МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут права
Кафедра кримінального права та процесу

Затверджено
Науково-методичною радою Університету,
протокол від «27» 09 2024 р. № 2
Голова НМР _____ Іван ШЕМЕЛИНЕЦЬ

Робоча програма
навчальної дисципліни
«Організована транснаціональна кіберзлочинність»

для підготовки здобувачів вищої освіти другого (магістерського) рівня
денної та заочної форми навчання
галузь знань 26 «Цивільна безпека»
спеціальність 262 «Правоохоронна діяльність»
Освітньо-професійна програма «Правове забезпечення протидії кіберзлочинності»

Статус дисципліни: обов'язкова

Ірпінь – 2024

Робоча програма навчальної дисципліни «Організована транснаціональна кіберзлочинність» складена на основі освітньо-професійної програми «Правове забезпечення протидії кіберзлочинності» другого (магістерського) рівня спеціальності 262 «Правоохоронна діяльність», затвердженої Вченою радою Університету «12»07 2024 року, протокол № 19.

Укладачі: Н. Сперкач, к.ю.н.

В. Любавіна, к.ю.н.

Гарант ОПП «Правове забезпечення протидії кіберзлочинності» Г. Дідківська

Робочу програму навчальної дисципліни розглянуто та схвалено кафедрою кримінального права та процесу, протокол від «27» серпня 2024 р. № 1

Завідувач кафедри Г. Дідківська, д.ю.н., професор

Розглянуто і схвалено Вченою радою Навчально-наукового інституту права, від «27» серпня 2024 р. № 1.

Голова вченої ради ННІ права В. Топчій

Завідувач навчально-методичного відділу І. Качур, к.біол.н., доцент

Реєстраційний №_____

ЗМІСТ

1. ПЕРЕДМОВА.

Метою навчальної дисципліни «Організована транснаціональна кіберзлочинність» полягає в отриманні знань щодо напрямів, способів та засобів організаційної та транснаціональної злочинності, оскільки ефективне запобігання злочинності в Україні неможливе без проведення заходів щодо забезпечення безпеки нашої держави від транснаціональної злочинності. Застосування новітніх інформаційних технологій при проведенні заходів із забезпечення внутрішньої та зовнішньої безпеки держави є вагомими напрями правоохоронної сфери. Також мета дисципліни проявляється у вивченні та вирішенні теоретико-прикладних проблем й питань щодо: захисту державної таємниці; забезпечення безпеки суб'єктів підприємницької діяльності; інформаційної сфери і права на інформацію; інноваційної діяльності та її правових аспектів; інтелектуальної власності та права на її об'єкти.

Завданнями навчальної дисципліни «Організована транснаціональна кіберзлочинність» є формування у здобувачів вищої освіти поглиблені знання та уявлення про сучасний стан злочинності; вивчення здобувачами вищої освіти загальні характеристики та запобігання транснаціонального злочину. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки та його розвиток, предмет, методологія та місце актуальних питань в системі наукових знань та її зв'язок з іншими науками; отримання поглиблених знань про поняття та ознаки транснаціональної кіберзлочинності в Україні, про фактори, які впливають на процеси запобігання і протидії в Україні та її соціальні наслідки; оволодіння знаннями про основні характеристики кіберзлочинності: кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем форми та види кібербезпеки; характеристика кіберзлочинності; отримання поглиблених знань про кіберзлочини; відпрацювання навичок та умінь аналізу; здатність застосовувати професійні знання й практичні навички для розв'язання складних спеціалізованих задач та проблем у галузі забезпечення національної безпеки.

Методи навчання:

1. за джерелом інформації і сприйняття навчальної інформації: словесні (лекція, семінарське заняття, бесіда, розповідь); наочні (презентація, слайди); практичні (збір інформації та її систематизація);

2. за логікою передачі і сприйняття навчального матеріалу: індуктивні, дедуктивні, аналітичні, синтетичні;

3. за ступенем самостійного мислення при засвоєнні знань: репродуктивні та продуктивні (частково-пошукові);

4. за ступенем управління навчальним процесом: самостійна робота здобувача вищої освіти з навчальною та науковою літературою, текстами лекцій, підготовка до семінарських занять, виконання письмових завдань, індивідуальна дослідницька робота.

Форми організації занять*:* лекційні заняття, семінарські заняття, самостійна робота та індивідуально-консультаційна робота.

Організація поточного контролю та підсумкового контролю знань: поточний контроль знань здобувачів вищої освіти здійснюється під час проведення навчальних занять і стосується перевірки засвоєння ними матеріалу, що отримано на лекційних заняттях, самостійної роботи та індивідуальної-консультаційної роботи. Поточний контроль може проводитись у формі усного опитування здобувачів вищої освіти за темою, яка виноситься до обговорення, виконанні письмових теоретичних та практичних завдань або комп'ютерного тестування на семінарських заняттях та лекціях, виступів здобувачів вищої освіти при обговоренні питань на семінарських заняттях, модульного контролю. Підсумковий контроль проводиться у формі екзамену.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Код академічної групи ПМПД

Показники	Характеристика навчальної дисципліни	
	Денна форма навчання	Заочна форма навчання
Кількість кредитів ЄКТС - 5		
Модулів – 3	Рік підготовки:	
Змістових модулів – 3	1-й	1-й
Загальна кількість годин - 150 годин	Семестр	
	2-й	2-й
	Лекції	
	26 год.	6 год.
	Семінарські заняття	
	24 год.	4 год.
	Самостійна робота	
	97 год.	138 год.
	Індивід.-консультац. робота	
	3 год.	2 год.
	Форма семестрового контролю: екзамен	

2.1. КОМПЕТЕНТНОСТІ І РЕЗУЛЬТАТИ НАВЧАННЯ

ОП «Правове забезпечення протидії кіберзлочинності»

Компетентності	Результати навчання
ІК. Здатність розв'язувати складні задачі і проблеми у сфері правоохоронної діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог. ФК2. Здатність збирати та оцінювати докази, використовувати криміналістичні методи та засоби в професійній діяльності, прогнозувати поведінку правопорушників та вживати превентивні заходи. ФК3. Здатність розробляти планові, керівні та процесуальні (процедурні) документи, вміти реалізовувати плани (проекти) в межах своєї професійної діяльності, систематизувати та обробляти інформацію, вживати заходів щодо усунення виявлених недоліків	ПРН5. Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення. ПРН22. Здійснювати заходи з виявлення, припинення та розслідування кіберзлочинів, проводити дії та заходи спрямовані на збір доказів та фіксацію фактичних даних про протиправну діяльність.

2.2. ПРЕРЕКВІЗИТИ ТА ПОСТРЕКВІЗИТИ

ОП «Правове забезпечення протидії кіберзлочинності»

Пререквізитами є навчальні дисципліни: «Управління правоохоронною діяльністю», «Актуальні проблеми кримінального права», «Актуальні питання кримінально-правової та кримінологічної характеристики кіберзлочинності в Україні»

Постреквізитами є навчальні дисципліни: «Кримінальні процесуальні та криміналістичні проблеми розслідування кіберзлочинів», «Міжнародні стандарти правоохоронної діяльності».

2.3.СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ОРГАНІЗОВАНА ТРАНСНАЦІОНАЛЬНА ЗЛОЧИННІСТЬ

Денна форма навчання

Код академічної групи ПМПД

№ п/п	Змістові модулі	Кількість годин				
		Лекції(год.)	Семінари (год.)	Інд.-конс. робота під кер. викладача (год)	СРС (год.)	Всього (год.)
МОДУЛЬ І = 2 кредити (60 годин)						
ЗМ 1 (Теми 1-4)						
Т.1	Загальна характеристика та запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки	4	2	-	8	14
Т.2	Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «злочини міжнародного характеру»	4	4	-	8	16
Т.3	Вчення про кібертероризм	4	4	-	8	16
Т.4	Державне управління у сфері запобігання і протидії організованій транснаціональній кіберзлочинності в Україні	2	2	2	8	14
Всього по модулю 1:		**14**	**12**	**2**	**32**	**60**
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
МОДУЛЬ ІІ = 1 кредит (30 годин)						
ЗМ 2 (Теми 5-7)						
Т.5	Методика розслідування транснаціональних кіберзлочинів	2	2	-	5	9
Т.6	Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні	2	2	-	5	9
Т.7	Форми та види кібербезпеки держави та напрями її забезпечення. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності	2	2	1	7	12
Всього по модулю 2:		6	**6**	**1**	**17**	**30**
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
МОДУЛЬ ІІІ = 2 кредити (60 годин)						
ЗМ 3 (Теми 8-10)						
Т.8	Характеристика Конвенції Організації Об'єднаних Націй проти транснаціональної організованої кіберзлочинності	2	2	-	16	20
Т.9	Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем	2	2	-	16	20

Т.10	Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів	2	2	-	16	20
Всього по модулю 3:		6	**6**	**0**	**48**	**60**
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
Форма підсумкового контролю: ***екзамен***						
Усього за навчальною дисципліною:		**26**	**24**	**3**	**87**	**150**

