МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут права
Кафедра кримінального права та процесу

Затверджено
Науково-методичною радою Університету,
протокол від «18» 09 2024 р. № 1
Голова НМР _____ Іван ШЕМЕЛИНЕЦЬ

Робоча програма
навчальної дисципліни
«Актуальні проблеми кваліфікації та протидії кіберзлочинності»

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 «Актуальні проблеми кваліфікації та протидії кіберзлочинності» 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: Г. Дідківська, д.ю.н., професор

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 «Актуальні проблеми кваліфікації протидії кіберзлочинності» є надання здобувачам вищої освіти поглиблених знань щодо теоретичних основ, сутності та особливостей запобіжної діяльності правоохоронних органів зокрема у сфері протидії кіберзлочинності, сучасних тенденцій розвитку кіберзлочинності та правових механізмів запобігання кіберзлочинам, а також детального аналізу окремих видів кіберзлочинів. При цьому здобувачі повинні з'ясувати: які існують актуальні проблеми щодо кваліфікації та протидії кіберзлочинності.

Завданнями навчальної дисципліни «Актуальні проблеми кваліфікації та протидії кіберзлочинності» є формування у здобувачів вищої освіти поглиблених знань та уявлень про сучасний стан законодавства в Україні щодо протидії кіберзлочинності ; вивчення здобувачами вищої освіти генезису виникнення кримінально-правової політики протидії кіберзлочинності; розширення уявлення здобувачів про предмет протидії та запобігання злочинності, його співвідношення з іншими науковими дисциплінами; висвітлення сучасних проблем щодо актуальних проблем кваліфікації та протидії кіберзлочинності; документування правової інформації; отримання поглиблених знань в частині попередження та запобігання злочинності; відпрацювання навичок та умінь аналізу і діагностики щодо актуальності проблем кваліфікації та протидії кіберзлочинності.

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 та практичні заняття, самостійна робота та індивідуально-консультаційна робота.

Організація поточного контролю та підсумкового контролю знань: основним завданням контролю знань студентів є оцінювання засвоювання ними теоретичних знань з дисципліни «Актуальні проблеми кваліфікації протидії кіберзлочинності». При цьому контрольні заходи мають стимулювати: систематичну самостійну роботу над навчальним матеріалом, забезпечити закріплення набутих теоретичних знань; прищепити навички відповідального ставлення до своїх обов'язків, самостійного цілеспрямованого пошуку потрібної інформації, чіткої організації свого робочого часу. Контроль роботи студента є необхідним компонентом навчального процесу, який має за мету визначення реального рівня професійної підготовки студента, а також надання необхідних рекомендацій, що сприяють подальшому розвитку творчої особистості студента. Логічним завершенням процесу контролю є процедура оцінювання. Результати навчальної діяльності студентів оцінюються за допомогою двох модульних контрольних заходів. Оцінювання здійснюється наступними способами*:* поточне тестування, оцінювання знань шляхом індивідуального усного опитування, перевірки засвоєння питань, відведених на самостійну роботу. Підсумкова форма контролю – екзамен.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Код академічної групи ПМПД-24-1; ПМПД-24-2; ПМПДЗ-24-1

Показники	**Характеристика навчальної дисципліни**	
	Денна форма навчання	**Заочна форма навчання**
Кількість кредитів ЄКТС - 4	4	4
Модулів - 2	Рік підготовки:	
Змістових модулів - 2	1-й	1-й
Загальна кількість годин - 120 годин	Семестр	
	2-й	2-й
	Лекції	
	22 год.	4 год.
	Семінарські заняття	
	18 год.	4 год.
	Самостійна робота	
	78 год.	110 год.
	Індивід.-консультац. робота: 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. СК13. Здатність у передбачених законом випадках застосовувати засоби фізичного впливу, спеціальні засоби та вогнепальну зброю, тактичні прийоми під час службової діяльності в разі отримання інформації чи безпосереднього виявлення ознак правопорушення перебуваючи на місці події та в інших службових ситуаціях. СК15. Здатність вживати заходів з метою запобігання, виявлення та припинення адміністративних і кримінальних правопорушень, заходів, спрямованих на усунення загроз приватним та публічним інтересам людини й держави. ФК1. Здатність забезпечувати та здійснювати заходи з виявлення, протидії та проваджень щодо кіберзлочинів. ФК2. Здатність збирати та оцінювати докази, використовувати криміналістичні методи та засоби в професійній діяльності, прогнозувати поведінку правопорушників та вживати превентивні заходи.	РН5. Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення. РН15. Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку. РН17. Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальних засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності). РН19. Аналізувати обстановку, рівень потенційних загроз та викликів, прогнозувати розвиток дій правопорушників, вживати заходів з метою запобігання, виявлення та припинення правопорушень. РН20. Застосовувати заходи, спрямовані на запобігання та протидію кіберзлочинам. РН21. Організовувати взаємодію національних правоохоронних організацій з

	міжнародними з метою протидії кіберзлочинності. РН22. 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 ОП «Правове забезпечення протидії кіберзлочинності» є навчальні дисципліни: «Управління правоохоронною діяльністю», «Актуальні проблеми кримінального права», «Актуальні питання кримінально-правової та кримінологічної характеристики кіберзлочинності в Україні».

Постреквізитами ОП «Правове забезпечення протидії кіберзлочинності» є навчальні дисципліни: «Кримінальні процесуальні та криміналістичні проблеми розслідування кіберзлочинів», «Міжнародні стандарти правоохоронної діяльності»,

2.3.СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Код академічної групи ПМПД-24-1; ПМПД-24-2

№ п/п	Змістові модулі	Кількість годин				
		Лекції (год.)	Семінарські (год.)	Інд.-конс. робота під кер. викладача (год)	СРС (год.)	Всього (год.)
МОДУЛЬ І – 2 кредити (60 годин)						
ЗМ 1 (Теми 1-5)						
Т.1	Поняття та загальна характеристика кіберзлочинності.	2	2	-	8	12
Т.2	Мета, завдання, функції та принципи кваліфікації та протидії кіберзлочинності.	2	2	-	8	12
Т.3	Становлення системи кваліфікації та протидії кіберзлочинності в Україні.	2	2	-	8	12
Т.4	Суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності.	2	2	-	8	12
Т.5	Особливості вчинення правопорушником кіберзлочинів.	2	2	-	8	12
Всього по модулю 1:		10	10	0	40	60
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
МОДУЛЬ ІІ – 2 кредити (60 годин)						
ЗМ 2 (Теми 6-9)						
Т.6	Технічні та інформаційні засоби вчинення кіберзлочинів.	4	-	-	9	13
Т.7	Шахрайство та підробка, вчинені з використанням технічних та інформаційних систем як вид кіберзлочину.	2	2	-	9	13
Т.8	Методика розслідування кіберзлочинів: організаційні засади та особливості	2	2	2	10	16
Т.9	Узаконення доходів, одержаних у сфері	2	2	-	10	14

