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
«Аналіз та прогнозування 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

галузь знань 25 «Воєнні науки, національна безпека, безпека державного кордону»
спеціальність 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»
освітньо-професійна програма «Національна фінансова безпека»
Статус дисципліни: обов'язкова

Ірпінь – 2024

Робоча програма навчальної дисципліни «Аналіз та прогнозування 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; спеціальності 256 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» освітньо-професійна програма «Національна фінансова безпека», затвердженої Вченою радою Університету «29» 08 2024 року, протокол № 1.

Укладачі: Г. Дідківська, д.ю.н., професор

Д. Лопащук, к.ю.н.

Гарант ОПП «Правове забезпечення протидії кіберзлочинності» Г. Дідківська

Гарант ОПП «Національна фінансова безпека» О. Боднарчук

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 «Аналіз та прогнозування кіберзлочинності» є надання здобувачам вищої освіти поглиблених знань щодо правових основ, сутності та особливостей запобіжної діяльності правоохоронних органів зокрема у сфері протидії кіберзлочинності, формування у здобувачів умінь та навичок здійснення аналізу криміногенної обстановки в окремому регіоні, місті, районі, складання профілактичних документів та реалізації системи запобіжних заходів окремим видам кіберзлочинності у практичній діяльності органів поліції. При цьому здобувачі повинні з'ясувати: яким чином і в якому обсязі кожен з правоохоронних органів здійснюють запобігання кіберзлочинності в цілому та окремих її видів.

Завданнями навчальної дисципліни «Аналіз та прогнозування кіберзлочинності» є формування у здобувачів вищої освіти поглиблених знань та уявлень про сучасний стан законодавства в Україні щодо протидії кіберзлочинності ; засвоєння методів сучасної кримінологічної науки в частині самостійного аналізу та прогнозування кіберзлочинності; вивчення здобувачами вищої освіти генезису виникнення кримінального законодавства та його розвитку; предмету, методології та місця актуальних питань щодо аналізу та прогнозування кіберзлочинності; оволодіння системою напрацьованих в кримінології спеціальних категорій та понять, які в цілому складають змістовий об'єм цієї навчальної дисципліни; поняття та зміст аналізу та прогнозування кіберзлочинності; отримання поглиблених знань про кіберзлочинність та сучасну теорію її запобігання шляхом удосконалення законодавства; відпрацювання навичок та умінь аналізу, діагностики та прогнозу етапів формування кіберзлочинності під час семінарських та практичних занять.

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 «Аналіз та прогнозування 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 – диференційований залік.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Код академічної групи ПМПД 24-1, 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.
	Практичні заняття	
	18 год.	4 год.
	Самостійна робота	
	78 год.	110 год.
	Індивід.-консультац. робота: 2 год.	
	Форма семестрового контролю: диференційований залік	

Код академічної групи ПМНБЗ 24-1

Показники	**Характеристика навчальної дисципліни**
	Заочна форма навчання
Кількість кредитів ЄКТС - 4	4
Модулів - 2	Рік підготовки:
Змістових модулів - 2	1-й
Загальна кількість годин - 120 годин	Семестр
	2-й
	Лекції
	4 год.
	Семінарські заняття
	4 год.
	Самостійна робота
	110 год.
	Індивід.- консультац. робота: 2 год.
	Форма семестрового контролю: диференційований залік

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.	РН2. Координувати діяльність суб'єктів забезпечення публічної безпеки і порядку, а також здійснювати взаємодію. РН4. Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових,

СК2. Здатність забезпечувати законність та правопорядок, безпеку особистості, суспільства, держави в межах виконання своїх посадових обов'язків. СК5. Здатність давати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності. ФК4. Здатність взаємодіяти з представниками міжнародних правоохоронних організацій у сфері протидії кіберзлочинності. ФК5. Здатність застосовувати спеціальні прийоми та засоби правоохоронної діяльності, а також інформаційні, кадрові та інші види ресурсів в професійній діяльності з урахуванням вітчизняного та зарубіжного досвіду з метою запобігання та протидії кіберзлочинності.	соціальних, економічних та етичних аспектів. РН5. Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення. РН12. Надавати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності РН13. Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію. РН15. Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку. РН16. Використовувати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань РН20. Застосовувати заходи, спрямовані на запобігання та протидію кіберзлочинам. РН22. Здійснювати заходи з виявлення, припинення та розслідування кіберзлочинів, проводити дії та заходи спрямовані на збір доказів та фіксацію фактичних даних про протиправну діяльність. РН23. Застосовувати методи кримінального аналізу та знання з сучасних інформаційних технологій під час вирішення професійних завдань правоохоронної діяльності.