Заочна форма навчання

Код академічної групи ПМПДЗ

№ п/п	**Змістові модулі**	**Кількість годин**				
		Лекції(год.)	**Семінари (год.)**	**Інд.-конс. робота під кер. викладача (год)**	**СРС (год.)**	**Всього (год.)**
МОДУЛЬ І = 2 кредити (60 годин)						
ЗМ1						
Т.1	Загальна характеристика та запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки	1	1	-	14	16
Т.2	Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «злочини міжнародного характеру»	1	1	-	14	16
Т.3	Вчення про кібертероризм	-	-	-	14	14
Т.4	Державне управління у сфері запобігання і протидії організованій транснаціональній кіберзлочинності в Україні	-	-		14	14
Всього по модулю 1:		**2**	**2**	**0**	**56**	**60**
МОДУЛЬ ІІ = 1 кредит (30 годин)						
ЗМ 2						
Т.5	Методика розслідування транснаціональних кіберзлочинів	1	1	-	9	11
Т.6	Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні	1	1	-	8	10
Т.7	Форми та види кібербезпеки держави та напрями її забезпечення. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності	-	-	1	8	9
Всього по модулю 2:		**2**	**2**	**1**	**25**	**30**
МОДУЛЬ ІІІ = 2 кредити (60 годин)						
ЗМ 3						
Т.8	Характеристика Конвенції Організації Об'єднаних Націй проти транснаціональної організованої	1	-	-	19	20

	кіберзлочинності					
Т.9	Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем	1	-	-	19	20
Т.10.	Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів	-	-	1	19	20
Всього по модулю:		**2**	0	**1**	**57**	**60**
Форма контролю: аудиторна контрольна робота						
Форма підсумкового контролю: ***екзамен***						
Усього за навчальною дисципліною:		**6**	**4**	**2**	**138**	**150**

РЕЙТИНГ-ПЛАН
Денна форма навчання

Години	**Тема**	**Форма заняття**	**Результати навчання**	**Вага оцінки**
Модуль 1				
4	Загальна характеристика та запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки	Лекція	ПРН5, ПРН22	0
2	Загальна характеристика та запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки	Семінарське заняття	ПРН5, ПРН22	2
4	Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «кіберзлочини міжнародного характеру»	Лекція	ПРН5, ПРН22	0
4	Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «кіберзлочини міжнародного характеру»	Семінарське заняття	ПРН5, ПРН22	2
4	Вчення про «кібертероризм»	Лекція	ПРН5, ПРН22	0
4	Вчення про «кібертероризм»	Семінарське	ПРН5, ПРН22	2

		заняття		
2	Державне управління у сфері запобігання і протидії організованій транснаціональній кіберзлочинності в Україні	Лекція	ПРН5, ПРН22	0
2	Державне управління у сфері запобігання і протидії організованій транснаціональній кіберзлочинності в Україні	Семінарське заняття	ПРН5, ПРН22	2
	Т 1-4	Проміжний модульний контроль		5
	Усього за Модулем І			**13**
2	Методика розслідування транснаціональних кіберзлочинів	Лекція	ПРН5, ПРН22	0
2	Методика розслідування транснаціональних кіберзлочинів	Семінарське заняття	ПРН5, ПРН22	2
2	Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні	Лекція	ПРН5, ПРН22	0
2	Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні	Семінарське заняття	ПРН5, ПРН22	2
2	Форми та види кібербезпеки держави та напрями її забезпечення. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності.	Лекція	ПРН5, ПРН22	0
2	Форми та види кібербезпеки держави та напрями її забезпечення. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності.	Семінар	ПРН5, ПРН22	2
	Теми 5-7	Модульний контроль		5
	Усього за Модулем 2			**11**
2	Характеристика Конвенції Організації Об'єднаних Націй проти транснаціональної	Лекція	ПРН5, ПРН22	0

	організованої кіберзлочинності			
2	Характеристика Конвенції Організації Об'єднаних Націй проти транснаціональної організованої кіберзлочинності	Семінарське заняття	ПРН5, ПРН22	2
2	Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем	Лекція	ПРН5, ПРН22	0
2	Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем	Семінарське заняття	ПРН5, ПРН22	2
2	Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів	Лекція	ПРН5, ПРН22	0
2	Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів	Семінарське заняття	ПРН5, ПРН22	2
	Тема 8-10	Модульний контроль		5
1	Індивідуальна робота	Тема 4,7		10
	Комп’ютерне тестування на платформі дистанційного навчання			5
	Усього за Модулем 3			**26**
	Екзамен			**50**
	Усього за курсом			**100**

Заочна форма навчання
Код академічної групи ПМСПЗ, ПМКПЗ

Години	**Тема**	**Форма заняття**	**Результати навчання**	**Вага оцінки**
1	Загальна характеристика та запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки	Лекція	ПРН5, ПРН22	0
1	Загальна характеристика та	Семінарське	ПРН5, ПРН22	5

	запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки	заняття		
1	Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «злочини міжнародного характеру»	Лекція	ПРН5, ПРН22	0
1	Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «злочини міжнародного характеру»	Семінарське заняття	ПРН5, ПРН22	5
1	Методика розслідування транснаціональних кіберзлочинів	Лекція	ПРН5, ПРН22	0
1	Методика розслідування транснаціональних кіберзлочинів	Семінарське заняття	ПРН5, ПРН22	5
1	Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні	Лекція	ПРН5, ПРН22	0
1	Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні	Семінарське заняття	ПРН5, ПРН22	5
2	Характеристика Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності	Лекція	ПРН5, ПРН22	0
2	Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності,	Лекція	ПРН5, ПРН22	0

	цілісності та доступності інформації, даних і систем			
	Модульна контрольна робота	Аудиторна контрольна робота		15
2	Індивідуальна робота	Тема 4,7		10
	Комп'ютерне тестування на платформі дистанційного навчання			5
	Усього за Модулем І, ІІ,ІІІ			**50**
	Екзамен			**50**
	Усього за курсом			**100**

2.4. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

У процесі навчання здобувачі денної та заочної форми навчання ДПУ використовують різні форми для опрацювання навчального матеріалу. Щоб забезпечити високу якість навчального процесу мають бути доступні інструменти:

1. Доступ до мережі інтернет для виконання тестових завдань на платформі Moodle ДПУ.
2. Наявність текстових та графічних редакторів для виконання наукових досліджень та презентації їх на семінарських, зокрема: в середовищі Windows (Write, NotePab/Блокнот, WordPab, Microsoft Word, Microsoft Excel, Microsoft Power Point); графічні редактори: піксельної графіки (Adobe Photoshop CS, Microsoft Paint) та інші.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ЗА ЗМІСТОВИМИ МОДУЛЯМИ

Модуль І.

Змістовий модуль І.

Тема 1. Загальна характеристика та запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.

План лекційного заняття

1. Поняття та загальна кримінологічна характеристика кіберзлочинності. Причини та умови кіберзлочинності.
2. Види кіберправопорушень та напрями забезпечення кібербезпеки України.
3. Загальна характеристика запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.

План семінарського заняття

1. Кіберзлочинність як соціально-правове явище сучасного світу, її поняття та ознаки.
2. Детермінанти кіберзлочинності.
3. Видова характеристика кіберзлочинності та її структура.
4. Місце кіберзлочинності у структурі системі злочинності, її показники.
5. Поняття та загальна кримінологічна характеристика кіберзлочинності. Причини та умови кіберзлочинності.
6. Види кіберправопорушень та напрями забезпечення кібербезпеки України.
7. Загальна характеристика запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.

Самостійна робота здобувачів вищої освіти

1. Складіть хронологічну таблицю розвитку кіберзлочинності.
2. Користуючись статистичними даними Офісу Генерального прокурора про стан злочинності в Україні складіть діаграму яка відображає структуру кіберзлочинності в Україні.
3. Користуючись статистичними даними Офісу Генерального прокурора про стан злочинності в Україні складіть схему, яка відображатиме динаміку кіберзлочинності в України за період від 2015 року.

Питання для самоконтролю

1. Вчення про кіберзлочинність: поняття, ознаки, види, структура та показники.
2. Проаналізуйте рівень, динаміку та характер сучасного стану кіберзлочинності в Україні.

3. Охарактеризуйте правову основу забезпечення кібербезпеки України.
4. Визначте та проаналізуйте детермінанти, які впливають на стан вчинення кіберправопорушень.
5. Визначте окремі види класифікацій кіберправопорушень за національним та міжнародним законодавством.
6. Проаналізуйте, які кіберзлочини належать до правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем та правопорушення, пов'язані з комп'ютерами.
7. Визначте види кіберзлочинів, які можна віднести до правопорушень, пов'язаних зі змістом (контентом) та умисні дії, пов'язаних з порушенням авторських та суміжних прав та кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.
8. Наведіть кримінологічну характеристику осіб, що вчиняють кіберзлочини: проаналізуйте їх соціально-демографічну та кримінально-правову характеристики.
9. Охарактеризуйте віктимологічну характеристику осіб, які стають або можуть стати жертвами кіберзлочинів.
10. Визначте основні, сучасні та дієві напрями забезпечення кібербезпеки України.
11. Проаналізуйте, які види запобігання кіберзлочинності є найбільш типовими для даного виду злочинності.
12. Вкажіть кримінологічні засади забезпечення кібербезпеки суспільстві та суб'єктів їх виконання.

