МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут права
Кафедра кримінального права та процесу

Затверджено
Науково-методичною радою Університету,
протокол від «30» 09 25 № 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 К Безпека та оборона
спеціальність К9 Правоохоронна діяльність
Освітньо-професійна програма «Правове забезпечення протидії кіберзлочинності»
Статус дисципліни: обов'язкова

галузь знань К Безпека та оборона
спеціальність К3 «Національна безпека (за окремими сферами забезпечення і видами діяльності)»
Освітньо-професійна програма «Національна фінансова безпека»
Статус дисципліни: обов'язкова

Ірпінь - 2025

Робоча програма навчальної дисципліни «Аналіз та прогнозування кіберзлочинності» складена на основі освітньо-професійної програми «Правове забезпечення протидії кіберзлочинності» другого (магістерського) рівня спеціальності К9 Правоохоронна діяльність, затвердженої Вченою радою Університету «29» 05 2025 року, протокол № 15; спеціальності К3 «Національна безпека (за окремими сферами забезпечення і видами діяльності)» на основі освітньо-професійної програми другого (магістерського) рівня «Національна фінансова безпека», затвердженої Вченою радою Університету «29» 05 2025 року, протокол № 15.

Укладачі: М. МАКСІМЕНЦЕВ, д-р юрид.наук, доцент, професор кафедри кримінального права та процесу

Д. ЛОПАЩУК, канд.юрид.наук, доцент, доцент кафедри кримінального права та процесу

Гарант ОПП «Правове забезпечення протидії кіберзлочинності» Г. ДІДКІВСЬКА, д-р юрид.наук, професор, професор кафедри кримінального права та процесу

Гарант ОПП «Національна фінансова безпека» А. ГАРБІНСЬКА-РУДЕНКО, канд.юрид.наук, доцент, доцент кафедри фінансового та податкового права

Робочу програму навчальної дисципліни розглянуто та схвалено кафедрою кримінального права та процесу, протокол від «27» серпня 2025 р. № 1-1.

Завідувач кафедри Г. ДІДКІВСЬКА, д-р юрид.наук, професор, професор кафедри

Розглянуто і схвалено Вченою радою Навчально-наукового інституту права, від «11» вересня 2025 р. № 3.

Голова вченої ради ННІ права В. ТОПЧІЙ, д.ю.н., професор

Завідувач навчально-методичного відділу Г. ГРИЩУК, доктор філософії

Реєстраційний № ____

ЗМІСТ

1. ПЕРЕДМОВА.

Анотація навчальної дисципліни. Навчальна дисципліна «Аналіз та прогнозування кіберзлочинності» спрямована на формування у здобувачів вищої освіти системних знань, умінь та навичок щодо виявлення тенденцій, закономірностей і факторів, що впливають на розвиток кіберзлочинності, а також розроблення науково обґрунтованих прогнозів її динаміки.

У межах курсу розглядаються теоретичні та практичні аспекти аналізу кіберзлочинності, методи збору й обробки даних, побудова статистичних моделей, використання інструментів штучного інтелекту та машинного навчання для прогнозування кіберзагроз. Особлива увага приділяється аналізу сучасних тенденцій у сфері кібербезпеки, впливу глобалізації, цифрової трансформації та міжнародного співробітництва на рівень кіберзлочинності.

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.

Міждисциплінарні зв'язки. ОП «Правове забезпечення протидії кіберзлочинності». Дисципліни-пререквізити: «Управління правоохоронною діяльністю», «Актуальні проблеми кримінального права», «Актуальні питання кримінально-правової та кримінологічної характеристики кіберзлочинності в Україні», «Актуальні питання євроінтеграції кримінального законодавства», «Оперативно-технічне забезпечення національної безпеки». Дисципліни-постреквізити: «Кримінальні процесуальні та криміналістичні проблеми розслідування кіберзлочинів», «Міжнародні стандарти правоохоронної діяльності».

ОП «Національна фінансова безпека». Дисципліни-пререквізити: «Інституційні засади запобігання загрозам територіальної цілісності та екстремізму», «Міжнародно-правові механізми захисту прав людини», «Державний розвиток в умовах загроз національній безпеці», «Державне управління у сфері національної безпеки», «Правове забезпечення діяльності сектору безпеки та оборони», «Теорія національної безпеки». Дисципліни-постреквізити: «Міжнародне співробітництво у сфері розшуку активів, що одержані незаконним шляхом», «Стратегічне планування та впровадження інновацій у фінансовій безпеці», «Попередження та боротьба з корупцією у сфері фінансової безпеки», «Інформаційна безпека держави», «Виявлення та розшук активів у кримінальному провадженні».