	кіберзлочинності: проблеми та шляхи їх вирішення					
Т.10	Міжнародне співробітництво держав у боротьбі з кіберзлочинністю	2	2	-	-	4
Всього по модулю 2:		12	8	2	38	60
Форма контролю: модульна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
Форма підсумкового контролю – екзамен.						
Усього за навчальною дисципліною:		22	18	2	78	120

Код академічної групи ПМПДЗ-24-1

№ п/п	**Змістові модулі**	**Кількість годин**				
		Лекції (год.)	**Семінарські (год.)**	**Інд.-конс. робота під кер. викладача (год)**	**СРС (год.)**	**Всього (год.)**
МОДУЛЬ І – 2 кредити (60 годин)						
ЗМ 1 (Теми 1-5)						
Т.1	Поняття та загальна характеристика кіберзлочинності.	2	-	-	11	13
Т.2	Мета, завдання, функції та принципи кваліфікації та протидії кіберзлочинності.	-	-	-	11	11
Т.3	Становлення системи кваліфікації та протидії кіберзлочинності в Україні.	-	-	-	11	11
Т.4	Суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності.	-	-	-	12	12
Т.5	Особливості вчинення правопорушником кіберзлочинів.	-	2	-	11	13
Всього по модулю 1:		2	2	0	56	60
МОДУЛЬ ІІ – 2 кредити (60 годин)						
ЗМ 2 (Теми 6-9)						
Т.6	Технічні та інформаційні засоби вчинення кіберзлочинів.	2	-	-	10	12
Т.7	Шахрайство та підробка, вчинені з використанням технічних та інформаційних систем як вид кіберзлочину.	-	2	-	12	14
Т.8	Методика розслідування кіберзлочинів: організаційні засади та особливості	-	-	2	10	12
Т.9	Узаконення доходів, одержаних у сфері кіберзлочинності: проблеми та шляхи їх вирішення	-	-	-	12	12
Т.10	Міжнародне співробітництво держав у боротьбі з кіберзлочинністю	-	-	-	10	10
Всього по модулю 2:		2	2	2	54	60
Форма контролю: аудиторна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
Форма підсумкового контролю – екзамен.						
Усього за навчальною дисципліною:		4	4	2	110	120

РЕЙТИНГ-ПЛАН
Денна форма навчання

Години	Тема	Форма заняття	Результати навчання	Вага оцінки
Модуль 1				
2	Т.1. Поняття та загальна характеристика кіберзлочинності.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.1. Поняття та загальна характеристика кіберзлочинності.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.2. Мета, завдання, функції та принципи кваліфікації та протидії кіберзлочинності	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.2. Мета, завдання, функції та принципи кваліфікації та протидії кіберзлочинності	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.3. Становлення системи кваліфікації та протидії кіберзлочинності в Україні.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.3. Становлення системи кваліфікації та протидії кіберзлочинності в Україні.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.4. Суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.4. Суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.5. Особливості вчинення правопорушником кіберзлочинів.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.5. Особливості вчинення правопорушником кіберзлочинів.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
	Т 1-5	Проміжний модульний контроль		5
	Усього за Модулем І			**20**
4	Т.6. Технічні та інформаційні засоби вчинення кіберзлочинів.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.7. Шахрайство та підробка, вчинені з використанням технічних та	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0

	інформаційних систем як вид кіберзлочину.			
4	Т.7. Шахрайство та підробка, вчинені з використанням технічних та інформаційних систем як вид кіберзлочину.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.8. Методика розслідування кіберзлочинів: організаційні засади та особливості	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.8. Методика розслідування кіберзлочинів: організаційні засади та особливості	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.9. Узаконення доходів, одержаних у сфері кіберзлочинності: проблеми та шляхи їх вирішення	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.9. Узаконення доходів, одержаних у сфері кіберзлочинності: проблеми та шляхи їх вирішення	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
2	Т.10. Міжнародне співробітництво держав у боротьбі з кіберзлочинністю	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0
2	Т.10. Міжнародне співробітництво держав у боротьбі з кіберзлочинністю	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	3
	Т 6-9	Проміжний модульний контроль		5
	Індивідуально-консультаційна робота	Тема 8		8
	Комп'ютерне тестування на платформі дистанційного навчання			5
	Усього за Модулем ІІ			**30**
	Екзамен			**50**
	Усього за курсом			**100**

Заочна форма навчання
Код академічної групи: ПМПДЗ-24-1

Години	**Тема**	**Форма заняття**	**Результати навчання**	**Вага оцінки**
Модуль І				
2	Поняття та загальна характеристика кіберзлочинності.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	0

2	Особливості вчинення правопорушником кіберзлочинів.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	10
	Усього за Модулем І			**10**
Модуль ІІ				
2	Технічні та інформаційні засоби вчинення кіберзлочинів.	Лекція	РН5, РН15, РН17, РН19, РН20, РН21, РН22	
2	Шахрайство та підробка, вчинені з використанням технічних та інформаційних систем як вид кіберзлочину.	Семінарське заняття	РН5, РН15, РН17, РН19, РН20, РН21, РН22	10
	Аудиторна контрольна робота			15
2	Індивідуально-консультаційна робота			10
	Комп'ютерне тестування на платформі дистанційного навчання			5
	Усього за Модулем ІІ			**40**
	Усього за Модулем І, ІІ			**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 заняттях, зокрема: в середовищі Windows (Write, NotePad/Блокнот, WordPad, Microsoft Word, Microsoft Excel, Microsoft PowerPoint); 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. Поняття та загальна характеристика кіберзлочинності.

План лекційного заняття

1. Поняття кіберзлочинності та її місце в загальній структурі злочинності.
2. Ознаки та види кіберзлочинності.
3. Поняття та система механізмів запобігання кіберзлочинності:.
4. Основні проблеми кваліфікації та протидії кіберзлочинності.