ОП «Національна фінансова безпека»

Компетентності	**Результати навчання**
ІК. Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у галузі національної безпеки (за окремими сферами забезпечення і видами діяльності). СК1. Здатність здійснювати професійну діяльність у відповідних сферах національної безпеки. СК3. Здатність використовувати понятійно-категоріальний апарат теорії національної безпеки, аналізувати та розвивати структуру системи забезпечення національної безпеки та принципи її функціонування. СК4. Здатність аналізувати та прогнозувати розвиток безпекового середовища (глобальний, регіональний та національний аспекти) за окремими сферами забезпечення та видами діяльності. СК7. Здатність інтегрувати знання та розв'язувати складні задачі національної безпеки (за окремими сферами забезпечення і видами діяльності) у широких та/або мультидисциплінарних контекстах за наявності неповної або обмеженої інформації з	РН3. Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (за сферами забезпечення та видами діяльності), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог. РН7. Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища РН11. Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності РН12. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки і є основою для прийняття ефективних рішень, проведення досліджень та критичного осмислення проблем у галузі національної безпеки. РН17. Організовувати заходи з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів, а також аналізувати міжнародний механізм в

урахуванням аспектів соціальної та етичної відповідальності. ФК3. Здатність до аналізу міжнародного механізму в частині забезпечення процедур розшуку та арешту активів, а також управління арештованим майном, що одержане незаконним шляхом. ФК4. Здатність до забезпечення національних інтересів держави у кіберпросторі.	частині забезпечення процедур розшуку та арешту активів РН18. Забезпечення національних інтересів держави у кіберпросторі.

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».

Пререквізитами ОП «Національна фінансова безпека» є навчальні дисципліни: «Державне управління у сфері національної безпеки», «Державний розвиток в умовах загроз національній безпеці».

Постреквізитами ОП «Правове забезпечення протидії кіберзлочинності» є навчальні дисципліни: «Організована транснаціональна кіберзлочинність», «Міжнародні стандарти правоохоронної діяльності».

Постреквізитами ОП «Національна фінансова безпека» є навчальні дисципліни: «Інформаційна безпека держави», «Стратегічне планування та впровадження інновацій у фінансовій безпеці», «Попередження та боротьба з корупцією у сфері фінансової безпеки».

2.3.СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

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

№ п/п	Змістові модулі	Кількість годин				
		Лекції(год.)	Практичні (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	Кіберзлочинність: поняття, види та її запобігання.	2	2	-	8	12
Т.2	Особливості методики розслідування кіберзлочинів.	2	2	-	8	12
Т.3	Електронні докази у кримінальному провадженні.	2	2	-	8	12
Т.4	Організаційно-тактичні основи розслідування кіберзлочинів.	2	2	-	8	12
Т.5	Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов’язані з фінансово економічною сферою відносин у кіберпросторі.	2	2	-	8	12
Всього по модулю 1:		10	10	0	40	60
Форма контролю: модульна контрольна робота (за рахунок практичного заняття – 40 хв.)						
МОДУЛЬ ІІ – 2 кредити (60 годин)						
ЗМ 2 (Теми 6-9)						
Т.6	Особа кіберзлочинця.	4	2	-	9	15

Т.7	Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	4	2	-	9	15
Т.8	Соціальна інженерія та кібербезпека користувачів.	2	2	2	10	16
Т.9	Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку.	2	2	-	10	14
Всього по модулю 2:		12	8	2	38	60
Форма контролю: модульна контрольна робота (за рахунок практичного заняття – 40 хв.)						
Форма підсумкового контролю – диференційований залік (ПМК).						
Усього за навчальною дисципліною:		22	18	2	78	120

Код академічної групи ПМПДЗ 24-1

№ п/п	**Змістові модулі**	**Кількість годин**				
		Лекції (год.)	**Практичні (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	Кіберзлочинність: поняття, види та її запобігання.	2	-	-	10	12
Т.2	Особливості методики розслідування кіберзлочинів.	-	2	-	12	14
Т.3	Електронні докази у кримінальному провадженні.	-	-	-	10	10
Т.4	Організаційно-тактичні основи розслідування кіберзлочинів.	-	-	-	12	12
Т.5	Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово економічною сферою відносин у кіберпросторі.	-	-	-	12	12
Всього по модулю 1:		2	2	0	56	60
МОДУЛЬ ІІ – 2 кредити (60 годин)						
ЗМ 2 (Теми 6-9)						
Т.6	Особа кіберзлочинця.	-	-	-	14	14
Т.7	Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	2	2	-	14	18
Т.8	Соціальна інженерія та кібербезпека користувачів.	-	-	2	12	14
Т.9	Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку.	-	-	-	14	14
Всього по модулю 2:		2	2	2	54	60
Форма контролю: аудиторна контрольна робота (за рахунок практичного заняття – 40 хв.)						