Рекомендована література

Основна:[7,8,9,10]
Допоміжна: [2, 3, 4, 5, 6, 7, 8]
Інформаційні ресурси Інтернет:[2,6,8,9,12]
Міжнародні видання:[2,7,9,11,13]

Тема 2. Загальна характеристика транснаціональної організованої кіберзлочинності. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «кіберзлочини міжнародного характеру».

План лекційного заняття

1. Транснаціональна організована кіберзлочинність: загроза глобальним суспільним благам.
2. Конвенція ООН проти транснаціональної організованої кіберзлочинності та додаткові протоколи до неї.
3. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «кіберзлочини міжнародного характеру».

План семінарського заняття

1. Транснаціональна організована кіберзлочинність: загроза глобальним суспільним благам.
2. Конвенція ООН проти транснаціональної організованої кіберзлочинності та додаткові протоколи до неї.
3. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «кіберзлочини міжнародного характеру».

Самостійна робота здобувачів вищої освіти

1. Міжнародний кримінальний суд.
2. Міжнародний суд ООН.
3. Визначте, чи є в діях М. склад кіберзлочину відповідно до Конвенції Ради Європи про кіберзлочинність та Кримінального кодексу України. Якщо так, то який? Громадянин України М. з метою несанкціонованого доступу до комп'ютера своєї дружини придбав комп'ютерну програму, яка створена для запису послідовності натискань на клавіатурі комп'ютера. За допомогою цієї програми М. планував отримати пароль до електронної скриньки дружини.

Питання для самоконтролю

1. Що є транснаціональною організованою кіберзлочинністю: загроза глобальним суспільним благам?
2. Що свідчить Конвенція ООН проти транснаціональної організованої кіберзлочинності та додаткові протоколи до неї?
3. Яке співвідношення понять «транснаціональна кіберзлочинність», «міжнародна

кіберзлочинність», «кіберзлочини міжнародного характеру»?

Рекомендована література

Основні: [7,8,9,10]
Допоміжна:[16,18,24,32,44]
Інформаційні ресурси Інтернет:[2,4,8,11,12]
Міжнародні видання:[3, 5, 6]

Тема 3. Вчення про кібертероризм.

План лекційного заняття

1. Феномен «кібертероризму» та історія його виникнення.
2. Кібертероризм: поняття та ознаки, види.
3. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
4. Кібертерористичний акт: поняття та види.
5. Запобігання кібертероризму.

План семінарського заняття

1. Феномен «кібертероризму» та історія його виникнення.
2. Кібертероризм: поняття та ознаки, види.
3. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
4. Кібертерористичний акт: поняття та види. 5. Запобігання кібертероризму.

Самостійна робота здобувачів вищої освіти

1. Охарактеризуйте поняття терористичних актів вчинених з використанням цифрових технологій. Проаналізуйте їх з позицій кримінології.
2. Підготуйте реферативне повідомлення на тему «Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система. Запобігання організованій транснаціональній кіберзлочинності».

Питання для самоконтролю

1. Який Феномен «кібертероризму» та історія його виникнення?
2. Яке поняття та ознаки, види кібертероризма?
3. Яке співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне)?
4. Які принципи запобігання кібертероризму існують?

Рекомендована література

Основна: [7,8,9,10]
Допоміжна: [10, 31, 32, 39]
Інформаційні ресурси Інтернет:[1,3,6,9,10]
Міжнародні видання:[2, 4]

Тема 4. Державне управління у сфері запобігання і протидії організованій транснаціональній кіберзлочинності в Україні.

План лекційного заняття

1. Особливості організаційних та нормативно-правових засад боротьби з організованою транснаціональною кіберзлочинністю.
2. Проблеми державного управління у сфері запобігання проявам організованої транснаціональної кіберзлочинності.
3. Напрями вирішення проблеми проявів організованої транснаціональної кіберзлочинності.

План семінарського заняття

1. Особливості організаційних та нормативно-правових засад боротьби з організованою транснаціональною кіберзлочинністю.
2. Проблеми державного управління у сфері запобігання проявам організованої транснаціональної кіберзлочинності.
3. Напрями вирішення проблеми проявів організованої транснаціональної кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану
2. Підходи і моделі реформування державних механізмів боротьби з кіберзлочинністю.
3. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-

функціональній структурі суб'єктів протидії кіберзлочинності.
4. Система запобігання кіберзлочинності в Україні.

Питання для самоконтролю

1.Які особливості організаційних та нормативно-правових засад боротьби з організованою транснаціональною кіберзлочинністю існують?
2.Які проблеми державного управління у сфері запобігання проявам організованої транснаціональної кіберзлочинності?
3.Які напрями вирішення проблеми проявів організованої транснаціональної кіберзлочинності, ви можете назвати?

Індивідуально-консультаційна робота здобувачів вищої освіти

1. Підготуйте реферативне повідомлення на тему «Цифрові технології при запобіганні організованим транснаціональним кіберправопорушенням».
2. Користуючись статистичними даними Інтерполу складіть схему щодо інформації про заходи із запобігання організованій транснаціональній кіберзлочинності на міжнародному рівні.

Рекомендована література

Основна: [7,8,9,10]
Допоміжна:[17, 18, 38]
Інформаційні ресурси Інтернет:[1,3,6,9,11]
Міжнародні видання:[8,10,13]

Модуль ІІ.
Змістовий модуль 2.
Тема 5. Методика розслідування транснаціональних кіберзлочинів.

План лекційного заняття

1. Загальні теоретичні основи методики розслідування транснаціональних кіберзлочинів: криміналістичний аналіз.
2. Теоретичні засади методики розслідування транснаціональних кіберзлочинів.
3. Основи криміналістичної характеристики міжнародної організованої транснаціональної кіберзлочинності.
4. Криміналістичний аналіз сучасної транснаціональної організованої кіберзлочинності.
5. Фактори, властивості, риси, тенденції розвитку сучасної транснаціональної організованої кіберзлочинності.
6. Загальна характеристика організованих злочинних груп в країнах Європейського Союзу.
7. Типові напрями кримінальної діяльності організованих злочинних груп в країнах Європейського Союзу.

План семінарського заняття

1. Загальні теоретичні основи методики розслідування транснаціональних кіберзлочинів: криміналістичний аналіз.
2. Теоретичні засади методики розслідування транснаціональних кіберзлочинів.
3. Основи криміналістичної характеристики міжнародної організованої транснаціональної кіберзлочинності.
4. Криміналістичний аналіз сучасної транснаціональної організованої кіберзлочинності.
5. Фактори, властивості, риси, тенденції розвитку сучасної транснаціональної організованої кіберзлочинності.
6. Загальна характеристика організованих злочинних груп в країнах Європейського Союзу.
7. Типові напрями кримінальної діяльності організованих злочинних груп в країнах Європейського Союзу.

Питання самостійної роботи здобувачів вищої освіти

1. Методичні основи розслідування транснаціональних кіберзлочинів.
2. Організаційні засади виявлення та початку кримінального провадження щодо транснаціональних кіберзлочинів.
3. Організаційно-тактичні основи розслідування транснаціональних кіберзлочинів.
4. Використання спеціальних знань під час розслідування транснаціональних кіберзлочинів.

Питання для самоконтролю

1. Які загальні теоретичні основи методики розслідування транснаціональних кіберзлочинів:

криміналістичний аналіз?
2. Який криміналістичний аналіз сучасної транснаціональної організованої кіберзлочинності?
3. Яка загальна характеристика організованих злочинних груп в країнах Європейського Союзу?
4. Які типові напрями кримінальної діяльності організованих злочинних груп в країнах Європейського Союзу?
5. Які фактори, властивості, риси, тенденції розвитку сучасної транснаціональної організованої кіберзлочинності?

Рекомендована література

Основна: [7,8,9,10].
Допоміжна:[15,18,23,35].
Інформаційні ресурси Інтернет:[10,11,12].
Міжнародні видання:[2, 6,8,10,12].

Тема 6. Прикладні проблеми реалізації політики у сфері протидії транснаціональній організованій кіберзлочинності в Україні.

План лекційного заняття

1. Організаційно-правові основи боротьби з організованою транснаціональною кіберзлочинністю.
2. Законодавство про боротьбу з організованою транснаціональною кіберзлочинністю.
3. Система органів, які здійснюють боротьбу з організованою кіберзлочинністю.
4. Система та повноваження органів, які здійснюють боротьбу з організованою транснаціональною кіберзлочинністю.
5. Основні напрями боротьби з організованою транснаціональною кіберзлочинністю.