План семінарського заняття

1. Поняття кіберзлочинності та її місце в загальній структурі злочинності.
2. Ознаки та види кіберзлочинності.
3. Поняття та система механізмів запобігання кіберзлочинності:.
4. Основні проблеми кваліфікації та протидії кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Класифікація кіберзлочинів.
2. Злочини, вчинені з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі

3. Визначення сутності кіберзлочинів.

Питання для самоконтролю

1. Якими термінами позначають явище «кіберзлочинність»? Як співвідносяться ці терміни?
2. Назвіть недоліки законодавчого визначення кіберзлочину в Україні.
3. Які існують заходи міжнародного співробітництва у сфері боротьби з кіберзлочинністю?
4. Які ознаки кіберзлочинності можна виділити?
5. Охарактеризуйте видову характеристику кіберзлочинності.
6. Проаналізуйте механізм запобігання кіберзлочинності.

Рекомендована література

Основна: [2, 4, 5, 8].
Допоміжна: [2, 4, 12, 15].
Інформаційні ресурси Інтернет [3, 5].
Міжнародні видання: [1, 2].

Тема 2. Мета, завдання, функції та принципи кваліфікації та протидії кіберзлочинності.

План лекційного заняття

1. Мета, завдання та функції протидії кіберзлочинності.
2. Стратегія протидії кіберзлочинності в США.
3. Європейська система запобігання кіберзлочинності.

План семінарського заняття

1. Мета, завдання та функції протидії кіберзлочинності.
2. Стратегія протидії кіберзлочинності в США.
3. Європейська система запобігання кіберзлочинності.
4. Використання світового досвіду для запобігання та протидії злочинності в Україні;

Самостійна робота здобувачів вищої освіти

1. Перелік джерел законодавства України щодо кримінально-правової охорони суспільних відносин у кіберпросторі.
2. Умови формування кримінальних мотивів вчинення кіберзлочину.
3. Прогнозування та планування в сфері кіберзахисту.
4. Проаналізуйте мету, задачі та функції запобігання кіберзлочинам на рівні держави та міжнародному рівні.

Питання для самоконтролю

1. Який підхід до визначення кіберзлочину домінує в зарубіжній кримінології?
2. Надайте характеристику загальним засадам запобігання та протидії кіберзлочинності в зарубіжних країнах.
3. Охарактеризуйте становлення та розвиток запобігання та протидії кіберзлочинності в зарубіжних країнах.
4. Визначте сучасний стан, динаміку, рівень кіберзлочинності в країнах Європи.
6. Охарактеризуйте організовану злочинність в США.

Рекомендована література

Основна: [2, 4, 5, 8].
Допоміжна: [2, 4, 12, 15].
Інформаційні ресурси Інтернет [3, 5].
Міжнародні видання: [1, 2].

Тема 3. Становлення системи кваліфікації та протидії кіберзлочинності в Україні

План лекційного заняття

1. Поняття системи протидії кіберзлочинності в Україні.
2. Класифікація запобіжних заходів протидії кіберзлочинності.
3. Організація і управління процесом протидії кіберзлочинності в Україні.

План семінарського заняття

1. Поняття системи протидії кіберзлочинності в Україні.
2. Класифікація запобіжних заходів протидії кіберзлочинності.
3. Організація і управління процесом протидії кіберзлочинності в Україні.
4. Інтегративна система кваліфікації та протидії кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Поняття системи протидії кіберзлочинності в Україні.
2. Заходи протидії кіберзлочинності в Україні.
3. Структура протидії кіберзлочинності.
4. Механізм протидії кіберзлочинності.
5. Методики кримінологічного аналізу кіберзлочинності в Україні.

Питання для самоконтролю

1. Визначте сучасний стан кіберзлочинності в Україні.
2. Надайте поняття системи протидії кіберзлочинності в Україні та охарактеризуйте її зміст.
3. Визначте провідні напрями моніторингу протидії кіберзлочинності в Україні.
4. У чому полягає узгодженість кримінального права та кримінології при запобіганні та протидії кіберзлочинності в Україні?
5. Надайте характеристику оцінки вимірювання кіберзлочинності в Україні.
6. Розкрийте заходи підвищення ефективності щодо протидії кіберзлочинності в Україні.
7. Виокреміть напрями протидії кіберзлочинності в Україні, надайте їх характеристику.

Рекомендована література

Основна: [2, 3, 4, 5, 7, 8]
Допоміжна: [4, 6, 14, 15]
Інформаційні ресурси Інтернет: [3, 4, 5]
Міжнародні видання: [1, 2, 3].

Тема 4. Суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності

План лекційного заняття

1. Суб'єкти системи протидії та запобігання кіберзлочинності.
2. Об'єкти запобіжного впливу кіберзлочинів.
3. Види, на які поділяються суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності.

План семінарського заняття

1. Суб'єкти системи протидії та запобігання кіберзлочинності.
2. Об'єкти запобіжного впливу кіберзлочинів.
3. Види, на які поділяються суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності.
4. Спеціалізовані та неспеціалізовані суб'єкти протидії кіберзлочинності.
5. Об'єкти загально-соціальної профілактики протидії та запобігання кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Чинники, що впливають на детермінацію кіберзлочинності;
2. Організаційно-управлінські функції щодо запобігання та протидії кіберзлочинності.
3. Запобіжна робота суб'єктів системи запобігання та протидії кіберзлочинності.
4. Комплексне планування запобігання та протидії кіберзлочинності.

Питання для самоконтролю

1. Надайте загальну характеристику суб'єктів для яких запобігання та протидія кіберзлочинності є однією з головних функцій у межах правоохоронної діяльності.
2. В чому полягає координація запобіжної діяльності правоохоронних органів?
3. Назвіть форми кримінологічної поінформованості населення про злочинність.
4. В чому полягає слідча профілактика?
5. Яка роль центрів реабілітації та адаптації у запобіганні рецидивної злочинності.

Рекомендована література

Основна: [4, 5, 6, 7, 8]
Допоміжна: [2, 3, 12, 13]
Інформаційні ресурси Інтернет: [3, 4, 5]
Міжнародні видання: [1, 3].

Тема 5. Особливості вчинення правопорушником кіберзлочинів.

План лекційного заняття

1. Загальна характеристика злочинця у сфері кібернетики.
2. Мотивація кіберзлочинців.
3. Інструменти та методи, що використовує правопорушник при скоєнні кіберзлочинів.