Форма підсумкового контролю – диференційований залік (ПМК).					
Усього за навчальною дисципліною:	4	4	2	110	120

Код академічної групи ПМНБЗ 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	Кіберзлочинність: поняття, види та її запобігання.	2	-	-	10	12
Т.2	Особливості методики розслідування кіберзлочинів.	-	2	-	12	14
Т.3	Електронні докази у кримінальному провадженні.	-	-	-	10	10
Т.4	Організаційно-тактичні основи розслідування кіберзлочинів.	-	-	-	12	12
Т.5	Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово економічною сферою відносин у кіберпросторі.	-	-	-	12	12
Всього по модулю 1:		2	2	0	56	60
МОДУЛЬ ІІ – 2 кредити (60 годин)						
ЗМ 2 (Теми 6-9)						
Т.6	Особа кіберзлочинця.	-	-	-	14	14
Т.7	Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	2	2	-	14	16
Т.8	Соціальна інженерія та кібербезпека користувачів.	-	-	2	12	14
Т.9	Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку.	-	-	-	14	14
Всього по модулю 2:		2	2	2	54	60
Форма контролю: аудиторна контрольна робота (за рахунок семінарського заняття – 40 хв.)						
Форма підсумкового контролю – диференційований залік (ПМК).						
Усього за навчальною дисципліною:		4	4	2	110	120

РЕЙТИНГ-ПЛАН
Денна форма навчання

Години	Тема	Форма заняття	Результати навчання	Вага оцінки
Модуль І, ІІ				
2	Т. 1. Кіберзлочинність: поняття, види та її запобігання.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.1. Кіберзлочинність: поняття, види та її запобігання.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
2	Т.2. Особливості методики розслідування кіберзлочинів.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.2. Особливості методики розслідування кіберзлочинів.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
2	Т.3. Електронні докази у кримінальному провадженні.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.3. Електронні докази у кримінальному провадженні.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
2	Т.4. Організаційно-тактичні основи розслідування кіберзлочинів.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.4. Організаційно-тактичні основи розслідування кіберзлочинів.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
2	Т.5. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов’язані з фінансово економічною сферою відносин у кіберпросторі.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.5. Розслідування кіберзлочинів, вчинених	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16,	3

	з корисливих мотивів, що пов'язані з фінансово економічною сферою відносин у кіберпросторі.		РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	
	Т 1-5	Проміжний модульний контроль		5
	Усього за Модулем І			**20**
4	Т.6. Особа кіберзлочинця.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.6. Особа кіберзлочинця.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
4	Т.7. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.7. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
2	Т.8. Соціальна інженерія та кібербезпека користувачів.	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.8. Соціальна інженерія та кібербезпека користувачів.	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
2	Т.9. Кібербезпека та основні принципи технічного захисту в умовах постійного	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23	0

	технологічного розвитку.		ОП2: РН3, РН7, РН11, РН12, РН17, РН18	
2	Т.9. Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку	Практичне заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	3
	Т 6-9	Проміжний модульний контроль		5
	Індивідуальна робота	Тема 8		8
	Комп'ютерне тестування на платформі дистанційного навчання			5
	Усього за Модулем ІІ			**30**
	Диференційований залік (ПМК)			**50**
	Усього за курсом			**100**

*ОП1 – «Правове забезпечення протидії кіберзлочинності»
ОП2 – «Національна фінансова безпека»

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

Години	**Тема**	**Форма заняття**	**Результати навчання**	**Вага оцінки**
Модуль І, ІІ				
2	Т.1. Кіберзлочинність: поняття, види та її запобігання	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	0
2	Т.2. Особливості методики розслідування кіберзлочинів	Практичне заняття/ семінарське заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	10
	Усього за Модулем І			10
2	Т.7. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему	Лекція	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	
2	Т.7. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему	Практичне заняття/ семінарське заняття	*ОП1: РН2, РН4, РН5, РН12, РН13, РН15, РН16, РН20, РН22, РН23 ОП2: РН3, РН7, РН11, РН12, РН17, РН18	10

	Модульна контрольна робота	Аудиторна контрольна робота		15
	Усього за Модулем ІІ			
2	Індивідуально-консультаційна робота	Тема 8		10
	Комп'ютерне тестування на платформі дистанційного навчання			5
	Усього за Модулем І, ІІ			**50**
	Диференційований залік			**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, 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. Кіберзлочинність: поняття, види та її запобігання.

План лекційного заняття

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.

План практичного заняття

КЕЙС 1. Винний в Інтернеті знайшов програмне забезпечення, що призначене для віддаленого керування доступом до персонального комп'ютера, і завантажив його на свій комп'ютер. Потім за допомогою цього програмного забезпечення створив вірусне програмне забезпечення, що дозволяло у разі його завантаження отримати віддалений доступ до іншого комп'ютера та керування ним. Після чого він виклав це вірусне програмне забезпечення як додаток до інтернет-ігор у вигляді архівного файлу на одному із сайтів, який створив. У подальшому цей файл з вірусним програмним забезпеченням завантажив один із користувачів мережі Інтернет.