План семінарського заняття

1. Організаційно-правові основи боротьби з організованою транснаціональною кіберзлочинністю.
2. Законодавство про боротьбу з організованою транснаціональною кіберзлочинністю.
3. Система органів, які здійснюють боротьбу з організованою кіберзлочинністю.
4. Система та повноваження органів, які здійснюють боротьбу з організованою транснаціональною кіберзлочинністю.
5. Основні напрями боротьби з організованою транснаціональною кіберзлочинністю.

Самостійна робота здобувачів вищої освіти

1. Наведіть приклад кримінального правопорушення транснаціонального характеру та зазначте його кваліфікацію, яке б стосувалося посягання на конфіденційність та цілісність або доступність комп'ютерної інформації, що має наслідком витік інформації за межами однієї держави. Повністю проаналізуйте наведений склад кримінального правопорушення.
2. Наведіть приклад кримінального правопорушення транснаціонального характеру та зазначте його кваліфікацію, яке б стосувалося створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів за межами однієї держави, а також їх розповсюдження або збут. Повністю проаналізуйте наведений склад кримінального правопорушення.

Питання для самоконтролю

1. Яка система та повноваження органів, які здійснюють боротьбу з організованою транснаціональною кіберзлочинністю?
2. Яка система органів, які здійснюють боротьбу з організованою кібезлочинністю?
3. Які організаційно-правові основи боротьби з організованою транснаціональною кіберзлочинністю?
4. Які Основні напрями боротьби з організованою транснаціональною кіберзлочинністю?

Рекомендована література

Основна: [7,8,9,10]
Допоміжна:[26, 34, 27]
Інформаційні ресурси Інтернет:[2,4,8,10,11]
Міжнародні видання:[2,6,8,10]

Тема 7. Форми та види кібербезпеки держави та напрями її забезпечення. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності.

План лекційного заняття

1. Сучасна кібербезпека України: поняття, зміст, ознаки.
2. Нормативно-правова основа кібербезпеки в Україні.
3. Напрями кібербезпеки України. Суб'єкти забезпечення кібербезпеки в Україні: види, повноваження.
4. Співробітництво України з міжнародними партнерами у сфері забезпечення кібербезпеки. Кібербезпека України в умовах дії правового режиму воєнного часу.
5. Стан правового забезпечення захисту інформації в Україні. Кібербезпека: поняття, форми, види, напрями забезпечення.
6. Способи вчинення кримінальних правопорушень у сфері комп'ютерної інформації.
7. Захист особи, індивідуальної, колективної і державної власності від злочинних комп'ютерних посягань.
8. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності та інформаційна безпека комп'ютерних систем.

План семінарського заняття

1. Сучасна кібербезпека України: поняття, зміст, ознаки.
2. Нормативно-правова основа кібербезпеки в Україні.
3. Напрями кібербезпеки України. Суб'єкти забезпечення кібербезпеки в Україні: види, повноваження.
4. Співробітництво України з міжнародними партнерами у сфері забезпечення кібербезпеки. Кібербезпека України в умовах дії правового режиму воєнного часу.
5. Стан правового забезпечення захисту інформації в Україні. Кібербезпека: поняття, форми, види, напрями забезпечення.
6. Способи вчинення кримінальних правопорушень у сфері комп'ютерної інформації.
7. Захист особи, індивідуальної, колективної і державної власності від злочинних комп'ютерних посягань.
8. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності та інформаційна безпека комп'ютерних систем.

Самостійна робота здобувачів вищої освіти

1. Підготувати презентацію (не менше 15 слайдів) за наступними темами (теми обираємо за списком у журналі):

1.1. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система. Запобігання організованій транснаціональній кіберзлочинності.

1.2. Сучасний стан кримінально - правового забезпечення боротьби з кіберзлочинністю. Детермінанти та основні напрямки запобігання організованій транснаціональній кіберзлочинності.

1.3. Поняття організованої транснаціональної кіберзлочинності та її місце в загальній структурі злочинності. Сучасний стан та напрями запобігання.

1.4. Стан сучасної кібербезпеки в Україні та у зарубіжних країнах. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі.

2. Схематично зобразіть перелік нормативно-правових документів, що регулюють сферу кібербезпеки України.
3. Проаналізуйте основні ідеї положення Конвенції про кіберзлочинність.
4. Підготуйте реферативний повідомлення на тему «Державна політика у сфері забезпечення кібербезпеки».

Питання для самоконтролю

1. Які напрями кібербезпеки України?
2. Які суб'єкти забезпечення кібербезпеки в Україні: види, повноваження?
3. Яка нормативно-правова основа кібербезпеки в Україні?
4. Який захист особи, індивідуальної, колективної і державної власності від злочинних комп'ютерних посягань?

Індивідуально-консультаційна робота здобувачів вищої освіти

1. Схематично зобразіть перелік основних нормативно-правових документів, що регулюють сферу кібербезпеки України та проаналізуйте основні ідеї і положення Конвенції про кіберзлочинність.

Рекомендована література

Основна: [7,8,9,10]

Допоміжна:[20, 24, 25, 33, 40, 41]
Інформаційні ресурси Інтернет: [10,11]
Міжнародні видання:[11,12]

Модуль ІІІ.

Змістовий модуль 3.

Тема 8. Характеристика Конвенції Організації Об'єднаних Націй проти транснаціональної організованої кіберзлочинності.

План лекційного заняття

1. Історичні аспекти прийняття Конвенції ООН проти транснаціональної організованої кіберзлочинності.
2. Статус Конвенції ООН проти транснаціональної організованої кіберзлочинності.
3. Мета та основна термінологія Конвенції ООН проти транснаціональної організованої кіберзлочинності.
4. Сфера застосування Конвенції ООН проти транснаціональної організованої кіберзлочинності.
5. Захист суверенітету та криміналізація участі в організованій злочинній групі в Конвенції ООН проти транснаціональної організованої кіберзлочинності.
6. Взаємна правова допомога держав у боротьбі проти транснаціональної організованої кіберзлочинності.

План семінарського заняття

1. Історичні аспекти прийняття Конвенції ООН проти транснаціональної організованої кіберзлочинності.
2. Статус Конвенції ООН проти транснаціональної організованої кіберзлочинності.
3. Мета та основна термінологія Конвенції ООН проти транснаціональної організованої кіберзлочинності.
4. Сфера застосування Конвенції ООН проти транснаціональної організованої кіберзлочинності.
5. Захист суверенітету та криміналізація участі в організованій злочинній групі в Конвенції ООН проти транснаціональної організованої кіберзлочинності.
6. Взаємна правова допомога держав у боротьбі проти транснаціональної організованої кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Охарактеризувати історичні передумови ухвалення Конвенції.
2. Проаналізувати основні поняття та визначення, які використовуються в Конвенції.
3. Визначити головні цілі та завдання Конвенції.
4. Розглянути структуру Конвенції та її протоколів.
5. Оцінити ефективність механізмів міжнародного співробітництва, передбачених Конвенцією.
6. Виявити проблеми та виклики у реалізації Конвенції.
7. Сформулювати висновки та пропозиції щодо вдосконалення міжнародного співробітництва у боротьбі з організованою кіберзлочинністю.

Питання для самоконтролю

1.Які історичні аспекти прийняття Конвенції ООН проти транснаціональної організованої кіберзлочинності?
2. Яка мета та основна термінологія Конвенції ООН проти транснаціональної організованої кіберзлочинності?
3. Який захист суверенітету та криміналізація участі в організованій злочинній групі в Конвенції ООН проти транснаціональної організованої кіберзлочинності?
4. Яка взаємна правова допомога держав у боротьбі проти транснаціональної організованої кіберзлочинності?

Рекомендована література

Основна: [7,8,9,10]
Допоміжна:[27, 28, 22, 13, 19, 45]
Інформаційні ресурси Інтернет: [10,11,12]
Міжнародні видання:[1,3,8]

Тема 9. Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем.

План лекційного заняття

1. Загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.
2. Види кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.
3. Причини та умови кримінальних правопорушень проти конфіденційності цілісності та доступності інформації, даних і систем.

План семінарського заняття

4. Загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.
5. Види кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.
6. Причини та умови кримінальних правопорушень проти конфіденційності цілісності та доступності інформації, даних і систем.

Самостійна робота здобувачів вищої освіти

1. Підготувати презентацію (не менше 15 слайдів) за наступними темами (теми обираємо за списком у журналі):

1.1. Характеристика кіберзлочинів пов’язаних з використанням комп’ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп’ютерне шахрайство та комп’ютерне підроблення тощо) .