Методи навчання:

- за джерелом інформації і сприйняття навчальної інформації: словесні (лекція, семінарське заняття, бесіда, розповідь); наочні (презентація, слайди); практичні (збір інформації та її систематизація);
- за логікою передачі і сприйняття навчального матеріалу: індуктивні, дедуктивні, аналітичні, синтетичні;
- за ступенем самостійного мислення при засвоєнні знань: репродуктивні та продуктивні (частково-пошукові);

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

Форми та засоби діагностики результатів навчання. Контроль успішності навчання здобувачів проводиться у формах поточного і підсумкового контролю. Формами поточного контролю є:

- усне опитування;
- тестування;
- розв'язування задач, виконання практичних завдань;
- письмові модульні контрольні роботи.

Підсумковий контроль – диференційований залік.

Організація поточного та підсумкового контролю здійснюється з використанням засобів дистанційного навчання в системі Moodle.

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Характеристика навчальної дисципліни для здобувачів другого (магістерського) рівня вищої освіти (120 год/4 кредити ЄКТС)

<table>
<tr><td rowspan="2">Показники</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td>Кількість кредитів ЄКТС - 4</td><td>4</td><td>4</td></tr>
<tr><td>Модулів - 2</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів - 2</td><td>1-й</td><td>1-й</td></tr>
<tr><td rowspan="11">Загальна кількість годин - 120 годин</td><td colspan="2">Семестр</td></tr>
<tr><td>2-й</td><td>2-й</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td>22 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Практичні заняття</td></tr>
<tr><td>18 год.</td><td>4 год.</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>78 год.</td><td>110 год.</td></tr>
<tr><td colspan="2">Індивід.-консультац. робота: 2 год.</td></tr>
<tr><td colspan="2">Форма семестрового контролю: диференційований залік</td></tr>
</table>

3. 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. 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.	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, 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 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.	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 частині забезпечення процедур розшуку та арешту активів РН18. Забезпечення національних інтересів держави у кіберпросторі. Н19. Застосовувати спеціальні знання з метою забезпечення національних інтересів держави у кіберпросторі в умовах гібридних загроз національній фінансовій безпеці.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

для здобувачів другого (магістерського) рівня вищої освіти денної форми навчання
(120 год/ 4 кредити ЄКТС)

№ 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

для здобувачів другого (магістерського) рівня вищої освіти заочної форми навчання
(120 год/ 4 кредити ЄКТС)

№ 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: контрольна робота (за рахунок практичного заняття – 40 хв.)						
Форма підсумкового контролю – диференційований залік (ПМК).						
Усього за навчальною дисципліною:		4	4	2	110	120

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗМІСТОВИЙ МОДУЛЬ І. КОМПЛЕКСНИЙ АНАЛІЗ ТА РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ У СУЧАСНОМУ ЦИФРОВОМУ СЕРЕДОВИЩІ

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.

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).

Рекомендована література:

Основні: [1, 3, 4, 6, 7]
Допоміжна: [8, 10, 11]
Інформаційні ресурси Інтернет: [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.

Рекомендована література:

Основна: [3, 4, 5, 6]
Допоміжна: [7, 9,10, 15]
Інформаційні ресурси Інтернет: [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.

Рекомендована література:

Основна: [2, 3, 4]
Допоміжна: [7, 9,10, 15]
Міжнародні видання: [1, 2, 3]
Інформаційні ресурси Інтернет: [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 скриньці, 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».

Рекомендована література:

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

ЗМІСТОВИЙ МОДУЛЬ 2. КІБЕРЗЛОЧИННІСТЬ ПРОТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ОСОБА ЗЛОЧИНЦЯ ТА ЗАХИСНІ МЕХАНІЗМИ

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?

Рекомендована література:

Основна: [2, 3, 5]
Допоміжна: [8, 10, 11]
Інформаційні ресурси Інтернет: [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 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.

Рекомендована література:

Основна: [2, 3, 5]
Допоміжна: [8, 10, 11]
Інформаційні ресурси Інтернет: [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.

Рекомендована література

Основна: [2, 3, 5]
Допоміжна: [8, 10, 11]
Інформаційні ресурси Інтернет: [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?