КЕЙС 2. Винний, за допомогою розрізаної двохсотгривневої купюри, нитки та клейкої стрічки, виготовив спеціальний пристрій, за допомогою якого він однією і тією ж купюрою неодноразово через термінал онлайн платежів поповнював свій мобільний рахунок. Отримані в такий спосіб кошти він перераховував на електронні гаманці й банківські картки, а потім знімав з них готівку. У такий спосіб винний вчинив 50 кримінальних правопорушень і заподіяв матеріальну шкоду на суму 50 тисяч гривень.

Самостійна робота здобувачів вищої освіти

1. Недоліки законодавчого визначення кіберзлочину в Україні.
2. Заходи міжнародного співробітництва у сфері боротьби з кіберзлочинністю.

Питання для самоконтролю

1. Назвіть існуючі у кримінології підходи до визначення поняття злочинність.
2. Який з вітчизняних кримінологічних підходів до визначення кіберзлочинності є найбільш

поширеним і чому?
3. Якими термінами позначають явище «кіберзлочинність»? Як співвідносяться ці терміни?
4. Назвіть підходи до того, в чому полягає кримінологічна однорідність кіберзлочинів. Який із них найбільш обґрунтований, на Вашу думку, і чому?
5. Які групи кіберзлочинів можна виділити за значенням інформаційної системи у механізмі реалізації кримінально протиправної діяльності?
6. Які напрями запобігання кіберзлочинності Ви знаєте?
7. Чим відрізняється профілактика кіберзлочинів від заходів забезпечення кіберстійкості інформаційної інфраструктури до впливу кіберзлочинності?
Рекомендована література
Основна: [2, 5, 6, 7]
Допоміжна: [8, 10, 11]
Інформаційні ресурси Інтернет: [1, 3, 4]
Міжнародні видання: [1, 3].

Тема 2. Особливості методики розслідування кіберзлочинів.

План лекційного заняття

1. Особливості криміналістичної характеристики кіберзлочинів.
2. Характеристика способів вчинення злочину.
3. Особливості етапів розслідування кіберзлочинів.

План семінарського заняття

1. Особливості криміналістичної характеристики кіберзлочинів.
2. Характеристика способів вчинення злочину.
3. Особливості етапів розслідування кіберзлочинів.
4. Охарактеризуйте організаційні форми початку кримінального провадження щодо кіберзлочинів.
5.Співвіднесіть способи вчинення кіберзлочинів з найбільш поширеними способами їх приховування.

План практичного заняття

КЕЙС 1. В описаній фабулі наявне несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Його предметом є відповідне коло інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а знаряддям виступатимуть комп'ютерна техніка підозрюваних, з якої здійснювалося несанкціоноване втручання (до прикладу, апаратно-програмні комплекси, які забезпечували функціонування ботоферми; сім-карти, що використовувалися для створення та подальшого ведення технічних акаунтів; «Proxy»-сервери для підміни IP-адрес та уникнення блокування відповідних інтернет-ресурсів).
КЕЙС 2. В описаній фабулі наявне створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Його предметом є відповідне коло інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а знаряддям виступатиме комп'ютерна техніка підозрюваного з адмін-панеллю доступу до заражених комп'ютерів шкідливим програмним забезпеченням, його інсталяційні файли.

Самостійна робота здобувачів вищої освіти

1. Окресліть чинники, що зумовлюють форми початку кримінального провадження.
2. Охарактеризуйте процес виявлення кіберзлочинів заявником (як користувачем).

Питання для самоконтролю

1. Назвіть суб'єктів оперативно-розшукової діяльності, котрі прямо або опосередковано здійснюють виявлення кіберзлочинів?
2. Назвіть типові джерела оперативної інформації про кіберзлочини?
3. Чому євроінтеграція кримінального законодавства України є необхідністю?

3. Чи належать місце та час вчинення кіберзлочинів до елементів криміналістичної характеристики кіберзлочинів? Чи мають вони значення для розслідування?
4. Які кримінологічні особливості особи кіберзлочинця та потерпілого (жертви) кіберзлочину?
5. Яке значення для розслідування кіберзлочинів відіграють логфайли та метадані?
6. Які можна виокремити способи запобігання кіберзлочинам?

Рекомендована література

Основні: [1, 3, 4, 6, 7]
Допоміжна: [8, 10, 11]
Інформаційні ресурси в Інтернеті: [1, 3, 4]
Міжнародні видання: [1, 3]

Тема 3. Електронні докази у кримінальному провадженні.

План лекційного заняття

1. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види.
2. Способи збирання електронних доказів.
3. Способи забезпечення допустимості цифрових доказів.

План практичного заняття

1. Поняття цифрового доказу.
2. Призначення та проведення комп'ютерно-технічної експертизи.
3. Отримання електронних доказів від учасників кримінального провадження.
4. Проаналізуйте наведену ситуацію та встановіть правильність дій слідчого під час проведення огляду.