4. Попередження скоєння кіберзлочинцями правопорушення.

План семінарського заняття

1. Загальна характеристика злочинця у сфері кібернетики.
2. Мотивація кіберзлочинців.
3. Інструменти та методи, що використовує правопорушник при скоєнні кіберзлочинів.
4. Попередження скоєння кіберзлочинцями правопорушення.

Самостійна робота здобувачів вищої освіти

1. Користуючись публікаціями у засобах масової інформації знайдіть реальні приклади кіберзлочинів. Проаналізуйте їх з точни зору соціально-демографічних та морально-психологічних ознак осіб, які їх вчинили.
2. Складіть таблицю «Морально-психологічні якості особи-кіберзлочинця»

Питання для самоконтролю

1. Розкрийте поняття «особа кіберзлочинця». Аргументуйте свою відповідь.
2. Яка можлива мотивація кіберзлочинця при скоєнні ним злочинів?
3. Які інструменти та методи, використовує правопорушник при скоєнні кіберзлочинів?
4. Як запобігти скоєнню злочину правопорушником у сфері кібернетики?

Рекомендована література

Основна: [2, 5, 6, 7, 9, 10]
Допоміжна: [2, 3, 6, 8]
Інформаційні ресурси Інтернет: [3, 5]
Міжнародні видання: [2, 3].

Модуль ІІ.
Змістовий модуль 2.

Тема 6. Технічні та інформаційні засоби вчинення кіберзлочинів.

План лекційного заняття

1. Класифікація технічних та інформаційних засобів вчинення кіберзлочинів.
2. Інформаційні технології, які найчастіше використовуються для вчинення кіберзлочинів.
3. Особливості кіберзлочинів, що вчиняються за допомогою технічних та інформаційних засобів.

План семінарського заняття

1. Класифікація технічних та інформаційних засобів вчинення кіберзлочинів.
2. Інформаційні технології, які найчастіше використовуються для вчинення кіберзлочинів.
3. Особливості кіберзлочинів, що вчиняються за допомогою технічних та інформаційних засобів.

Самостійна робота здобувачів вищої освіти

1. Складіть задачу про кримінальне правопорушення яке вчиняється із використанням технічних та інформаційних засобів у сфері кібернетики.
2. Проаналізуйте Кримінальний кодекс України та знайдіть приклади кримінальних правопорушень, які вчиняються за допомогою технічних та інформаційних засобів.

Питання для самоконтролю

1. Які нові технології можуть стати інструментом для нових видів кіберзлочинів?.
2. Які інформаційні та технічні засоби найчастіше використовує кіберзлочинець?
3. Сформулюйте класифікацію технічних та інформаційних засобів вчинення кіберзлочинів
4. Які є причини вчинення кримінальних правопорушень за допомогою даних засобів?
5. Визначте умови вчинення кримінальних правопорушень інформаційними та технічними засобами.

Рекомендована література

Основна: [5, 6, 8, 10]
Допоміжна: [2, 3, 4, 12]
Інформаційні ресурси Інтернет: [1, 3, 5]
Міжнародні видання: [2, 3].

Тема 7. Шахрайство та підробка, вчинені з використанням технічних та інформаційних систем як вид кіберзлочину.

План лекційного заняття

1. Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами.
2. Шахрайство, що вчинене з використанням комп’ютерних технологій та інформаційно-комунікаційних систем.
3. Вплив штучного інтелекту на еволюцію кіберзлочинності.

План семінарського заняття

1. Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами.
2. Шахрайство, що вчинене з використанням комп’ютерних технологій та інформаційно-комунікаційних систем.
3. Вплив штучного інтелекту на еволюцію кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Назвіть ідеї і положення міжнародних практик запобігання кіберзлочинам, що знайшли своє втілення в національному законодавстві та практичній діяльності у сфері боротьби з кіберзлочинністю.
2. Назвіть, які кримінально карані діяння у віртуальному просторі відображаються у офіційній статистиці України.
3. Причини і умови кіберзлочинів, пов’язаних з контентом (змістом даних), розміщених у комп’ютерних мережах (зокрема злочини, пов’язані з дитячою порнографією).

Питання для самоконтролю

1. Охарактеризуйте кіберзлочини, що пов'язані з комп'ютерами.
2. Яка специфіка кіберзлочинів пов'язаних з комп'ютерами?
3. Назвіть відмінності кіберзлочинів пов'язаних з комп'ютерами від традиційних злочинів.
4. Яких змін зазнала кіберзлочинність після появи штучного інтелекту?
5. Як штучний інтелект впливає на еволюцію кіберзлочинності?

Рекомендована література

Основна: [5, 6, 8, 9]
Допоміжна: [1-4, 12, 13]
Інформаційні ресурси Інтернет: [1, 3, 5]
Міжнародні видання: [1, 3].

Тема 8. Методика розслідування кіберзлочинів: організаційні засади та особливості

План лекційного заняття

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

План семінарського заняття

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

Самостійна робота здобувачів вищої освіти

1. Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів.
2. Характеристика корупційної кіберзлочинності.
3. Причини та умови корупційної злочинності.
4. Запобігання корупційній злочинності.

Питання для самоконтролю

1. Які основні труднощі виникають при зборі та фіксації доказів у кіберпросторі? Які сучасні методи та інструменти можуть бути використані для їх подолання?
2. Визначте організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів.
3. Як змінюються методи розслідування кіберзлочинів з розвитком технологій?
4. Які нові виклики постають перед слідчими у зв'язку з появою штучного інтелекту, блокчейну та

інших інновацій?
Рекомендована література
Основна: [2, 4, 5, 8].
Допоміжна: [2, 4, 12, 15].
Інформаційні ресурси Інтернет [3, 5].
Міжнародні видання: [1, 2].

Тема 9. Узаконення доходів, одержаних у сфері кіберзлочинності: проблеми та шляхи їх вирішення

План лекційного заняття

1. Види узаконення доходів, що одержані у сфері кіберзлочинності.
2. Механізми узаконення злочинних доходів, одержаних у сфері кіберзлочинності та їх викриття.
3. Використання інформаційних систем для відмивання доходів, одержаних у сфері кібернетичної злочинності.
4. Попередження та запобігання легалізації доходів, одержаних у сфері кіберзлочинності.

