Міжнародний гуманітарний університет
Факультет права та економіки
Кафедра кримінального права, процесу та криміналістики

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Комп'ютерна криміналістика

Галузь знань 26 «Цивільна безпека»
Спеціальність 262 «Правоохоронна діяльність»
Назва освітньої програми Правоохоронна діяльність
Рівень вищої освіти перший (бакалаврський) рівень

Розробники і викладачі *(зазначаються розробники і викладачі, які викладають дисципліну - посада, наук. ступінь, вчене звання, П.І.Б.)*	**Контактний тел.**	**E-mail**
д.ю.н., професор Подобний О.О.	067-766-85-19	kafedraKPPK@i.ua

1. АНОТАЦІЯ ДО КУРСУ

Навчальна дисципліна «Комп'ютерна криміналістика» покликана забезпечити раціональне досягнення всіх завдань кримінального провадження (ст. 2 КПК У країни), передусім, швидкого, повного й неупередженого розслідування та судового розгляду кримінальних правопорушень, що вчинюються із використанням високих інформаційних технологій.

Криміналістичні методи і засоби можуть використовуватися всюди, де існує діяльність, пов'язана з доказуванням, установленням певних фактів. Головна мета курсу «Комп'ютерна криміналістика» – показати ті можливості, які відкриваються у збиранні, дослідженні й використанні доказової інформації в кримінальних провадженнях про вчинення кіберзлочинів.

Передумовами для вивчення курсу «Комп'ютерна криміналістика» є опанування навичками і компетенціями, що пов'язаними з дисциплінами «Тактико-спеціальна підготовка», «Судові та правоохоронні органи України», «Державна таємниця», «Забезпечення прав людини в правоохоронній діяльності», «Криміналістика», «Основи оперативно-розшукової діяльності».

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

У процесі реалізації програми дисципліни «Комп'ютерна криміналістика» формуються наступні компетентності із передбачених освітньою програмою:

Інтегральна компетентність

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

Загальні компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК7. Здатність до адаптації та дії в новій ситуації.

ЗК8. Здатність приймати обґрунтовані рішення, критичного, стратегічного, дизайн-мислення.

Спеціальні (фахові) компетентності

СК3. Здатність професійно оперувати категоріально-понятійним апаратом права і правоохоронної діяльності.

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.

СК10. Здатність визначати належні та придатні для юридичного аналізу факти.

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

СК15. Здатність до застосування спеціальної техніки, спеціальних, оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності.

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

СК19. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом.

Навчальна дисципліна «Комп'ютерна криміналістика» забезпечує досягнення програмних результатів навчання (РН), передбачених освітньою програмою:

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.

РН10. Виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

РН12. Адаптуватися і ефективно діяти за звичних умов правоохоронної діяльності та за умов ускладнення оперативної обстановки.

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.

РН17. Використовувати основні методи та засоби забезпечення правопорядку в державі, дотримуватись прав і свобод людини і громадянина, попередження та припинення нелегальної (незаконної) міграції та інших загроз національної безпеки держави (кібербезпеку, економічну та інформаційну безпеку, тощо).

РН18. Застосовувати штатне озброєння підрозділу (вогнепальну зброю, спеціальні засоби, засоби фізичної сили); інформаційні системи, інформаційні технології, 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.

РН21. Організовувати заходи щодо режиму секретності та захисту інформації.

Заплановані результати навчання за навчальною дисципліною

Знання:

- історія криміналістики та комп'ютерної криміналістики; предмет комп'ютерної криміналістики, її систему, категорії; завдання, принципи, методи; особливості застосування теорій криміналістичної ідентифікації та групофікації в розслідуванні крмп'ютерних злочинів; теорію криміналістичної діагностики;

- загальні положення компютеро-криміналістичної техніки; електронне слідознавство; інформаційно-довідкове забезпечення розслідування та його автоматизацію;

- загальні положення компютеро-криміналістичної тактики; організацію і планування розслідування; тактику проведення у розслідуванні комп'ютерних злочинів таких процесуальних дій як огляд, обшук, слідчий експеримент, використання спеціальних знань, негласних слідчих (розшукових) дій;

- загальні положення криміналістичної методики під час розслідування комп'ютерних злочинів.