КЕЙС 1. Під час огляду ЕОМ слідчим було виявлено дані, які можуть бути використані під час доказування у кримінальному провадженні як докази, зокрема файли із кресленнями щодо виготовлення вибухових речовин. Виявивши вказані дані, слідчий скопіював їх на власний флеш-носій, що відзначив у протоколі огляду.

Самостійна робота здобувачів вищої освіти

1. Причини наявності труднощів у використанні цифрової інформації у доказуванні.
2. Процедура фіксації цифрової інформації та забезпечення її доказового значення.
3. Практика ВС щодо використання електронного документа як доказу.

Питання для самоконтролю

1. Якими унікальними особливостями характеризується інформація, створена за допомогою високих інформаційних технологій?
2. На яких рівнях функціонує інформація в ЕОМ?
3. Які особливості перевірки цифрового алібі?
4. Яким умовам повинна відповідати виявлена помилка програмного забезпечення?
5. Які основні методи фіксації інформації з веб-сайту?
6. Розмежуйте поняття електронного доказу та його носія.
7. Чи є поняття електронного документа та електронного доказу тотожними?

Рекомендована література

Основна: [3, 4, 5, 6]
Допоміжна: [7, 9,10, 15]
Інформаційні ресурси в Інтернеті: [2, 3, 4, 6]
Міжнародні видання:[1, 3]

Тема 4. Організаційно-тактичні основи розслідування кіберзлочинів.

План лекційного заняття

1. Типові слідчі ситуації та завдання початкового та наступного етапів розслідування кіберзлочинів.
2. Характеристика тактичних операцій розслідування кіберзлочинів: їх послідовність, специфіка їх внутрішньої структури.
3. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин.

План практичного заняття

1. Основні завдання початкового етапу розслідування кіберзлочинів.

2. Тактична операція «Персоналізація відомостей про особу/осіб злочинця/ів».
3. Тактична операція «Збирання електронних (цифрових) носіїв інформації».
4. Тактична операція «Встановлення кінцевого мотиву злочинної діяльності в кіберпросторі».
5. Тактична операція «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи».
6. Тактична операція «Встановлення технології злочинної діяльності з використанням кіберпростору».
7. Тактична операція «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі».
8. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин.

Самостійна робота здобувачів вищої освіти

1. Обрати, керуючись рішенням і умовами конкретної слідчої ситуації (яку необхідно охарактеризувати), що випливає зі змісту задачі, програму дій слідчого, скласти план розслідування. Визначити також необхідність проведення тактичної операції одразу після внесення інформації в ЄРДР. Визначте діяльність щодо її організації та проведення.

а) блок інформації: В ході перевірки оперативної інформації було встановлено, що невстановлені особи несанкціоновано втручалися в роботу комп'ютерів юридичних осіб, на яких було встановлено програмне забезпечення дистанційного доступу до рахунків, відкритих у банківських установах (система «Клієнт-Банк»). Отримавши доступ до інформації, яка на них зберігається й обробляється, злочинці здійснювали перерахування коштів загальною сумою 357 303,44 грн на рахунок фіктивно створеного підприємства.

б) блок інформації: У ході слідства в результаті контролю за вчиненням злочину було встановлено лише особу, на яку було відкрито з її відома фіктивне підприємство з метою переведення коштів у готівкову форму.

Питання для самоконтролю

1. Назвіть типові тактичні операції розслідування кіберзлочинів, охарактеризуйте їх послідовність та їх внутрішню структуру.
2. Які можна назвати тактичні рекомендації щодо підготовки до СРД, спрямованої на збирання інформації в електронному вигляді.
3. Наведіть алгоритм дій під час огляду локального комп'ютерного засобу з метою збирання інформації в електронному вигляді.
4. Навіщо додавати до протоколу слідчої дії робочий та контрольний примірник усіх програмних засобів, а також даних, що вміщують доказову інформацію?
5. Які дії потрібно провести з мобільним пристроєм під час його вилучання, якщо його екран заблоковано?

Рекомендована література

Основна: [2, 3, 4]

Допоміжна: [7, 9,10, 15]

Міжнародні видання: [1, 2, 3]

Інформаційні ресурси в Інтернеті: [1, 2, 3, 5, 6]

Тема 5. Розслідування кіберзлочинів, вчинених з корисливих мотивів, що пов'язані з фінансово економічною сферою відносин у кіберпросторі.

План лекційного заняття

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.
2.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.
3. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.

План практичного заняття

1. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.

2.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.
3. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.