План семінарського заняття

1. Види узаконення доходів, що одержані у сфері кіберзлочинності.
2. Механізми узаконення злочинних доходів, одержаних у сфері кіберзлочинності та їх викриття.
3. Використання інформаційних систем для відмивання доходів, одержаних у сфері кібернетичної злочинності.
4. Попередження та запобігання легалізації доходів, одержаних у сфері кіберзлочинності.

Самостійна робота здобувачів вищої освіти

1. Проаналізувавши дані статистичної інформації Офісу Генерального прокурора «Єдиний звіт про кримінальні правопорушення» (https://www.gp.gov.ua/ua/1stat):
1) побудуйте секторальну діаграму, що відображає структуру кіберзлочинності в Україні за видами кеберзлочинів за останній звітній період (один рік);
2) створіть графічне зображення динаміки кіберзлочинності в Україні за останні 5 років та поясність, які чинники можуть впливати на зростання або зниження рівня злочинності.

Питання для самоконтролю

1. Дайте визначення поняттю легалізація доходів, що одержані у сфері кіберзлочинності
2. Назвіть види узаконення доходів, одержаних у сфері кіберзлочинності.
3. Які інформаційні системи використовуються для відмивання доходів, одержаних у сфері кібернетичної злочинності?
4. Як попередити та запобігти легалізації доходів, одержаних у сфері кіберзлочинності?

Тема 10. Міжнародне співробітництво держав у боротьбі з кіберзлочинністю

План лекційного заняття

1. Основні напрямки співпраці у боротьбі з кібернетичною злочинністю.
2. Кібервійна як міжнародний злочин.
3. Способи запобігання та уникнення кібервійн.

План семінарського заняття

1. Сучасні напрямки співпраці у боротьбі з кібернетичною злочинністю.
2. Кібервійна як міжнародний злочин.
3. Способи запобігання та уникнення кібервійн.

Самостійна робота здобувачів вищої освіти

1. На основі аналізу статистичної інформації Офісу Генерального прокурора «Єдиний звіт про кримінальні правопорушення» (https://www.gp.gov.ua/ua/1stat) та статистичної інформації Держкомстату України (http://www.ukrstat.gov.ua/) «Про чисельність населення, станом на 1 січня 2024 року»:
1) обчисліть коефіцієнт злочинної інтенсивності в сфері вчинення кіберзлочинів в цілому по Україні у розрахунку на 10 тис. населення за останній звітній період (один рік);
2) здійсніть рейтингування областей України за кількістю облікованих кіберзлочинів, а також за коефіцієнтом злочинної інтенсивності та поясність одержані результати.

Питання для самоконтролю

1. Назвіть сучасні напрямки співпраці у боротьбі з кібернетичною злочинністю.

2. Охарактеризуйте кібервійну як злочин міжнародного масштабу.
3. Як уникнути кібервійн?
4. Вкажіть тенденції розвитку кіберзлочинності, які прогнозуються на майбутнє та як вони можуть вплинути на нові форми кіберзлочинних активностей.

Рекомендована література
Основна: [2, 5, 6, 7, 9, 10]
Допоміжна: [2, 3, 6, 8]
Інформаційні ресурси Інтернет: [3, 5]
Міжнародні видання: [2, 3].

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.	3/10
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 тестових завдань.	2/7-9
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.	1/4-6
Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.	0/0-3

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 8 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**	
8	**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.
6-7	**8-9**	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
3-5	**4-7**	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.
0-2	**0-3**	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 за результатами 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 національноюшкалою**	
			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 повторногоскладання	незадовільно	не зараховано
0-34	F	незадовільно з обов'язковим повторним вивченням курсу		

Результати складання диференційованого заліку вносяться у відомість обліку успішності здобувача вищої освіти, залікову книжку, індивідуальний навчальний план здобувача вищої освіти.

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

Засобами оцінювання та методами демонстрування результатів навчання під час вивчення курсу є:

- модульні контрольні роботи;
- стандартизовані тести;
- комп'ютерне тестування на платформі MOODLE;
- командні проекти;
- аналітичні звіти, реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- наукові статті та тези;
- виступи на всеукраїнських та міжнародних наукових заходах;
- інші види індивідуальних та групових завдань;
- екзамен.

6. ФОРМИ ТА ПИТАННЯ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Контрольний захід, для визначення підсумкових знань за перший модуль, проводиться у письмовому вигляді та може включати такі види завдань:

- Теоретичні питання;
- Тестові завдання;
- Завдання понятійного апарату.

Контрольний захід, для визначення підсумкових знань з навчальної дисципліни, проводиться у письмовому вигляді та може включати такі види завдань:

- Теоретичні питання;
- Тестові завдання;
- Ситуативні задачі.

ПЕРЕЛІК ПИТАНЬ ПОТОЧНОГО КОНТРОЛЮ

МОДУЛЬ 1

1. Поняття кіберзлочинності та її місце в загальній структурі злочинності.
2. Ознаки та види кіберзлочинності.
3. Поняття та система механізмів запобігання кіберзлочинності:.
4. Основні проблеми кваліфікації та протидії кіберзлочинності.
5. Мета, завдання та функції протидії кіберзлочинності.