Уміння:

- вільно орієнтуватися в криміналістичних знаннях з метою використання їх у розслідуванні кіберзлочинів;

- оцінювати первинну інформацію про кіберзлочин та визначати слідчу ситуацію, обирати програми розслідування, розробляти відповідні плани; проводити розслідування злочину, керуючись висунутими версіями і планами;

- визначати необхідність застосування в конкретній слідчій ситуації та використовувати належні техніко-криміналістичні засоби, прийоми і методи, призначені для виявлення, фіксації, вилучення, забезпечення схоронності доказів у електронній формі в інтересах розкриття і розслідування кіберзлочинів;

- визначати необхідність і можливість призначення в конкретній слідчій ситуації криміналістичної експертизи, формулювати питання, які належить вирішити експертові, готувати матеріали, що надсилаються на експертизу з урахуванням вимог, які ставляться до них та їх оформлення;

- розробляти з використанням криміналістичних рекомендацій план підготовки і проведення слідчої дії, тактичної операції, використання спеціальних знань, проводити відповідну слідчу дію, призначати судову експертизу, організовувати взаємодію слідчого з працівниками оперативних підрозділів й іншими суб'єктами під час розслідування кіберзлочинів з використанням рекомендованих криміналістикою тактичних прийомів.

3. ОБСЯГ ТА ОЗНАКИ КУРСУ

Загалом		**Вид заняття** (денне відділення / заочне відділення)			**Ознаки курсу**		
ЄКТС	**годин**	**Лекційні заняття**	**Практичні заняття**	**Самостійна робота**	**Курс, (рік навчання)**	**Семестр**	**Обов'язкова / вибіркова**
4	90	16/4	14/4	60/82	3	6	Вибіркова

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	**Кількість годин**							
	денна форма				**Заочна форма**			
	усього	**у тому числі**			**усього**	**у тому числі**		
		лекц.	**прак**	**сам. роб.**		**лекц.**	**прак**	**сам. роб.**
Тема 1. Загальні положення комп'ютерної криміналістики	10	2		8	11			11
Тема 2 Технічні засади комп'ютерної криміналістики	10	2	2	6	12	2	2	8
Тема 3. Тактичні засади комп'ютерної криміналістики	10	2	2	6	12	2	2	8
Тема 4. Криміналістична характеристика кіберзлочинів	12	2	2	8	11			11
Тема 5. Відкриття кримінального провадження та взаємодія під час розслідування кіберзлочинів	12	2	2	8	11			11
Тема 6. Організація розслідування злочинів у кіберпросторі	12	2	2	8	11			11
Тема 7. Використання спеціальних знань у розслідуванні кіберзлочинів	12	2	2	8	11			11
Тема 8. Особливості розслідування окремих видів кіберзлочинів	12		2	8	11			11
Усього годин	**90**	**16**	**14**	**60**	**90**	**4**	**4**	**82**
ПІДСУМКОВИЙ КОНТРОЛЬ – ЗАЛІК								

5. ТЕХНІЧНЕ Й ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ / ОБЛАДНАННЯ

Студенти отримують теми та питання курсу, основну і додаткову літературу, рекомендації, завдання та оцінки за їх виконання як традиційним шляхом, так і з використанням університетської платформи он-лайн навчання на базі Moodle. Окрім того, практичні навички у пошуку та аналізу інформації за курсом, з оформлення індивідуальних завдань студенти отримують, користуючись університетськими комп'ютерними класами та бібліотекою. Техічне забезпечення: Kali Linux - дистрибутив Debian-похідних Linux, призначений для цифрової криміналістики і тестування на проникнення

6. ПИТАННЯ ДО ПРАКТИЧНИХ ЗАНЯТЬ

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.Загальні положення комп'ютерної криміналістики** 1. Особливості кіберпростору як об'єкта криміналістичного дослідження 2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі 3. Криміналістична класифікація кіберзлочинів.		
2	**Тема 2. Технічні засади комп'ютерної криміналістики** 1. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп'ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв'язку; захищені модульні системи зберігання даних. 2. Технічні канали витоку інформації та способи її несанкціонованого зняття. 3. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв).	2	2
3	**Тема 3. Тактичні засади комп'ютерної криміналістики** 1. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп'ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску. 2. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук). 3. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані дані).	2	2
4	**Тема 4. Криміналістична характеристика кіберзлочинів** 1. Структура криміналістичної характеристики кіберзлочинів. 2. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів. 3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів. 4. Характеристика типових способів/технологій вчинення кіберзлочинів.	2	
5	**Тема 5. Відкриття кримінального провадження та взаємодія під час розслідування кіберзлочинів** 1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин. 2. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що	2	