1.2. Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

1.3. Правові засади співпраці держав-членів Європейського Союзу у сфері боротьби із кіберзлочинністю

1.4. Загальна характеристика кібербезпеки: сучасний стан та напрями вдосконалення. Запобігання організованій транснаціональній кіберзлочинності в Україні та окремих зарубіжних державах

2. Складіть задачу про кримінальне правопорушення яке посягає на конфіденційність тільки цілісність або доступність інформації. 2. Проаналізуйте положення Особливої частини Кримінального кодексу України та знайдіть приклади кримінальних правопорушень які посягають на конфіденційність цілісність та доступність інформації яких немає у розділі 16-му Розділі Особливої частини Кримінального кодексу України.

Питання для самоконтролю

1. Які причини та умови кримінальних правопорушень проти конфіденційності цілісності та доступності інформації, даних і систем?
2. Яка загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем?
3. Які види кримінальних правопорушень, посягають на конфіденційність, цілісність та доступність інформації, даних і систем?

Рекомендована література

Основна: [7,8,9,10]
Допоміжна: [1, 27,30,32,45]
Інформаційні ресурси Інтернет: [10,11,12]
Міжнародні видання:[4,5,6]

Тема 10. Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів.

План лекційного заняття

1. Загальна характеристика кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
2. Кримінально-правова характеристика та види кіберзлочинів пов’язаних з кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
3. Кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особливої частини Кримінального кодексу України.

План семінарського заняття

1. Загальна характеристика кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
2. Кримінально-правова характеристика та види кіберзлочинів пов’язаних з кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
3. Кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особливої частини Кримінального кодексу України.
4. Загальна характеристика кіберзлочинів пов’язаних з контентом.
5. Кримінально-правова характеристика та види кіберзлочинів пов’язаних з контентом

Самостійна робота здобувачів вищої освіти

Наведіть приклад кримінального правопорушення транснаціонального характеру та зазначте його кваліфікацію, яке б стосувалося несанкціонованого збуту або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, співучасником якого є громадянин іншої держави. Повністю проаналізуйте наведений склад кримінального правопорушення.

Питання для самоконтролю

1. Яка загальна характеристика кримінальних правопорушень з комп'ютерами?
2. Яка кримінально-правова характеристика та види кіберзлочинів пов’язаних з кримінальних правопорушень з комп'ютерами?
3. Яка кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особливої частини Кримінального кодексу України?

Рекомендована література

Основні: [7,8,9,10]
Допоміжна:[14, 21, 45]
Інформаційні ресурси Інтернет: [3,6,8,10]
Міжнародні видання:[4,8,10]

4. КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Розподіл балів за семінарське заняття

Критерії оцінювання	Кількість балів
В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань,використовуючи при цьому обов’язкову та додаткову літературу. Правильно вирішив усі тестові завдання.	2; 4-5
Володіє навчальним матеріалом в достатньому обсязі, аргументовано його викладає під час усних виступів та письмових відповідей, однак не достатньо глибоко розкриває зміст теоретичних питань. Правильно вирішив більшість тестові завдання	1,5; 2-3
Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань	0,5-1; 1
Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.	0; 0

Критерії оцінювання контрольних робіт.

Формою проміжного поточного контролю є контрольні роботи, які проводяться у письмовій формі та кожна з яких оцінюється від 0 до 5 балів для денної форми навчання.

Формою проміжного поточного контролю є контрольні роботи, які проводяться у письмовій формі та кожна з яких оцінюється від 0 до 15 балів для заочної форми навчання.

Розподіл балів за різні види завдань в межах контрольної роботи

Вид завдання	Максимальна кількість балів за виконання
Теоретичні питання (2 питання по 1,25)	2,5
Тестовий блок (закритої форми - 10 по 0,25)	2,5
Всього	5

Критерії оцінювання аудиторної контрольної роботи (заочна форма навчання)

Формою аудиторної контрольної роботи, яка проводиться у тестовій формі на платформі Moodle та оцінюється від 0 до 15 балів.

Розподіл балів за різні види завдань в межах контрольної роботи

Вид завдання	Максимальна кількість балів за виконання
Тестовий блок (закритої форми - 20 по 0,75)	15
Всього	15

Критерії оцінювання індивідуальної роботи

Індивідуальна робота здійснюється у формі дослідницького проекту – написання анотації/тез оцінюється від 0 до 10 балів для денної форми навчання.

Індивідуальна робота здійснюється у формі дослідницького проекту – написання анотації/тез оцінюється від 0 до 10 балів для заочної форми навчання.

Шкала оцінювання індивідуальної роботи здобувачів вищої освіти

Кількість балів		Критерії оцінювання
ДФН	**ЗФН**	
9-10	**9-10**	Оцінюється робота здобувача вищої освіти, який у повному обсязі розкрив сутність питання. При цьому використовував актуальну наукову термінологію, належним чином обґрунтовував свої думки та зробив узагальнені підсумки.
7-8	**7-8**	Оцінюється робота здобувача вищої освіти, який в основному розкрив зміст питання. Проте, при висвітленні деяких питань не вистачало достатньої аргументації, допускалися при цьому окремі неістотні неточності та незначні помилки
1-6	**1-6**	Оцінюється робота здобувача вищої освіти, який дав фрагментарну характеристику питання (без аргументації й обґрунтування, підсумків), у характеристиці питання присутні неточності та помилки або характеристика часткова.
0	**0**	Оцінюється робота здобувача вищої освіти, який дав неправильну характеристику питання, допустив істотні помилки, оперував неактуальною застарілою інформацією або не виконав і вчасно не здав завдання.

Підсумкове оцінювання знань здобувачів вищої освіти здійснюється зарезультатами поточного контролю (від 0 до 100 балів) та екзамену (від 0 до 50 балів).

Критерієм успішного проходження здобувачем освіти підсумкового оцінювання є отримання не менше 25 балів за поточний контроль та 25 балів за підсумковий контроль у формі екзамену.

Відповідність підсумкової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ЄКТС

Сума балів за 100-бальною шкалою	Оцінка в ЄКТС	Значення оцінки ЄКТС	Оцінка за національною шкалою	
			Екзамен/ Диференційований залік	Залік
90-100	A	відмінно	відмінно	зараховано
80-89	B	дуже добре	добре	
70-79	C	добре		
60-69	D	задовільно	задовільно	
50-59	E	достатньо		
35-49	FX	незадовільно з можливістю повторного складання	незадовільно	не зараховано
0-34	F	незадовільно з обов'язковим повторним вивченням курсу		

Результати складання екзамену оцінюються та вносяться у відомість обліку успішності здобувача вищої освіти, залікову книжку, індивідуальний навчальний план здобувача вищої освіти (крім «незадовільно» і «не зараховано»).

НЕФОРМАЛЬНА ОСВІТА

Шкала та критерії перезарахування результатів навчання, здобутих в неформальній освіті здобувача (до 25% обсягу контактних годин дисципліни)

Кількість балів	Форма заняття та діяльності	Критерії оцінювання	Рекомендовані ресурси для здобуття результату
10	Індивідуальна робота	Оцінюється робота за результатами надання сертифікату обсягом 30 годин (1 кредит ECTS) або більше	Масові онлайн курси https://www.dpu.edu.ua/osvita/neformalna-informalna-osvita
3	Семінарське заняття, практичне заняття	Оцінюється робота за результатами надання сертифікату за темою	Масові онлайн курси на платформі EdERA, Прометеус тощо. Онлайн курси мережевої академії Cisco (https://www.netacad.com/) тощо.
0		Відсутній результат або результат не відповідає тематиці дисципліни	

5. ЗАСОБИ ДІАГНОСТИКИ РЕЗУЛЬТАТІВ НАВЧАННЯ

Перелік засобів діагностики, які застосовуються при вивченні навчальної дисципліни:

- модульні контрольні роботи;
- комп'ютерне тестування на платформі MOODLE ДПУ;
- командні проєкти;
- презентаційні матеріали, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- студентські презентації та виступи на наукових заходах;
- усні відповіді під час опитування на семінарських заняттях на платформі Google Meet чи Zoom;

- робота у команді над опрацюванням певних наукових проектів;
- написання тез доповідей на науково-практичні конференції;
- інші види індивідуальних та групових завдань;
- екзамен.

6. ФОРМИ ТА ПИТАННЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Контрольні заходи, для визначення поточних знань за перший, другий і третій модулі, проводиться у письмовому вигляді (або шляхом тестування на платформі MOODLE ДПУ) та може включати такі види завдань:

- теоретичні питання;
- тестові завдання;
- завдання понятійного апарату.

Контрольний захід, для визначення підсумкових знань з навчальної дисципліни, проводиться у формі екзамену, який складається з теоретичної (письмової) та тестової частин. Теоретична частина полягає у виконанні письмової екзаменаційної роботи з курсу, а тестова у розв'язанні тестових завдань (дистанційна форма навчання MOODLE ДПУ).