6. Стратегія протидії кіберзлочинності в США.
7. Європейська система запобігання кіберзлочинності.
8. Поняття системи протидії кіберзлочинності в Україні.
9. Класифікація запобіжних заходів протидії кіберзлочинності.
10. Організація і управління процесом протидії кіберзлочинності в Україні.
11. Суб'єкти системи протидії та запобігання кіберзлочинності.
12. Об'єкти запобіжного впливу кіберзлочинів.
13. Види, на які поділяються суб'єкти та об'єкти системи протидії та запобігання кіберзлочинності
14. Загальна характеристика злочинця у сфері кібернетики.
15. Мотивація кіберзлочинців.
16. Інструменти та методи, що використовує правопорушник при скоєнні кіберзлочинів.
17. Попередження скоєння кіберзлочинцями правопорушення.
18. Класифікація технічних та інформаційних засобів вчинення кіберзлочинів.
19. Інформаційні технології, які найчастіше використовуються для вчинення кіберзлочинів.
20. Особливості кіберзлочинів, що вчиняються за допомогою технічних та інформаційних засобів.
21. Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами.
22. Шахрайство, що вчинене з використанням комп'ютерних технологій та інформаційно-комунікаційних систем.
23. Вплив штучного інтелекту на еволюцію кіберзлочинності.
24. Методичні основи розслідування кіберзлочинів.
25. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів.
26. Організаційно-тактичні основи розслідування кіберзлочинів.
27. Використання спеціальних знань під час розслідування кіберзлочинів.
28. Види узаконення доходів, що одержані у сфері кіберзлочинності.
29. Механізми узаконення злочинних доходів, одержаних у сфері кіберзлочинності та їх викриття.
30. Використання інформаційних систем для відмивання доходів, одержаних у сфері кібернетичної злочинності.
31. Попередження та запобігання легалізації доходів, одержаних у сфері кіберзлочинності.
32. Основні напрямки співпраці у боротьбі з кібернетичною злочинністю.
32. Кібервійна як міжнародний злочин.
33. Способи запобігання та уникнення кібервійн.
34. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів.
35. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.
36. Детермінанти та основні напрями запобігання кіберзлочинності.
37. Особливості криміналістичної характеристики кіберзлочинів.
38. Характеристика способів вчинення злочину.
39. Особливості етапів розслідування кіберзлочинів.
40. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види.
41. Способи збирання електронних доказів.
42. Способи забезпечення допустимості цифрових доказів.
43. Типові слідчі ситуації та завдання початкового та наступного етапів розслідування кіберзлочинів.
44. Характеристика тактичних операцій розслідування кіберзлочинів: їх послідовність, специфіка їх внутрішньої структури.
45. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин.
46. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.
47. Особливості розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування; особливості тактики окремих слідчих дій.
48. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.

МОДУЛЬ 2

1. Поняття особи кіберзлочинця.
2. Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця.
3. Типологія кіберзлочинців.
4. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології.
5. Соціальна інженерія, розкриття її сутності та ключових термінів у контексті кібербезпеки.
6. Розгляд інструментів та методів, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу до інформації.
7. Аналіз психологічних аспектів, які використовуються в соціальній інженерії для впливу на користувачів та підвищення їхньої вразливості до атак.
8. Оцінка важливості освіти користувачів у запобіганні соціальним атакам, а також розгляд технічних та організаційних контрзаходів для ефективного захисту від соціально-інженерних атак.
9. Аспекти кібербезпеки та основні принципи технічного захисту в умовах швидкого технологічного розвитку.
10. Аналіз сучасних тенденцій технологічного розвитку та їхнього впливу на кібербезпеку.
11. Методи та технічні рішення забезпечення безпеки в хмарних сервісах та мобільних пристроях.
12. Виклики та заходи безпеки, пов'язані зі зростанням кількості підключених до Інтернету пристроїв у різних сферах життя.
13. Роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.
14. Основні етапи генезису кіберзлочинності.
15. Характерні риси кіберзлочинності.
16. Яким чином кіберзлочинність впливає на міжнародне соціальне середовище?
17. Основні загрози кіберзлочинності для суспільної безпеки.
18. Які правові системи найбільше піддаються кіберзлочинним посяганням?
19. Класифікація комп'ютерних злочинців за віком та психофізіологічними особливостями.
20. Цілі та об'єкти правопорушень характерні для різних типів комп'ютерних злочинців.
21. Види злочинів у сфері використання сучасних інформаційних технологій найпоширеніші.
22. Міжнародна класифікація кіберзлочинів.
23. Які заходи можна застосувати для ефективної боротьби з кіберзлочинністю на міжнародному рівні?
24. Правові засади протидії кіберзлочинності існують в Україні.
25. Міжнародне законодавство в сфері протидії кіберзлочинності.
26. Організаційні засади протидії кіберзлочинності.
27. Основні проблеми у сфері протидії кіберзлочинності в Україні.
28. Напрямки удосконалення протидії кіберзлочинності можна виділити.
29. Яке значення має міжнародне співробітництво у сфері протидії кіберзлочинності?
30. Як відбувається координація між національними та міжнародними організаціями у боротьбі з кіберзлочинністю?
31. Ключові аспекти правових засад протидії кіберзлочинності в Україні можна виділити.
32. Які методи і стратегії використовуються в Україні для організаційної протидії кіберзлочинності?
33. Які міжнародні ініціативи та договори сприяють ефективній протидії кіберзлочинності?
34. Інформаційна безпека та її основні складові.
35. Яким чином інформаційна безпека впливає на загальну безпеку держави?
36. Основні напрямки інформаційної безпеки.
37. Правові методи здійснення інформаційної безпеки.
38. Технічні та програмні засоби захисту інформації.
39. Криптографічні методи захисту інформації і як вони застосовуються.
40. Охарактеризуйте еволюцію загроз інформаційній безпеці вплинула на сучасні системи захисту.
41. В чому полягає вплив має інтернет на розвиток шкідливих програм.
42. Основні методи шахрайства використовують зловмисники і як можна їм протидіяти.
43. Вкажіть основні класифікаційні ознаки сучасних кіберзагроз.
44. Класифікація кіберзагроз за їх характеристиками та методами атак.

45. Основні види кіберзагроз і які їх можливі наслідки для організацій та користувачів.
46. Методи соціально-інженерних атак використовуються сучасними кіберзлочинцями.
47. Технічні підходи здійснення атак через експлойти вразливостей.
48. Популярні вектори атак у сучасному кіберпросторі.
49. Як штучний інтелект і блокчейн можуть бути використані для створення складних кіберзагроз?
50. Новітні технології передбачення та запобігання кіберзагрозам.
51. Як можна проаналізувати та вивчити конкретні випадки сучасних кібератак для розробки ефективних стратегій захисту?
52. Основні принципи технічного захисту інформаційних систем в умовах швидкого технологічного розвитку.
53. Сучасні тенденції технологічного розвитку впливають на кібербезпеку.
54. Яким чином побудувати архітектуру іт-інфраструктури з урахуванням вимог до безпеки?
55. Методи технічного захисту інформаційних систем в хмарних.
56. Основні виклики та рішення для забезпечення безпеки мобільних пристроїв.
57. Поняття та ознаки кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних даних та систем
58. Поняття та ознаки незаконного доступу, незаконного перехоплення, втручання в дані, втручання в систему.
59. Характеристика складу кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних даних та систем.