	можуть свідчити про вчинення певного виду кіберзлочинів. 3. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються. 4. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.		
6	**Тема 6. Організація розслідування злочинів у кіберпросторі** 1. Періодизація розслідування кіберзлочинів. 2. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання. 3. Тактичні операції розслідування кіберзлочинів.	2	
7	**Тема 7. Використання спеціальних знань у розслідуванні кіберзлочинів** 1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів. 2. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. 3. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності; експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).	2	
8	**Тема 8. Особливості розслідування окремих видів кіберзлочинів** 1. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі. 2. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі. 3. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. 4. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.	2	
	Всього	**16**	**4**

7. САМОСТІЙНА РОБОТА

До самостійної роботи студентів щодо вивчення дисципліни «Комп'ютерна криміналістика» включаються:

1. Знайомство з науковою та навчальною літературою відповідно зазначених у програмі тем.
2. Опрацювання лекційного матеріалу.
3. Підготовка до семінарських занять.
4. Самостійне опрацювання окремих питань навчальної дисципліни.
5. Підготовка до підсумкового контролю.

Тематика і питання до самостійної підготовки та індивідуальних завдань

№ з/п	Назва теми	Кількість годин	
		денна форма	заочна форма
1	**Тема 1.Загальні положення комп'ютерної криміналістики** 1. Особливості кіберпростору як об'єкта криміналістичного дослідження 2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі 3. Криміналістична класифікація кіберзлочинів. **Реферати** 1. Особливості кіберпростору як об'єкта криміналістичного дослідження 2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі 3. Криміналістична класифікація кіберзлочинів.	8	11
2	**Тема 2. Технічні засади комп'ютерної криміналістики** 1. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп'ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв'язку; захищені модульні системи зберігання даних. 2. Технічні канали витоку інформації та способи її несанкціонованого зняття. 3. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв). **Реферати** 1. Технічні канали витоку інформації та способи її несанкціонованого зняття.	6	8
3	**Тема 3. Тактичні засади комп'ютерної криміналістики** 1. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп'ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску. 2. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук). 3. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані дані). **Реферати** 1. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів. 2. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів. 3. Методи компютерно-технічної експертизи.	6	8
4	**Тема 4. Криміналістична характеристика кіберзлочинів** 1. Структура криміналістичної характеристики кіберзлочинів. 2. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів. 3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів. 4. Характеристика типових способів/технологій вчинення кіберзлочинів.	8	11

	Реферати 1. Структура криміналістичної характеристики кіберзлочинів. 2. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення кіберзлочинів. 3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів кіберзлочинів. 4. Характеристика типових способів/технологій вчинення кіберзлочинів.		
5	**Тема 5. Відкриття кримінального провадження та взаємодія під час розслідування кіберзлочинів** 1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин. 2. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів. 3. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються. 4. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин. **Реферати** 1. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. 2. Джерела інформації про кіберзлочин. 3. Організаційні форми початку кримінального провадження щодо кіберзлочинів. 4. Джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів. 5. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються. 6. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.	8	11
6	**Тема 6. Організація розслідування злочинів у кіберпросторі** 1. Періодизація розслідування кіберзлочинів. 2. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання. 3. Тактичні операції розслідування кіберзлочинів. **Реферати** 1. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв'язання. 2. Тактичні операції розслідування кіберзлочинів.	8	11
7	**Тема 7. Використання спеціальних знань у розслідуванні кіберзлочинів** 1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів. 2. Залучення експерта для проведення судової комп'ютерно-технічної експертизи під час розслідування кіберзлочинів. 3. Залучення експерта для проведення інших судових експертиз під час розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності; експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД). **Реферати** **Тема 7. Використання спеціальних знань у розслідуванні кіберзлочинів** 1. Специфіка залучення спеціаліста під час розслідування кіберзлочинів.	8	11

8	**Тема 8. Особливості розслідування окремих видів кіберзлочинів** 1. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі. 2. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі. 3. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. 4. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі. **Реферати** 1. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі. 2. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі. 3. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. 4. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.	8	11
	Всього	**60**	**82**