ПЕРЕЛІК ПИТАНЬ ПОТОЧНОГО КОНТРОЛЮ

МОДУЛЬ 1

1. Поняття та загальна кримінологічна характеристика кіберзлочинності. Причини та умови кіберзлочинності.
2. Види кіберправопорушень та напрями забезпечення кібербезпеки України
3. Загальна характеристика запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки
4. Транснаціональна організована злочинність: загроза глобальним суспільним благам.
5. Конвенція ООН проти транснаціональної організованої злочинності та додаткові протоколи до неї.
6. Співвідношення понять «транснаціональна кіберзлочинність», «міжнародна кіберзлочинність», «кіберзлочини міжнародного характеру»
7. Феномен «кібертероризму» та історія його виникнення.
8. Кібертероризм: поняття та ознаки, види.
9. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
10. Кібертерористичний акт: поняття та види. Запобігання кібертероризму.
11. Особливості організаційних та нормативно-правових засад боротьби з організованою транснаціональною кіберзлочинністю.
12. Проблеми державного управління у сфері запобігання проявам організованої транснаціональної кіберзлочинності.
13. Напрями вирішення проблеми проявів організованої транснаціональної кіберзлочинності.

МОДУЛЬ 2

1. Загальні теоретичні основи методики розслідування транснаціональних кіберзлочинів: криміналістичний аналіз.
2. Теоретичні засади методики розслідування транснаціональних кіберзлочинів.
3. Основи криміналістичної характеристики міжнародної організованої транснаціональної кіберзлочинності.
4. Криміналістичний аналіз сучасної транснаціональної організованої кіберзлочинності.
5. Фактори, властивості, риси, тенденції розвитку сучасної транснаціональної організованої кіберзлочинності.
6. Загальна характеристика організованих злочинних груп в країнах Європейського Союзу.
7. Типові напрями кримінальної діяльності організованих злочинних груп в країнах Європейського Союзу.
8. Організаційно-правові основи боротьби з організованою транснаціональною кіберзлочинністю.
9. Законодавство про боротьбу з організованою транснаціональною кіберзлочинністю.
10. Система органів, які здійснюють боротьбу з організованою злочинністю.
11. Система та повноваження органів, які здійснюють боротьбу з організованою транснаціональною кіберзлочинністю.

12. Основні напрями боротьби з організованою транснаціональною кіберзлочинністю.
13. Сучасна кібербезпека України: поняття, зміст, ознаки.
14. Нормативно-правова основа кібербезпеки в Україні.
15. Напрями кібербезпеки України. Суб'єкти забезпечення кібербезпеки в Україні: види, повноваження.
16. Співробітництво України з міжнародними партнерами у сфері забезпечення кібербезпеки. Кібербезпека України в умовах дії правового режиму воєнного часу.
17. Стан правового забезпечення захисту інформації в Україні. Кібербезпека: поняття, форми, види, напрями забезпечення.
18. Способи вчинення кримінальних правопорушень у сфері комп'ютерної інформації.
19. Захист особи, індивідуальної, колективної і державної власності від злочинних комп'ютерних посягань.
20. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності та інформаційна безпека комп'ютерних систем.

МОДУЛЬ 3

1. Історичні аспекти прийняття Конвенції ООН проти транснаціональної організованої кіберзлочинності.
2. Статус Конвенції ООН проти транснаціональної організованої кіберзлочинності.
3. Мета та основна термінологія Конвенції ООН проти транснаціональної організованої кіберзлочинності.
4. Сфера застосування Конвенції ООН проти транснаціональної організованої кіберзлочинності.
5. Захист суверенітету та криміналізація участі в організованій злочинній групі в Конвенції ООН проти транснаціональної організованої кіберзлочинності.
6. Взаємна правова допомога держав у боротьбі проти транснаціональної організованої кіберзлочинності.
7. Загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.
8. Види кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.
9. Причини та умови кримінальних правопорушень проти конфіденційності цілісності та доступності інформації, даних і систем.
10. Загальна характеристика кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
11. Кримінально-правова характеристика та види кіберзлочинів пов'язаних з кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
12. Кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особливої частини Кримінального кодексу України.

ПЕРЕЛІК ПИТАНЬ ПІДСУМКОВОГО КОНТРОЛЮ

1. Кіберзлочинність як соціально-правове явище сучасного світу, її поняття та ознаки.
2. Детермінанти кіберзлочинності.
3. Видова характеристика кіберзлочинності та її структура.
4. Місце кіберзлочинності у структурі системі злочинності, її показники.
5. Поняття та загальна кримінологічна характеристика кіберзлочинності. Причини та умови кіберзлочинності.
6. Види кіберправопорушень та напрями забезпечення кібербезпеки України
7. Загальна характеристика запобігання кіберзлочинності. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки
8. Вчення про кіберзлочинність: поняття, ознаки, види, структура та показники
9. Проаналізуйте рівень, динаміку та характер сучасного стану кіберзлочинності в Україні.
10. Охарактеризуйте правову основу забезпечення кібербезпеки України.
11. Визначте та проаналізуйте детермінанти, які впливають на стан вчинення

кіберправопорушень.

12. Визначте окремі види класифікацій кіберправопорушень за національним та міжнародним законодавством.

13. Проаналізуйте, які кіберзлочини належать до правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем та правопорушення, пов’язані з комп’ютерами.

14. Визначте види кіберзлочинів, які можна віднести до правопорушень, пов’язаних зі змістом (контентом) та умисні дії, пов’язаних з порушенням авторських та суміжних прав та кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

15. Наведіть кримінологічну характеристику осіб, що вчиняють кіберзлочини: проаналізуйте їх соціально-демографічну та кримінально-правову характеристики.

16. Охарактеризуйте віктимологічну характеристику осіб, які стають або можуть стати жертвами кіберзлочинів

17. Визначте основні, сучасні та дієві напрями забезпечення кібербезпеки України

18. Проаналізуйте, які види запобігання кіберзлочинності є найбільш типовими для даного виду злочинності

19. Вкажіть кримінологічні засади забезпечення кібербезпеки суспільстві та суб’єктів їх виконання

20. Транснаціональна організована злочинність: загроза глобальним суспільним благам

21. Конвенція ООН проти транснаціональної організованої злочинності та додаткові протоколи до неї.

22. Співвідношення понять «транснаціональна злочинність», «міжнародна злочинність», «злочини міжнародного характеру»

23. Міжнародний кримінальний суд

24. Міжнародний суд ООН

25. Феномен «кібертероризму» та історія його виникнення.

26. Кібертероризм: поняття та ознаки, види.

27. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).

28. Кібертерористичний акт: поняття та види. 5. Запобігання кібертероризму.

29. Особливості організаційних та нормативно-правових засад боротьби з організованою транснаціональною кіберзлочинністю.

30. Проблеми державного управління у сфері запобігання проявам організованої транснаціональної кіберзлочинності.

31. Напрями вирішення проблеми проявів організованої транснаціональної кіберзлочинності.

32. Державні механізми запобігання і протидії кіберзлочинності в умовах воєнного стану

33. Підходи і моделі реформування державних механізмів боротьби з кіберзлочинністю.

34. Напрями впорядкування правового підґрунтя діяльності та взаємовідносин в організаційно-функціональній структурі суб’єктів протидії кіберзлочинності.

35. Система запобігання кіберзлочинності в Україні.

36. Загальні теоретичні основи методики розслідування транснаціональних кіберзлочинів: криміналістичний аналіз

37. Теоретичні засади методики розслідування транснаціональних кіберзлочинів

38. Основи криміналістичної характеристики міжнародної організованої транснаціональної кіберзлочинності

39. Криміналістичний аналіз сучасної транснаціональної організованої кіберзлочинності

40. Фактори, властивості, риси, тенденції розвитку сучасної транснаціональної організованої кіберзлочинності

41. Загальна характеристика організованих злочинних груп в країнах Європейського Союзу

42. Типові напрями кримінальної діяльності організованих злочинних груп в країнах Європейського Союзу

43. Методичні основи розслідування транснаціональних кіберзлочинів.

44. Організаційні засади виявлення та початку кримінального провадження щодо транснаціональних кіберзлочинів.

45. Організаційно-тактичні основи розслідування транснаціональних кіберзлочинів.