Самостійна робота здобувачів вищої освіти

1. Обрати, керуючись рішенням і умовами конкретної слідчої ситуації (яку необхідно охарактеризувати), що випливає зі змісту задачі, програму дій слідчого, скласти план розслідування. Визначити також необхідність проведення тактичної операції одразу після внесення інформації в ЄРДР. Визначте діяльність щодо її організації та проведення.
1 блок інформації: До підрозділу ДКП НП України надійшло електронне повідомлення про кримінальне правопорушення (як звернення до органу поліції) від гр. О., який повідомляв про те, що 23 жовтня о 01:04 годині, користуючись можливостями сервісної служби «Арбітраж WebMoney» він отримав sms-повідомлення про нібито переказ ним грошових коштів зі свого електронного гаманця коштів в сумі 1 тис. грн. на інший додатковий гаманець. О. встиг накласти на переказ «арешт», що унеможливило їх відчуження невстановленій йому особі.
2 блок інформації: В ході перевірки інформації співробітниками ДКП було встановлено що гр. К., який мешкає у м. Черкаси, 23 жовтня о 00:59 годині, реалізуючи свій злочинний умисел, направлений на несанкціоноване втручання в роботу комп'ютера гр. О., діючи умисно, за місцем своєї реєстрації та проживання, використовуючи свій комп'ютер, через мережу Інтернет, за допомогою паролю, який він незаконно отримав внаслідок роботи розповсюдженого ним в мережі програмного засобу, здійснив несанкціоноване проникнення до електронної поштової скриньки гр. О. в результаті чого отримав доступ до відомостей про електронний гаманець гр.О. та його особисту переписку. З метою таємного викрадення, належних О. грошових коштів К. створив в електронній грошовій системі додатковий електронний гаманець, зареєстрував його на своїй електронній поштовій скринці, після чого, використовуючи свій комп'ютер, через мережу Інтернет здійснив без відома О., незаконний переказ грошових коштів з електронного гаманця О. на свій додатковий електронний гаманець. При цьому він, використовуючи свій комп'ютер, розповсюдив шкідливий програмний засіб, що призначений для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації, шляхом прихованого перехоплення натискань клавіш на клавіатурі, моніторингу буферу обміну, запису знімків екрану монітору (скріншотів), моніторингу відвідуваних веб-сайтів з послідуючим відправленням такої інформації на конкретну електронну скриньку. К. налаштував його таким чином, щоб за його допомогою можна було здійснити несанкціоноване втручання в роботу комп'ютерів інших користувачів мережі «Інтернет». Вказаний програмний засіб шляхом розміщення в мережі Інтернет під виглядом комп'ютерної програми для викрадення ігрових грошей в онлайн грі «FG» на спеціально створеному інтернет-сайті домену «.ua».

Питання для самоконтролю

1. В чому полягає сутність та криміналістична класифікація кіберзлочинів, вчинюваних з корисливих мотивів у фінансово-економічній сфері ?
2. Які існують основні способи вчинення кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків?
3. Чим характеризується предмет посягання кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків?
4. Які існують типи злочинців, що вчиняють кіберзлочини, що спрямовані на заволодіння чужим майном?
5. Охарактеризуйте програму розслідування кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків.

Рекомендована література

Основна: [2, 3, 4, 5]
Допоміжна: [8, 10, 11, 14]
Інформаційні ресурси в Інтернеті: [1, 3,5]
Міжнародні видання: [2, 3]

Модуль ІІ.

Змістовий модуль 2.

Тема 6. Особа кіберзлочинця.

План лекційного заняття

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.

План практичного заняття

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.

Самостійна робота здобувачів вищої освіти

1. Розкрийте поняття «особа кіберзлочинця». Аргументуйте свою відповідь.
2. Які типології кіберзлочинців Ви знаєте? За якими критеріями визначаються типології кіберзлочинців? Яке практичне значення має типологія кіберзлочинців?

Питання для самоконтролю

1. В чому полягає сутність та криміналістична класифікація кіберзлочинів, вчинюваних з корисливих мотивів у фінансово-економічній сфері ?
2. Які існують основні способи вчинення кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків?
3. Чим характеризується предмет посягання кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків?
4. Які існують типи злочинців, що вчиняють кіберзлочини, що спрямовані на заволодіння чужим майном?
5. Охарактеризуйте програму розслідування кіберзлочинів, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочинів у сфері функціонування електронних розрахунків.

Рекомендована література

Основна: [2, 3, 5]

Допоміжна: [8, 10, 11]

Інформаційні ресурси в Інтернеті: [1, 3, 5]

Міжнародні видання: [1, 2]

Тема 7. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

План лекційного заняття

1. Поняття та ознаки кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних даних та систем
2. Поняття та ознаки незаконного доступу, незаконного перехоплення, втручання в дані, втручання в систему.
3. Характеристика складу кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних даних та систем.