8. ВИДИ ТА МЕТОДИ КОНТРОЛЮ

Робоча програма навчальної дисципліни передбачає наступні види та методи контролю:

Види контролю	Складові оцінювання
поточний контроль, який здійснюється у ході: проведення практичних занять, виконання індивідуального завдання; проведення консультацій та відпрацювань.	**50%**
підсумковий контроль, який здійснюється у ході проведення заліку.	**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, залік

Питання до заліку

1. Особливості кіберпростору як об’єкта криміналістичного дослідження
2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі
3. Криміналістична класифікація кіберзлочинів.
4. Спеціальні технічні засоби: апаратні; експертні програми; набори хешей; архівування; криміналістичні інформаційні системи; програмні засоби розслідування комп’ютерних злочинів; апаратно-програмні засоби шифрування мобільного зв’язку; захищені модульні системи зберігання даних.
5. Технічні канали витоку інформації та способи її несанкціонованого зняття.
6. Методи та засоби блокування технічних каналів витоку інформації (захист інформації від витоку акустичним, віброакустичним, оптоелектронним каналами та від закладних пристроїв).
7. Специфіка тактики проведення слідчих (розшукових) дій у розслідуванні кіберзлочинів: огляд комп’ютера; вилучення лог-файлів та їх доказове значення; тактика обшуку; пошук інформації на диску.
8. Тактичні прийоми негласних слідчих (розшукових) дій у розслідуванні кіберзлочинів: перехоплення та дослідження трафіку; дослідження статистики трафіку; інші дані про трафік (аналіз назв пакетів, поштова скринька, достовірність, посвідчення); кефлогери; інтернет-моніторинг (пошук).
9. Методи компютерно-технічної експертизи (дослідження файлових систем, копіювання носіїв, хеж-функції для встановлення тотожності, дослідження файлів; зашифровані дані).
10. Структура криміналістичної характеристики кіберзлочинів.
11. Характеристика типових предметів посягання та їх зв’язок з мотивами вчинення кіберзлочинів.
12. Характеристика та взаємозв’язок типової особи злочинця й типових слідів кіберзлочинів.
13. Характеристика типових способів/технологій вчинення кіберзлочинів.
14. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Джерела інформації про кіберзлочин.
15. Організаційні форми початку кримінального провадження щодо кіберзлочинів та джерела обставин, що можуть свідчити про вчинення певного виду кіберзлочинів.
16. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються.
17. Особливості відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.
18. Періодизація розслідування кіберзлочинів.
19. Типові слідчі ситуації у розслідуванні кіберзлочинів, тактичні завдання та засоби їх розв’язання.
20. Тактичні операції розслідування кіберзлочинів.
21. Спеціальні знання та специфіка залучення спеціаліста під час розслідування кіберзлочинів.
22. Залучення експерта для проведення судової комп’ютерно-технічної експертизи під час розслідування кіберзлочинів.
23. Залучення експерта для проведення інших судових експертиз підчас розслідування кіберзлочинів: експертиза у сфері інтелектуальної власності; експертиза телекомунікаційних систем (обладнання) та засобів; комплексні експертизи (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).
24. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов’язані з фінансово-економічною сферою відносин у кіберпросторі.

25. Розслідування кіберзлочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі.

26. Розслідування злочинів, вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі.

27. Розслідування кіберзлочинів, вчинених з ідейних мотивів, пов'язаних зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

9. ОЦІНЮВАННЯ ПОТОЧНОЇ, САМОСТІЙНОЇ ТА ІНДИВІДУАЛЬНОЇ РОБОТИ СТУДЕНТІВ З ПІДСУМКОВИМ КОНТРОЛЕМ У ФОРМІ ЕКЗАМЕНУ/ ЗАЛІКУ

Денна форма навчання			
Поточний контроль			
Види роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи на семінарських (практичних) заняттях			
1.1. Підготовка до практичних занять	Відповідно до робочої програми та розкладу занять	Перевірка обсягу та якості засвоєного матеріалу під час практичних занять	**25**
Виконання завдань для самостійного опрацювання			
1.2. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення	-//-	Розгляд відповідного матеріалу під час аудиторних занять або ІКР[1], перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
1.3. Підготовка реферату (есе) за заданою тематикою	Відповідно до розкладу занять і графіку ІКР	Обговорення (захист) матеріалів реферату (есе)	**10**
1.4. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	-//-	Обговорення результатів проведеної роботи під час аудиторних занять або ІКР, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен / залік			**50**
Всього балів			**100**