46. Використання спеціальних знань під час розслідування транснаціональних кіберзлочинів.
47. Організаційно-правові основи боротьби з організованою транснаціональною кіберзлочинністю
48. Законодавство про боротьбу з організованою транснаціональною кіберзлочинністю
49. Система органів, які здійснюють боротьбу з організованою кіберзлочинністю
50. Система та повноваження органів, які здійснюють боротьбу з організованою транснаціональною кіберзлочинністю
51. Основні напрями боротьби з організованою транснаціональною кіберзлочинністю
52. Сучасна кібербезпека України: поняття, зміст, ознаки.
53. Нормативно-правова основа кібербезпеки в Україні.
54. Напрями кібербезпеки України. Суб'єкти забезпечення кібербезпеки в Україні: види, повноваження.
55. Співробітництво України з міжнародними партнерами у сфері забезпечення кібербезпеки. Кібербезпека України в умовах дії правового режиму воєнного часу.
56. Стан правового забезпечення захисту інформації в Україні. Кібербезпека: поняття, форми, види, напрями забезпеченн
57. Способи вчинення кримінальних правопорушень у сфері комп'ютерної інформації
58. Захист особи, індивідуальної, колективної і державної власності від злочинних комп'ютерних посягань
59. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності та інформаційна безпека комп'ютерних систем
60. Теоретико-правові засади міжнародного співробітництва держав у сфері протидії транснаціональній організованій кіберзлочинності та інформаційна безпека комп'ютерних систем
61. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.
62. Запобігання організованій транснаціональній кіберзлочинності.
63. Сучасний стан кримінально - правового забезпечення боротьби з кіберзлочинністю.
64. Детермінанти та основні напрямки запобігання організованій транснаціональній кіберзлочинності
65. Поняття організованої транснаціональної кіберзлочинності та її місце в загальній структурі злочинності. Сучасний стан та напрями запобігання
66. Стан сучасної кібербезпеки в Україні та у зарубіжних країнах. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі
67. Історичні аспекти прийняття Конвенції ООН проти транснаціональної організованої злочинності
68. Статус Конвенції ООН проти транснаціональної організованої злочинності
69. Мета та основна термінологія Конвенції ООН проти транснаціональної організованої злочинності
70. Сфера застосування Конвенції ООН проти транснаціональної організованої злочинності
71. Захист суверенітету та криміналізація участі в організованій злочинній групі в Конвенції ООН проти транснаціональної організованої злочинності
72. Взаємна правова допомога держав у боротьбі проти транснаціональної організованої злочинності
73. Загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісность та доступність інформації, даних і систем.
74. Види кримінальних правопорушень, які посягають на конфіденційність, цілісность та доступність інформації, даних і систем.
75. Причини та умови кримінальних праопорушень проти конфеденційності цілісності та доступності інформації, даних і систем
76. Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо) .
77. Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
78. Правові засади співпраці держав-членів Європейського Союзу у сфері боротьби із

кіберзлочинністю
79. Загальна характеристика кібербезпеки: сучасний стан та напрями вдосконалення. Запобігання організованій транснаціональній кіберзлочинності в Україні та окремих зарубіжних державах
80. Загальна характеристика кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
81. Кримінально-правова характеристика та види кіберзлочинів пов’язаних з кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
82. Кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особливої частини Кримінального кодексу України.
83. Загальна характеристика кіберзлочинів пов’язаних з контентом.
84. Кримінально-правова характеристика та види кіберзлочинів пов’язаних з контентом

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

1. Конвенція Організації Об’єднаних Націй проти транснаціональної злочинності 2000 року, ратифікована Законом України від 4 лютого 2004 року №1433-IV «Про ратифікацію Конвенції Організації Об’єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів по суші, морю і повітрю)».
2. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності: Ратифіковано із застереженнями і заявами Законом N 1433-IV (1433-15) від 04.02.2004. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text
3. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Прийнята резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 року. 2000. URL: https://zakon.rada.gov.ua/laws/show/995_789.
4. Конвенція про запобігання злочину геноциду і покарання за нього. Прийнято і запропоновано для підписання, ратифікації чи приєднання резолюцією 260 A (III) Генеральної Асамблеї від 9 грудня 1948 року. URL: http://www.preventgenocide.org/ua/konventsia.htm
5. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14
6. Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III. *Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
7. Кримінальний Кодекс України: Закон України від 5 квітня 2001 року. № 2341-III. *Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131.* URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
8. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/show/4651-17 5. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17
9. Кримінальне право України (Загальна та Особлива частини) : посіб. для підгот. до зовніш. незалеж. оцінювання / В. І. Тютюгін, М. А. Рубащенко ; відп. ред. В. І. Тютюгін. – 2-ге вид., перероб. і допов. – Харків : Право, 2021. – 336 с.
Кримінальне право України. Особлива частина: навчальний посібник / Попович О.В., Томаш Л.В., Латковський П.П., Бабій А.Ю. Чернівці, 2022. 319.
10. Кіберзлочинність та електронні докази. Cybercrime and digital evidence : навч. Посібник. Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf

Допоміжна:

1. Аніщук В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Т. 2 № 77. С. 139-143. URL: https://doi.org/10.24144/2307-3322.2023.77.2.23
2. Бакалинський О., Бакалинська О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2017. № 9. С. 100–108. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf
3. Батиргареєва В.С. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформації суспільства. Інформація і право. №1(40). С. 21-34. URL: https://doi.org/10.37750/2616-6798.2022.1(40).254339
4. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. Науковий вісник Ужгородського університету: серія: Право. 2023. Т.2. Вип. 75. С. 83-87. URL: https://doi.org/10.24144/2307-3322.2022.75.2.13
5. Буркаль В. С. Протидія транснаціональній організованій злочинності у сфері економіки : дисертація на здобуття наукового ступеня кандидата юридичних наук. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Ірпінь : Університет Державної фіскальної служби України, 2019. 242 с.
6. Гребенюк М., Черняк А. Деякі питання організаційно-правового характеру боротьби з організованою кіберзлочинністю в сучасних умовах. Підприємництво, господарство і право. 2019. № 4. С. 244–248.
7. Жаровська Г.П. Транснаціональна злочинність як реальна загроза національній безпеці України / Жаровська Г.П.. Науковий вісник Ужгородського національного університету. 2014. №27. С. 33–37.
8. Зінченко О. І. Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми. Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології». Вип. 39. 2021. С.118-122. URL: https://periodicals.karazin.ua/politology/article/view/17813
9. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: Матеріали міжнародної науково-практичної конференції. 21 квітня 2017 р., м. Київ, в 2-х частинах. Частина друга. / Упоряд.: В. М. Фурашев, С. Ю. Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. – 124 с. URL: http://ippi.org.ua/sites/default/files/ch-2_.pdf
10. Кіберзлочинність та електронні докази. Cybercrime and digital evidence : навч. Посібник. Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf
11. Колб О. Г., Колб Р. О. Нормативно-правові неузгодженості та суперечності інформаційної діяльності – одна із загроз національної безпеки України. Вісник Пенітенціарної асоціації України. Пенітенціарна асоціація України; Науково-дослідний інститут публічного права. Київ: ФОП Кандиба Т. П., 2020. № 3 (13). С. 90-97.
12. Кримінологія : підручник. О.М. Джужа, В.В. Василевич, В.В. Чернєй, С.С. Чернявський та ін. ; за заг. ред. д-ра юрид. наук, проф. В.В. Чернєя ; за наук. ред. д-ра юрид. наук, проф. О. М. Джужі. Київ : Нац. акад. внутр. справ, 2020. 612 с.URL: https://vo.uu.edu.ua/pluginfile.php/520868/mod_resource/content/3/2020_%D0%9F%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA_%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%8F.pdf
13. Леган І.М. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму. Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція. 2021. № 50. С. 118-121. URL: https://doi.org/10.32841/2307-1745.2021.50.25
14. Лугіна Н.А. та ін. Кримінологічна характеристика сучасного кіберзлочинця. Порівняльно-аналітичне право. 2019. №6. С. 400-402.
15. Любавіна В.П. Сутність кіберзлочинності та способи боротьби. *Молодий вчений, Серія: Юридичні науки. № 8 (108), 2022,* С. 22-25. URL: https://molodyivchenyi.ua/index.php/journal/article/view/5540/5426
16. Мамедова Е. Категоріальні та історико-правові аспекти державної політики кібербезпеки в Україні. Юридичний вісник. 2022. № 6. С. 272–281. URL: https://doi.org/10.32837/yuv.v0i6.2293