План семінарського заняття

1. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
2. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний

доступ, незаконне перехоплення, втручання в дані, втручання в систему.
3. Причини та умови злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
4. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

План практичного заняття

КЕЙС 1. В описаній фабулі наявне несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Його предметом є відповідне коло інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а знаряддям виступатимуть комп'ютерна техніка підозрюваних, з якої здійснювалося несанкціоноване втручання (до прикладу, апаратно-програмні комплекси, які забезпечували функціонування ботоферми; сім-карти, що використовувалися для створення та подальшого ведення технічних акаунтів; «Proxy»-сервери для підміни IP-адрес та уникнення блокування відповідних інтернет-ресурсів).
КЕЙС 2. В описаній фабулі наявне створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Його предметом є відповідне коло інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, а знаряддям виступатиме комп'ютерна техніка підозрюваного з адмін-панеллю доступу до заражених комп'ютерів шкідливим програмним забезпеченням, його інсталяційні файли.

Самостійна робота здобувачів вищої освіти

1. Аналіз правових та інституційних основ протидії кіберзлочинності в Україні.
2. Кібернетична складова агресії росії проти України: кваліфікація за міжнародним правом.

Питання для самоконтролю

1. Назвіть існуючі у кримінології підходи до визначення поняття злочинність.
2. Який з вітчизняних кримінологічних підходів до визначення кіберзлочинності є найбільш поширеним і чому?
3. Якими термінами позначають явище «кіберзлочинність»? Як співвідносяться ці терміни?
4. Назвіть підходи до того, в чому полягає кримінологічна однорідність кіберзлочинів. Який із них найбільш обґрунтований, на Вашу думку, і чому?
5. Які групи кіберзлочинів можна виділити за значенням інформаційної системи у механізмі реалізації кримінально протиправної діяльності?
6. Які напрями запобігання кіберзлочинності Ви знаєте?
7. Чим відрізняється профілактика кіберзлочинів від заходів забезпечення кіберстійкості інформаційної інфраструктури до впливу кіберзлочинності?

Рекомендована література
Основна: [2, 3, 5]
Допоміжна: [8, 10, 11]
Інформаційні ресурси в Інтернеті: [1, 3, 5]
Міжнародні видання: [1, 2, 3]

Тема 8. Соціальна інженерія та кібербезпека користувачів.

План лекційного заняття

1. Соціальна інженерія, розкриття її сутності та ключових термінів у контексті кібербезпеки.
2. Розгляд інструментів та методів, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу до інформації.
3. Аналіз психологічних аспектів, які використовуються в соціальній інженерії для впливу на користувачів та підвищення їхньої вразливості до атак.

4. Оцінка важливості освіти користувачів у запобіганні соціальним атакам, а також розгляд технічних та організаційних контрзаходів для ефективного захисту від соціально-інженерних атак.

План практичного заняття

1. Соціальна інженерія, розкриття її сутності та ключових термінів у контексті кібербезпеки.
2. Розгляд інструментів та методів, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу до інформації.
3. Аналіз психологічних аспектів, які використовуються в соціальній інженерії для впливу на користувачів та підвищення їхньої вразливості до атак.
4. Оцінка важливості освіти користувачів у запобіганні соціальним атакам, а також розгляд технічних та організаційних контрзаходів для ефективного захисту від соціально-інженерних атак.

Самостійна робота здобувачів вищої освіти

1. Навчитись ідентифікації атак із застосуванням соціальної інженерії та встановити інструменти збору інформації. Отримати навики збору відкритої інформації.
2. Інструменти збору інформації в Інтернеті. Отримання особистих даних для доступу до соціальних мереж з використанням Social Engineering Toolkit (SET) та Credential Harvest method. Процес визначення цілей соціоінженерної атаки.

План індивідуально-консультаційної роботи

Підготуйте презентацію на одну з тем:
1. Вчення про кіберзлочинність: поняття, ознаки, види, структура та показники.
2. Зміст поняття «кіберзлочинець» та його характеристика.
3. Вчення про кібертероризм.
4. Поняття та система запобігання кіберзлочинності.
5. Вчення про кібербезпеку.
6. Особливості методики розслідування кіберзлочинів.
7. Запобігання кіберзлочинам в Європейському Союзі.

Питання для самоконтролю

1. Що таке соціальна інженерія і які ключові терміни пов'язані з нею?
2. Які інструменти та методи використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу?
3. Вкажіть ключові психологічні аспекти соціальної інженерії, які впливають на користувачів і роблять їх вразливими до атак.
4. Охарактеризуйте основні види соціальних атак, зокрема фішинг, блефи, обман та імперсонація.
5. Які стратегії та рекомендації для користувачів допомагають виявляти та запобігати соціальним атакам?
6. Які технічні та організаційні контрзаходи є ефективними для захисту від соціально-інженерних атак?
7. В чому полягає важливість освіти користувачів для ефективного запобігання соціальним атакам.
8. Як взаємодія та обмін інформацією в спільноті допомагають попереджати соціальні атаки

Рекомендована література

Основна: [2, 3, 5]
Допоміжна: [8, 10, 11]
Інформаційні ресурси в Інтернеті: [1, 3, 5]
Міжнародні видання: [1, 2]

Тема 9. Кібербезпека та основні принципи технічного захисту в умовах постійного технологічного розвитку.