[1] Індивідуально-консультативна робота викладача зі студентами

Заочна форма навчання			
Поточний контроль			
Види самостійної роботи	**Планові терміни виконання**	**Форми контролю та звітності**	**Максимальний відсоток оцінювання**
Систематичність і активність роботи під час аудиторних занять			
1.1. Підготовка до аудиторних занять	Відповідно до розкладу	Перевірка обсягу та якості засвоєного матеріалу під час аудиторних занять	**15**
За виконання контрольних робіт (завдань)			
1.2. Підготовка контрольних робіт	-//-	Перевірка контрольних робіт (завдань)	**15**
Виконання завдань для самостійного опрацювання			
1.3. Підготовка програмного матеріалу (тем, питань), що виноситься на самостійне вивчення	-//-	Розгляд відповідного матеріалу під час аудиторних занять або ІКР, перевірка конспектів навчальних текстів тощо	**10**
Виконання індивідуальних завдань (науково-дослідна робота студента)			
2.1. Підготовка реферату (есе) за заданою тематикою	Відповідно до графіку ІКР	Обговорення (захист) матеріалів реферату (есе) під час ІКР	**5**
2.3. Інші види індивідуальних завдань, в т.ч. підготовка наукових публікацій, участь у роботі круглих столів, конференцій тощо.	-//-	Обговорення результатів проведеної роботи під час ІКР, наукових конференцій та круглих столів.	**5**
Разом балів за поточний контроль			**50**
Підсумковий контроль екзамен / залік			**50**
Всього балів підсумкової оцінки			**100**

Таблиця відповідності результатів контролю знань за різними шкалами

100-бальною шкалою	**Шкала за ECTS**	**За національною шкалою**	
		екзамен	**залік**
90-100 (10-12)	A	Відмінно	Зараховано
82-89 (8-9)	B	Добре	
74-81(6-7)	C		
64-73 (5)	D	Задовільно	
60-63 (4)	E		
35-59 (3)	Fx	Незадовільно	Не зараховано

10. КРИТЕРІЇ ПІДСУМКОВОЇ ОЦІНКИ ЗНАНЬ СТУДЕНТІВ
(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.

11. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса :ТЕС, 2020. 372 с.
2. Самойленко О. А. Виявлення та розслідування кіберзлочинів : навчально-методичний посібник. Одеса, 2020. 112 с.
3. Якименко І.З. Конспект лекцій з дисципліни «Цифрова криміналістика». URL: http://dspace.wunu.edu.ua/bitstream/316497/36005/1/%.pdf
4. Криміналістика/ Під ред. В.В. Тіщенко. Одеса: Видавничий дім «Гельветика», 2017. 556 с.
5. Криміналістика: підруч. , В.Ю. Шепітько, В.О. Коновалова, В.А. Журавель [та ін.]: за ред. В.Ю. Шепітька. 5-те вид. передобл. та допов. Київ: Ін Юре, 2016. 640 с.
6. Логінова Н.І., Дробожур Р.Р. Правовий захист інформації: навчальний посібник. Одеса: Фенікс, 2015. 264 с.
7. Бем М.В., Городиський І.М., Саттон Г., Родіоненко О.М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. Київ: К.І.С., 2015. 220 с.
8. Доступ до публічної інформації: практичний посібник для державних службовців. Київ: Національне агентство України з питань державної служби, 2012. 22 с.
9. Куліш А.М., Кобзєва Т.А., Шапіро В.С. Інформаційне право України: навчальний посібник. Суми: Сумський державний університет, 2016. 108 с.
10. Кукарін О.Б. Електронний документообіг та захист інформації: навч. посібник. Київ: НАДУ, 2015. 84 с.