ПЕРЕЛІК ПИТАНЬ ПІДСУМКОВОГО КОНТРОЛЮ

1. Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів.
2. Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.
3. Детермінанти та основні напрями запобігання кіберзлочинності.
4. Особливості криміналістичної характеристики кіберзлочинів.
5. Характеристика способів вчинення злочину.
6. Особливості етапів розслідування кіберзлочинів.
7. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види.
8. Способи збирання електронних доказів.
9. Способи забезпечення допустимості цифрових доказів.
10. Типові слідчі ситуації та завдання початкового та наступного етапів розслідування кіберзлочинів.
11. Характеристика тактичних операцій розслідування кіберзлочинів: їх послідовність, специфіка їх внутрішньої структури.
12. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин.
13. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.
14. Особливості розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування; особливості тактики окремих слідчих дій.
15. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.
16. Поняття особи кіберзлочинця.
17. Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця.
18. Типологія кіберзлочинців.
19. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології.
20. Соціальна інженерія, розкриття її сутності та ключових термінів у контексті кібербезпеки.
21. Розгляд інструментів та методів, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу до інформації.
22. Аналіз психологічних аспектів, які використовуються в соціальній інженерії для впливу на

користувачів та підвищення їхньої вразливості до атак.
23. Оцінка важливості освіти користувачів у запобіганні соціальним атакам, а також розгляд технічних та організаційних контрзаходів для ефективного захисту від соціально-інженерних атак.
24. Аспекти кібербезпеки та основні принципи технічного захисту в умовах швидкого технологічного розвитку.
25. Аналіз сучасних тенденцій технологічного розвитку та їхнього впливу на кібербезпеку.
26. Методи та технічні рішення забезпечення безпеки в хмарних сервісах та мобільних пристроях.
27. Виклики та заходи безпеки, пов'язані зі зростанням кількості підключених до Інтернету пристроїв у різних сферах життя.
28. Роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.
29. Основні етапи генезису кіберзлочинності.
30. Характерні риси кіберзлочинності.
31. Яким чином кіберзлочинність впливає на міжнародне соціальне середовище?
32. Основні загрози кіберзлочинності для суспільної безпеки.
33. Які правові системи найбільше піддаються кіберзлочинним посяганням?
34. Класифікація комп'ютерних злочинців за віком та психофізіологічними особливостями.
35. Цілі та об'єкти правопорушень характерні для різних типів комп'ютерних злочинців.
36. Види злочинів у сфері використання сучасних інформаційних технологій найпоширеніші.
37. Міжнародна класифікація кіберзлочинів.
38. Які заходи можна застосувати для ефективної боротьби з кіберзлочинністю на міжнародному рівні?
39. Правові засади протидії кіберзлочинності існують в Україні.
40. Міжнародне законодавство в сфері протидії кіберзлочинності.
41. Організаційні засади протидії кіберзлочинності.
42. Основні проблеми у сфері протидії кіберзлочинності в Україні.
43. Напрямки удосконалення протидії кіберзлочинності можна виділити.
44. Яке значення має міжнародне співробітництво у сфері протидії кіберзлочинності?
45. Як відбувається координація між національними та міжнародними організаціями у боротьбі з кіберзлочинністю?
46. Ключові аспекти правових засад протидії кіберзлочинності в Україні можна виділити.
47. Які методи і стратегії використовуються в Україні для організаційної протидії кіберзлочинності?
48. Які міжнародні ініціативи та договори сприяють ефективній протидії кіберзлочинності?
49. Інформаційна безпека та її основні складові.
50. Яким чином інформаційна безпека впливає на загальну безпеку держави?
51. Основні напрямки інформаційної безпеки.
52. Правові методи здійснення інформаційної безпеки.
53. Технічні та програмні засоби захисту інформації.
54. Криптографічні методи захисту інформації і як вони застосовуються.
55. Охарактеризуйте еволюцію загроз інформаційній безпеці вплинула на сучасні системи захисту.
56. В чому полягає вплив має інтернет на розвиток шкідливих програм.
57. Основні методи шахрайства використовують зловмисники і як можна їм протидіяти.
58. Вкажіть основні класифікаційні ознаки сучасних кіберзагроз.
59. Класифікація кіберзагроз за їх характеристиками та методами атак.
60. Основні види кіберзагроз і які їх можливі наслідки для організацій та користувачів.
61. Методи соціально-інженерних атак використовуються сучасними кіберзлочинцями.
62. Технічні підходи здійснення атак через експлойти вразливостей.
63. Популярні вектори атак у сучасному кіберпросторі.
64. Як штучний інтелект і блокчейн можуть бути використані для створення складних кіберзагроз?
65. Новітні технології передбачення та запобігання кіберзагрозам.
66. Як можна проаналізувати та вивчити конкретні випадки сучасних кібератак для розробки ефективних стратегій захисту?
67. Основні принципи технічного захисту інформаційних систем в умовах швидкого технологічного розвитку.
68. Сучасні тенденції технологічного розвитку впливають на кібербезпеку.

69. Яким чином побудувати архітектуру іт-інфраструктури з урахуванням вимог до безпеки?
70. Методи технічного захисту інформаційних систем в хмарних.
71. Основні виклики та рішення для забезпечення безпеки мобільних пристроїв.
72. Кіберзлочинність у сфері економіки.
73. Характеристика кіберзлочинів у сфері економіки.
74. Захист від кіберзлочинності об'єктів критичної інфраструктури.
75. Причини та умови кіберзлочинів у сфері економіки.
76. Запобігання кіберзлочинам у сфері економіки.
77. Особливості розслідування злочинів, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.
78. Особливості тактики окремих слідчих дій.
79. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.
80. Сутність та криміналістична класифікація кіберзлочинів, вчинених з антидержавно-політичних мотивів.
81. Особливості розслідування злочининів, що пов'язані з антидержавницькими діями у кіберпросторі: криміналістична характеристика, характеристика початкового етапу і програми (алгоритми) розслідування.
82. Характеристика програми розслідування злочинів, що пов'язані з антидержавницькими діями у кіберпросторі.
83. Особливості розслідування інцидентів кібертероризма.
84. Результати діяльності кіберполіції в Україні.
85. Кіберзагрози національній безпеці.
86. Кіберзагрози міжнародній безпеці.
87. Основні галузі права для регулювання відносин у кіберпростір в Україні: проблема міжгалузевих питань.
88. Перспективи розвитку проекту «Країна у смартфоні».
89. Перспективи правового регулювання криптовалюти в Україні.
90. Виявлення кіберзлочинів як напрямок правоохоронної діяльності. Типові джерела оперативної інформації про кіберзлочини.
91. Особливості перевірки інформації про кіберзлочини, що вчинені або готуються.
92. Відкриття кримінального провадження за заявою та повідомленням особи про кіберзлочин.
93. Організаційні заходи слідчого для перевірки отриманої первинної від заявника інформації.
94. Організаційні і тактичні особливості залучення спеціаліста для надання письмової та усної консультації підчас розслідування кіберзлочинів.
95. Залучення експерта під час розслідування кіберзлочинів для проведення судової комп'ютерно-технічної експертизи.
96. Залучення експерта для комплексних судових експертиз підчас розслідування кіберзлочинів (КТЕ та експертизи відео звукозапису; КТЕ і ТЕД).
97. Особливості призначення та проведення експертизи у сфері інтелектуальної власності. при розслідуванні кіберзлочинів.
98. Проведення психологічної експертизи при розслідуванні кіберзлочинів.
99. Типові тактичні операції розслідування кіберзлочинів та їх зв'язок із типовими слідчими ситуаціями, внутрішня структура кожної операції.
100. Особливості вилучення мобільних пристроїв.

7. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна:

1. Конституція України : Закон України від 28. 06. 1996 р. № 254к/96. Відомості Верховної Ради України. 1996. № 30. Ст. 141.
2. Кримінальний кодекс України: Закон України від 05.04.2001 р. № 2341-III.
3. Відомості Верховної Ради України. 2001. № 25-26. Ст.131.

4. Ковальський В. С., Семаков Г. С., Костенко О. М. Кримінологія: підручник. Київ: Юрінком, 2019. 344 с.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради.* 2017 № 45. URL: http://surl.li/crgcgy.
6. Кримінологія: підручник. А. М. Бабенко, О. Ю. Бусол, О. М. Костенко та ін.; за заг.ред. Ю. В. Нікітіна, С. Ф. Денисова, Є.Л. Стрельцова.- 2-ге вид., перероб. Та допов. Харків: Право, 2021. 416 с.
7. Кримінологія: академічний підручник. [Богатирьов І. Г., Колб О. Г., Топчій В. В. та ін.]; за заг.ред. доктора юридичних наук, професора, заслуженого діяча науки і техніки України Богатирьова І. Г. Чернівці: Технодрук, 2020. 336 с.
8. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. С 372.
9. Аленін Ю. П., Аркуша Л. І. Кримінальний процес: навч. посібник. Одеса: Фенікс, 2020. С. 582.
10. Кримінальний процес: підручник / за заг. ред. Д. П. Письменного, Л. Д. Удалової, М. А. Погорецького, С. С. Чернявського. Київ: «Центр учбової літератури», 2022. С. 780

Допоміжна:

1. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. рекомендації. [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.]; за заг. ред. О. В. Корнейка. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.
2. Тимошенко В. І., Шакун В. І. Теоретичні основи кримінології: монографія. Київ: Юрінком Інтер, 2021. 240 с.
3. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України" Указ Президента України від 15.03.2016 № 96/2016. Дата оновлення: 15.03.2016 URL: http://zakon2.rada.gov.ua/laws/show/96/2016
4. Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Національного банку України від 28.09.2017 №95. URL: //zakon2.rada.gov.ua/laws/show/v0095500-17
5. Про внесення змін до деяких законодавчих актів України щодо посилення захисту права дитини на належне утримання шляхом вдосконалення порядку стягнення аліментів: Закон України від 17.05.2017 № 2037-VIII. *Відомості Верховної Ради*. 2017. №25. Ст. 291.
6. Дідківська Г. В. Сімейне неблагополуччя в системі детермінантів злочинності неповнолітніх в Україні: монографія. Вінниця: Нілан ЛТД, 2019. 220 с.
7. Ільїна О. В. Співвідношення кримінально-правової політики з кримінально-виконавчою політикою. Актуальні проблеми вітчизняної юриспруденції. № 3. Дніпро. 2022. С. 98-104.
8. Лантінов Я. О. Щодо конкуренції між термінами "кримінально-правова політика" та "політика протидії злочинності". Форум Права. № 2 (73). Харків. 2022. С. 22-28.
9. Лащук Є. В. Поняття принципів кримінально-правової політики та їх співвідношення з принципами кримінального права. Вісник Південного регіонального центру Національної академії правових наук України № 20. Одеса. 2019. С. 160-171.
10. Кримінальне право УЄ і будівництво загальноєвропейського правового простору: монографія. за заг. ред. Ю. О. Костенка. Харків: Право, 2019.
11. Дідківська Г. В. Олійник Н. Л. Порівняльна характеристика національного та міжнародного кримінального законодавства у сфері регулювання фіктивного підприємництва. Ірпінський юридичний часопис: науковий журнал (Серія: право). 2019. Випуск 2. С. 137–144.
12. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.
13. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. В. Лисодєда ін.; за заг. ред. Б. М. Головкіна. Харків : Право, 2020. 384 с. (Розділ 12).
14. Філіппов С. О. Протидія транскордонній злочинності: глобальний контекст і реалії України: монографія. Одеса: Фенікс, 2019. 452 с.

Інформаційні ресурси Інтернет:

1. Офіційний сайт Верховного Суду України. URL: www.scourt.gov.ua
2. Офіційний сайт Вищого спеціалізованого суду України з розгляду цивільних і

кримінальних справ. URL: www.sc.gov.ua
3. Законодавство України. URL: zakon4.rada.gov.ua/laws/main
4. Офіційний сайт Міністерства юстиції України. URL: www.minjust.gov.ua
5. Національна бібліотека України ім. В.І. Вернадського. URL: www.nbuv.gov.ua
6. Єдиний державний реєстр судових рішень. URL: reyestr.court.gov.ua

Міжнародні видання:

1. Internet Organised Crime Threat Assessment (IOCTA), Europol, 2021. URL : https://www.europol.europa.eu
2. Hong Y., Neilson W. Cybercrime and Punishment. The Journal of legal studies. 2020. Vol. 49 (2). P. 431–466.
3. Galyna Didkivska, Serhiy Miroshnychenko, Iryna Zavydniak, Inna Biriukova Andrii, Hmyrin Dmitry, Lopashchuk. International Cooperation in Investigating Economic Crimes of Transnational Nature. Derecho Publico: Cuestions Politicas. Vol. 40 Num. 72 (2022).

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