17. Міжнародні злочини. Енциклопедія сучасної України. URL: https://esu.com.ua/article-65159
18. Мошенець О. Міжнародний кримінальний суд – шлях до Гааги та репарацій.*LB.ua*.URL:https://lb.ua/blog/olena_moshenets/527492_mizhnarodniy_kriminalniy_sud-shlyah.html
19. Нашинець-Наумова А. Ю. Кіберзлочинність. нова кримінальна загроза. Наукові розвідки з актуальних проблем публічного та приватного права : Матеріали IV Всеукр. науково-практ. конф., м. Київ, 24 квіт. 2021 р. Київ, 2021. С. 111–114.
20. Неділько Я.В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). Держава і право. 2020. Вип. 88. С. 202-211. URL: doi.org//10.33663/1563-3349-2020-88-202
21. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 року, № 2149-IX. URL: https://ips.ligazakon.net/document/view/T222149?an=1
22. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII: станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
23. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. № 2163-VIII. *Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.* URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
24. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р.: станом на 3 лют. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
25. Прокопчук Т. Міжнародні стандарти кримінально-правової охорони інформації з обмеженим доступом. Підприємництво, господарство і право. 2021. № 3. С. 232-239. URL: https://doi.org/10.32849/2663-5313/2021.3.38
26. Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності: Протокол ратифіковано Законом N 1433-IV (1433-15) від 04.02.2004. URL: https://zakon.rada.gov.ua/laws/show/995_791#Text
27. Протокол проти незаконного ввозу мігрантів по суші, морю і повітрю, що доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності: Протокол ратифіковано Законом N 1433-IV (1433-15) від 04.02.2004 URL: https://zakon.rada.gov.ua/laws/show/995_790#Text
28. Протокол проти незаконного виготовлення та обігу вогнепальної зброї, її складових частин і компонентів, а також боєприпасів до неї, який доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності: Закон України № 159-VII від 02.04.2013. URL: https://zakon.rada.gov.ua/laws/show/995_792#Text
29. Пшеничний І. В. Організована транснаціональна злочинність і роль правоохоронних органів у протидії їй : дис. ... канд. юрид. наук [Електронний ресурс] /І. В. Пшеничний. К., 2000. 220 с. URL: http://inter.criminology. onua.edu.ua/?p=1492.
30. Радутний О. Е. Інформація, яка надходить у режимі реального часу через веб-камеру, як предмет злочину, що передбачений ст. 301 КК України. Інформація і право. 2014. № 1. С. 115-119. URL: http://nbuv.gov.ua/UJRN/Infpr_2014_1_16 7. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник. Одеса. 2020. 112 с.
31. Рульов І. Співвідношення кібертероризму та кіберзлочину. Юридичний вісник. 2021. № 3. С. 178–185. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/2202
32. Рябчун Ю. Міжнародний суд ООН в Гаазі зобов'язав росію негайно призупинити воєнні дії в Україні. *Суспільне. Новини.* URL: https://suspilne.media/218256-miznarodnij-sud-oon-v-gaazi-ogolosue-risenna-u-spravi-ukraina-proti-rosii-nazivo/
33. Самойленко О. А. Відкриття кримінального провадження щодо злочинів, вчинених у кіберпросторі. Підприємство, господарство і право. 2019. №8. С. 222-225
34. Сащенко М. Проблемні аспекти запобігання кіберзлочинності в україні. Молодий вчений. 2022. Вип. 1 (101). С. 17-20. https://doi.org/10.32839/2304-5809/2022-1-101-4
35. Стельмахов В.Ю. Шляхи подолання транснаціональної організованої злочинності / Стратегія кібербезпеки України «Безпечний кіберпростір – запорука успішного розвитку країни». Затверджена Указом Президента України від 26 серпня 2021 року № 447/2021.

36. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Серія Право. 2018. Вип. 6 (18). С. 154–163.
37. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. 2020. Т. 31 (70) Ч. 2, № 2. С. 119–124. URL: https://juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf
38. Ткаля О. В. Проблемні аспекти розуміння транснаціональної організованої злочинності. Порівняльно-аналітичне право. 2019. № 1. С. 318–321.
39. Трофименко О. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Т. 21, № 3. С. 150–157. URL: http://surl.li/ikwhsp
40. Уткіна Г. А., Лопушенко Г. М. Кіберзлочинність та перспективи її протидії. Регіональні особливості злочинності: сучасні тенденції та стратегії протидії: збірник. матеріалів Всеукраїнської науково-практичної конференції. Кривий Ріг - 14 травня 2021 р. С. 379-380.
41. Філіппов С. О. Кримінологічні засади протидії транскордонній злочинності : дисертація на здобуття наукового ступеня доктора юридичних наук. 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». Хмельницький : Університет Державна прикордонна служба України, 2019. 561 с.
42. Форос Г.В. Кримінально правова охорона з обмеженим доступом. Південноукраїнський правничий часопис. 2016. № 3-4.С. 64-66. URL: http://www.sulj.oduvs.od.ua/archive/2016/3-4/21.pdf
43. Шемчук В.В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки. Том 29 (68) № 6 2018.* С. 119-124. URL: https://www.juris.vernadskyjournals.in.ua/journals/2018/6_2018/23.pdf
44. Шостко О.Ю., Подільчак О.М. Сучасні світові тенденції злочинності. Проблеми законності. 2020. Вип. 148. С. 184–200.
45. Маліцька В. Воєнний стан в Україні. Пояснюємо, до якого числа та що треба знати. Вікна. URL: https://vikna.tv/video/ukrayina/voyennyj-stan-v-ukrayini-prodovzhyly-do-yakogo-chysla-i-shho-potribno-znaty/
46. Національна поліція в умовах воєнного стану: зміни в законодавстві. *Право в умовах війни.* URL: https://law-in-war.org/naczionalna-policziya-v-umovah-voyennogo-stanu-zminy-v-zakonodavstvi/
47. Ортинський В. Взаємодія підрозділів правоохоронних органів України у протидії контрабанді наркотичних засобів: теоретичні та практичні аспекти. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13273/3.pdf

Інформаційні ресурси Інтернет:

1. Єдиний веб-портал органів виконавчої влади України. Урядовий портал. URL: https://www.kmu.gov.ua/
2. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/
3. Офіційне інтернет-представництво Президента України. Офіційний веб-портал. URL: https://www.president.gov.ua/ Офіційний інтернет-портал Верховної Ради України. Офіційний веб-портал. URL: https://www.rada.gov.ua/
4. Офіційний інтернет-портал Збройних Сил України. Офіційний веб-портал. URL: https://www.zsu.gov.ua/
5. Офіційний сайт Міністерства внутрішніх справ. Офіційний веб-портал.URL: https://mvs.gov.ua/
6. Офіційний сайт Міністерства оборони України. Офіційний веб-портал. URL: https://www.mil.gov.ua/
7. Офіційний сайт Національної гвардії України. Офіційний веб-портал. URL: https://ngu.gov.ua/
8. Офіційний сайт Національної поліції України. Офіційний веб-портал. URL: https://www.npu.gov.ua/
9. Офіційний сайт Офісу Генерального прокурора. Офіційний веб-портал. URL: https://www.gp.gov.ua/
10. Офіційний сайт Служби безпеки України. Офіційний веб-портал. URL: https://ssu.gov.ua/
11. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/
12. Офіціний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/

Міжнародні видання:

1. Computer Emergency Response Team of Ukraine – CERT-UA. cert.gov.ua. URL: https://cert.gov.ua/

2. Dr. Marina Caparini Transnational organized crime: A threat to global public goods. Stockholm international peace research institute. URL: https://www.sipri.org/commentary/topical-backgrounder/2022/transnational-organized-crime-threat-global-public-goods

3. Marco Marsili. The War on Cyberterrorism. Democracy and Security. Volume 15. Issue 2. P. 172-199. URL: https://sci-hub.se/10.1080/17419166.2018.1496826

4. United Nations Convention against Transnational Organized Crime and the Protocols Thereto. Office on Drugs and Crime. URL: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html United Nations Convention against transnational organized crime and the Protocols thereto. URL: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

5. Злочини міжнародного характеру. (З практики застосування термінів, слів та словосполучень у юриспруденції). URL: https://ips.ligazakon.net/document/TS002019

6. Community-Police Engagement Resources. URL: https://www.discoverpolicing.org/explore-the-field/educational-resources-for-law-enforcement-and-the-community/

7. How does the FBI interact with other federal law enforcement agencies? URL: https://www.fbi.gov/about/faqs/what-is-the-fbi-doing-to-improve-its-interaction-with-other-federal-law-enforcement-agencies

8. How the International Criminal Court works. Official site International Criminal Court. URL: https://www.icc-cpi.int/about/how-the-court-works International Criminal Court. Human Rights watch. URL: https://www.hrw.org/topic/international-justice/international-criminal-court

9. Pol, F.R. (2020) Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. Policy Design and Practice, 1, 73–94. Recovered from: https://www.researchgate.net/publication/339486326_Anti-money_laundering_The_world's_least_effective_policy_experiment_Together_we_can_fix_it/link/5e55561e4585152ce8ee54c5/download

10. Pol, F.R. (2020) Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. Policy Design and Practice, 1, 73–94. Recovered from: https://www.researchgate.net/publication/339486326_Anti-money_laundering_The_world's_least_effective_policy_experiment_Together_we_can_fix_it/link/5e55561e4585152ce8ee54c5/download

11. Pontes, R., Lewis, N., McFarlane, P., & Craig, P. (2021) Anti-money laundering in the United Kingdom: new directions for a more effective regime. Journal of Money Laundering Control. Vol. print number before print. Recovered from: https://doi.org/10.1108/JMLC-04-2021-0041.

12. Problem aspects of interaction of law enforcement authorities in the field of countering money laundering. URL: https://amazoniainvestiga.info/index.php/amazonia/article/view/1850/2293

13. The Role of the International Criminal Court. URL: https://www.cfr.org/backgrounder/role-international-criminal-court

8. ЛИСТ ОНОВЛЕННЯ ТА ПЕРЕЗАТВЕРДЖЕННЯ

ЛИСТ ОНОВЛЕННЯ ТА ПЕРЕЗАТВЕРДЖЕННЯ
РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«»

РОЗГЛЯНУТО ТА СХВАЛЕНО
на засіданні кафедри кримінального права та процесу
від _____ 20__р. № __

Лист оновлення та перезатвердження РПНД

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри	Підпис гаранта ОП