Допоміжна

11. Бандурка О. М. Теорія і практика оперативно-розшукової діяльності : монографія. Харків : Злота миля, 2012. 620 с.
12. Степанюк Р.Л.. Перлін С.І. (2022). Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. Вісник ДДУВС імені Е.О.
13. Бірюков В.В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: моногр. Луганськ: РВВ ЛДУВС, 2009. 664 с.
14. Подобний О.О. Глава 24. Загальні засади й тактика негласних слідчих (розшукових) дій. Криміналістика: підручник / За ред. В. В. Тіщенка. Херсон: Видавничий дім «Гельветика», 2017. С. 325-346.
15. Подобний О. О. Актуальні аспекти вдосконалення оперативно-розшукового і кримінально-процесуального законодавства. Сучасні проблеми правового, економічного і соціального розвитку держави: матеріали міжнародної науково-практичної конференції (Харків, 10 квітня 2012 р.). Харків: ХНУВС, 2012. С. 271-274.
16. Подобний О. О., Пасечник М. Л. Слідча таємниця як засада кримінального провадження. Актуальні проблеми кримінальної юстиції: матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 26-27 червня 2019 р.).
17. Пасечник М. Л. Категорія «інформація» як основа визначення поняття «слідча таємниця». Юридичний бюлетень. 2018. № 7. С. 303-309.
18. Системна інформатизація правоохоронної діяльності / за ред. В. Дурдинця, М. Швеця. Київ: НДЦПІ АПрН України, 2007. 382 с.
19. Тіщенко В.В., Барцицька А.А. Теоретичні засади формування технологічного підходу в криміналістиці : монографія. НУ "ОЮА". Одеса : Фенікс, 2012. 199 с.
20. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса : Юридична література, 2011. 216 с.

Нормативно-правові акти:

21. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР / Верховна Рада України. Відомості Верховної Ради України. 1996. № 30. Ст. 141.

22. Кримінальний кодекс України : Закон України від 05. 04. 2001 р. № 2341-III / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 27.04.2021).

23. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 2213-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 27.04.2021)

24. Про інформацію : Закон України від 02. 10. 1992 р. № 2657-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua (дата звернення: 27.04.2021).

25. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI в редакції Закону України від 09.04.2015 № 319-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua

26. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16 листопада 1992 року № 2782-XII / Верховна Рада України. URL: http://zakon1.rada.gov.ua

27. Про Національну поліцію : закон України від 02. 07. 2015 р. № 580-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 27.04.2021).

28. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text (дата звернення: 27.04.2021).

29. Про державну таємницю : Закон України від 21. 01. 1994 р. № 3855-XII / Верховна Рада України. URL: https://zakon.rada.gov.ua (дата звернення: 27.04.2021).

30. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 року № 3475-IV. Відомості Верховної Ради України. 2006. № 30. Ст. 258.

31. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 року № 80/94-ВР / Верховна Рада України. URL: http://zakon1.rada.gov.ua (дата звернення: 20.06.2018).

32. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI в редакції Закону України від 19.10.2017№ 2168-VIII / Верховна Рада України. URL: http://zakon1.rada.gov.ua

33. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19

34. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27 вересня 1999 р. № 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99

35. Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Служби безпеки України від 12.08.2005 № 440. URL: https://zakon.rada.gov.ua/laws/show/z0902-05

36. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: Наказ Генеральної прокуратура України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: http://zakon4.rada.gov.ua/laws/show/v0114900-12.

37. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України від 8 жовтня 1997 р. № 1126. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF

38. Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших

матеріальних носіїв інформації, що містять службову інформацію: Постанова Кабінету Міністрів України від 19 жовтня 2016 р. № 736. URL: https://zakon.rada.gov.ua/laws/show/736-2016-%D0%BF

Інформаційні ресурси

39. Офіційний портал Верховної Ради України (законодавство). URL: https://www.rada.gov.ua/
40. Сайт Міністерства юстиції України. URL: https://minjust.gov.ua/
41. Урядовий портал Єдиний веб-портал органів виконавчої влади України. URL: https://www.kmu.gov.ua/
42. Сайт Міністерства внутрішніх справ України. URL: https://mvs.gov.ua/
43. Сайт Національної поліції. URL: https://www.npu.gov.ua/
44. Сайт Міністерства енергетики та захисту довкілля України. URL: http://www.menr.gov.ua
45. Офіційний сайт Державної служби України з питань праці. URL: http://www.dsp.gov.ua
46. Офіційний сайт Фонду соціального страхування України. URL: http://www.fssu.gov.ua
47. Національна бібліотека України імені В.І. Вернадського. URL: http://www.nbuv.gov.ua/
48. Сайт Державної служби з надзвичайних ситуацій. URL: http://dsns.gov.ua/ua/Nebezpeki-tehnogennogo-harakteru.html
49. Сайт Міжнародного гуманітарного університету. URL: https://mgu.edu.ua/