План лекційного заняття

1. Аспекти кібербезпеки та основні принципи технічного захисту в умовах швидкого технологічного розвитку.
2. Аналіз сучасних тенденцій технологічного розвитку та їхнього впливу на кібербезпеку.
3. Методи та технічні рішення забезпечення безпеки в хмарних сервісах та мобільних пристроях.
4. Виклики та заходи безпеки, пов'язані зі зростанням кількості підключених до Інтернету пристроїв у різних сферах життя.
5. Роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.

План практичного заняття

1. Аспекти кібербезпеки та основні принципи технічного захисту в умовах швидкого технологічного розвитку.
2. Аналіз сучасних тенденцій технологічного розвитку та їхнього впливу на кібербезпеку.
3. Методи та технічні рішення забезпечення безпеки в хмарних сервісах та мобільних пристроях.
4. Виклики та заходи безпеки, пов'язані зі зростанням кількості підключених до Інтернету пристроїв у різних сферах життя.
5. Роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.

Самостійна робота здобувачів вищої освіти

1. Ознайомтеся з повним текстом порад для безпеки в мережі Інтернет від команди CERT-UA (cert.gov.ua/?p848) та порівняйте їх з правилами інтернет-безпеки від Профспілки працівників освіти і науки України (pon.org.ua/novyny/5427-bezpeka-v-nternet-scho-potrbnoznati.html). Зверніть увагу, які рекомендації збігаються. З якими загрозами вони пов’язані?

Питання для самоконтролю

1. Які основні принципи технічного захисту інформації в умовах швидкого технологічного розвитку?
2. Які сучасні виклики та стратегії захисту від кіберзагроз існують у постійно прогресуючому технічному середовищі?
3. Вкажіть сучасні тенденції технологічного розвитку та як вони впливають на кібербезпеку.
4. Які архітектурні засади побудови ІТ-інфраструктури враховують вимоги до безпеки в сучасному технологічному середовищі?
5. Які методи та технічні рішення забезпечують безпеку в хмарних сервісах, які є ключовими елементами сучасної ІТ-інфраструктури?
6. Які методи та технології використовуються для захисту мобільних пристроїв та даних в умовах активного використання мобільних технологій?
7. Які виклики та заходи безпеки пов'язані зі зростанням кількості пристроїв, підключених до Інтернету, у різних сферах життя?
8. Яку роль відіграє штучний інтелект у виявленні та вирішенні кіберзагроз у реальному часі?

Рекомендована література

Основна: [2, 3, 5]

Допоміжна: [8, 10, 11, 14]

Інформаційні ресурси в Інтернеті: [1, 3, 5]

Міжнародні видання: [1, 2]

4. КРИТЕРІЇ ОЦІНЮВАННЯ РІВНЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ ЗДОБУВАЧІВ ВИЩОЇ ОСВІТИ

Розподіл балів за семінарське/практичне 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 диференційованого заліку (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 диференційованого заліку.

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;
- диференційований залік.

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. 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.

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. Поняття та ознаки кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних даних та систем
73. Поняття та ознаки незаконного доступу, незаконного перехоплення, втручання в дані, втручання в систему.
74. Характеристика складу кіберзлочинів проти конфіденційності, цілісності та доступності комп'ютерних даних та систем.

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. 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.
6. 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.
7. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за заг. ред. А. Ф. Волобуєва. Одеса : ТЕС, 2020. С 372.
8. Аленін Ю. П., Аркуша Л. І. Кримінальний процес: навч. посібник. Одеса: Фенікс, 2020. С. 582.
9. 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 запобігання та протидію домашньому насильству: Закон України від 07.12.2017 № 2229-VIII. *Відомості Верховної Ради.* 2018. № 5. ст.35. http://zakon2.rada.gov.ua/laws/show/96/2016
4. 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
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017. *Відомості Верховної Ради*. 2017. № 45. ст.403. http://zakon2.rada.gov.ua/laws/show/96/2016
6. 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
7. 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.
8. Дідківська Г. В. Сімейне неблагополуччя в системі детермінантів злочинності неповнолітніх в Україні: монографія. Вінниця: Нілан ЛТД, 2019. 220 с.
9. Ільїна О. В. Співвідношення кримінально-правової політики з кримінально-виконавчою політикою. Актуальні проблеми вітчизняної юриспруденції. № 3. Дніпро. 2022. С. 98-104.
10. Лантінов Я. О. Щодо конкуренції між термінами "кримінально-правова політика" та

"політика протидії злочинності". Форум Права. № 2 (73). Харків. 2022. С. 22-28.
11. 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.
12. Кримінальне право УЄ і будівництво загальноєвропейського правового простору: монографія. за заг. ред. Ю. О. Костенка. Харків: Право, 2019.
13. 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.
14. Головкін Б. М. Теперішнє і майбутнє кримінології. Проблеми законності. 2020. Вип. 149. С. 168–184.
15. 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).
16. 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