістика та її роль у формуванні доказової інформації в умовах воєнних дій : монографія / В. Ю. Шепітько, М. В. Шепітько, К. В. Латиш, М. В. Капустіна, Є. Є. Демидова ; за заг. ред. В. Ю. Шепітька. Харків : Право, 2025. 200 с. ISBN 978-617-8617-93-6.
8. Якименко І. З. Цифрова криміналістика : консп. лекцій / уклад. І. З. Якименко. Тернопіль : ТНЕУ, 2019. 109 с.
9. Інформаційна безпека : навч. посіб. / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. Ю. Я. Бобала та І. В. Горбатого; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». Львів : Вид-во Львів. політехніки, 2019. 580 с.
10. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 460 с.
11. Методичні рекомендації щодо виявлення, фіксації та вилучення криміналістично значущої інформації з мобільних пристроїв під час розслідування кримінальних правопорушень / Д.С. Афонін, К.Ю. Ісмайлов, Д.В. Лісніченко, О.І. Постол. Одеса: Одеський державний університет внутрішніх справ, 2018. 38 с.
12. Навчально-методичні рекомендації щодо пошуку оперативнозначущої інформації на електронних носіях / К.Ю. Ісмайлов, В.О. Русавський, Л.В. Лефтеров. Одеса: Одеський державний університет внутрішніх справ, 2019. 14 с.

Допоміжна

1. Злочини проти інформаційної безпеки держави : поняття, виявлення, досудове розслідування : монографія / І. В. Гора, В. А. Колесник, В. В. Малюк, В. О. Ходанович, А. М. Черняк, Л. І. Щербина. Київ : 7БЦ, 2023. 512 с.
2. Гора І. В. До питання про цифрову криміналістику в системі криміналістичних знань / І. В. Гора, В. А. Колесник, І. І. Попович // Науковий вісник Міжнародного гуманітарного університету. Сер. : Юриспруденція. 2024. № 68. С. 86–91.
3. Ціжма Ю. І. Діджиталізація як сучасна рушійна сила вдосконалення судово-експертної діяльності / Ю. І. Ціжма, О. А. Лишак, О. А. Ціжма // Криміналістика і судова експертиза : міжвідом. наук.-метод. зб. / КНДІ судових експертиз ; редкол. : О. Г. Рувін [та ін.]. Київ : Вид. Ліра-К, 2023. Вип. 68. С. 40-47.
4. Костенко М. В. Особливості інноваційного процесу у сфері криміналістики / М. В. Костенко // Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці : матеріали міжнар. «круглого столу» (Харків, 12 груд. 2019 р.) / редкол. : В. Ю. Шепітько, В. А. Журавель, В. М. Шевчук, Г. К. Авдєєва. Харків : Право, 2019. — С. 72–75.
5. Грохольський В.Л., Ісмайлов К.Ю., Форос Г.В. Науково-практичний коментар до Закону України «Про основні засади забезпечення кібербезпеки України» / за заг. ред. д.юн., проф. В.Л. Грохольського. Одеса: ОДУВС, 2020. 142 с.

6. OSINT Open Source Intelligence. Інструменти та методи: навчальний посібник / Користін О., Демедюк С., Ісмайлов К., Ланде Д. та ін., за заг. ред. Користіна О.Є., Демедюка С.В. Київ: 7БЦ, 2025. 460 с.
7. Інформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро : ДДУВС, 2021. 492 с.

Інформаційні ресурси

1. Національна бібліотека України імені В. І. Вернадського : веб-сайт. URL: http://www.nbuv.gov.ua.
2. Верховна Рада України. Законодавство України : офіційний веб-портал. URL: https://zakon.rada.gov.ua.
3. Кіберполіція Національної поліції України : офіційний веб-сайт. URL: https://cyberpolice.gov.ua.
4. Державна служба спеціального зв'язку та захисту інформації України : офіційний веб-сайт. URL: https://cip.gov.ua.
5. Кіберцентр UA30 (CERT-UA) : офіційний веб-сайт. URL: https://cert.gov.ua.
6. Єдиний державний реєстр судових рішень : веб-сайт. URL: https://reyestr.court.gov.ua
7. Наукова періодика України : портал електронних фахових видань. URL: http://nbuv.gov.ua/ujrn.
8. Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса : офіційний веб-сайт. URL: https://nncise.org.ua.
9. Слідча практика: віртуальний огляд місця події. URL: https://ved.com.ua