Рекомендована література

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

6. ПИТАННЯ ПІДСУМКОВОГО КОНТРОЛЮ

1. Поняття кіберзлочинності та її місце в загальній структурі злочинності.
2. Види кіберзлочинів.
3. Поняття європейського конвенційного механізму запобігання кіберзлочинності.
4. Система європейського конвенційного механізму запобігання кіберзлочинності.
5. Детермінанти та основні напрями запобігання кіберзлочинності.
6. Особливості криміналістичної характеристики кіберзлочинів.
7. Характеристика способів вчинення злочину.
8. Особливості етапів розслідування кіберзлочинів.
9. Поняття електронних (цифрових) доказів у кримінальному провадженні та їх види.
10. Способи збирання електронних доказів.
11. Способи забезпечення допустимості цифрових доказів.
12. Типові слідчі ситуації та завдання початкового та наступного етапів розслідування кіберзлочинів.
13. Характеристика тактичних операцій розслідування кіберзлочинів: їх послідовність, специфіка їх внутрішньої структури.
14. Особливості тактики провадження окремих слідчих (розшукових) дій у справах про кіберзлочин.
15. Сутність та криміналістична класифікація кіберзлочинів, вчинених з корисливих мотивів.
16. 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.
17. Особливості розслідування кіберзлочинів, що порушують встановлений порядок обігу певних речей: криміналістична характеристика, типові слідчі ситуації початкового етапу і програми (алгоритми) розслідування.
18. Поняття особи кіберзлочинця.
19. Структура особистості кіберзлочинця.
20. Соціально-демографічні ознаки особистості кіберзлочинця.
21. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця.
22. Типологія кіберзлочинців.
23. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології.
24. Соціальна інженерія, розкриття її сутності та ключових термінів у контексті кібербезпеки.
25. Розгляд інструментів та методів, що використовуються соціальними інженерами для маніпуляції та отримання несанкціонованого доступу до інформації.
26. Аналіз психологічних аспектів, які використовуються в соціальній інженерії для впливу на користувачів та підвищення їхньої вразливості до атак.
27. Оцінка важливості освіти користувачів у запобіганні соціальним атакам, а також розгляд технічних та організаційних контрзаходів для ефективного захисту від соціально-інженерних атак.
28. Аспекти кібербезпеки та основні принципи технічного захисту в умовах швидкого технологічного розвитку.
29. Аналіз сучасних тенденцій технологічного розвитку та їхнього впливу на кібербезпеку.
30. Методи та технічні рішення забезпечення безпеки в хмарних сервісах та мобільних пристроях.
31. Виклики та заходи безпеки, пов'язані зі зростанням кількості підключених до Інтернету пристроїв у різних сферах життя.
32. Роль штучного інтелекту у виявленні та вирішенні кіберзагроз у реальному часі.
33. Основні етапи генезису кіберзлочинності.
34. Характерні риси кіберзлочинності.
35. Яким чином кіберзлочинність впливає на міжнародне соціальне середовище?
36. Основні загрози кіберзлочинності для суспільної безпеки.
37. Які правові системи найбільше піддаються кіберзлочинним посяганням?
38. Класифікація комп'ютерних злочинців за віком та психофізіологічними особливостями.
39. Цілі та об'єкти правопорушень характерні для різних типів комп'ютерних злочинців.
40. Види злочинів у сфері використання сучасних інформаційних технологій найпоширеніші.
41. Міжнародна класифікація кіберзлочинів.
42. Які заходи можна застосувати для ефективної боротьби з кіберзлочинністю

на міжнародному рівні?

43. Правові засади протидії кіберзлочинності існують в Україні.
44. Міжнародне законодавство в сфері протидії кіберзлочинності.
45. Організаційні засади протидії кіберзлочинності.
46. Основні проблеми у сфері протидії кіберзлочинності в Україні.
47. Напрямки удосконалення протидії кіберзлочинності можна виділити.
48. Яке значення має міжнародне співробітництво у сфері протидії кіберзлочинності?
49. Як відбувається координація між національними та міжнародними організаціями у боротьбі з кіберзлочинністю?
50. Ключові аспекти правових засад протидії кіберзлочинності в Україні можна виділити.
51. Які методи і стратегії використовуються в Україні для організаційної протидії кіберзлочинності?
52. Які міжнародні ініціативи та договори сприяють ефективній протидії кіберзлочинності?
53. Інформаційна безпека та її основні складові.
54. Яким чином інформаційна безпека впливає на загальну безпеку держави?
55. Основні напрямки інформаційної безпеки.
56. Правові методи здійснення інформаційної безпеки.
57. Технічні та програмні засоби захисту інформації.
58. Криптографічні методи захисту інформації і як вони застосовуються.
59. Охарактеризуйте еволюцію загроз інформаційній безпеці вплинула на сучасні системи захисту.
60. Який вплив має інтернет на розвиток шкідливих програм?
61. Основні методи шахрайства використовують зловмисники і як можна їм протидіяти.
62. Вкажіть основні класифікаційні ознаки сучасних кіберзагроз.
63. Класифікація кіберзагроз за їх характеристиками та методами атак.
64. Основні види кіберзагроз і які їх можливі наслідки для організацій та користувачів.
65. Методи соціально-інженерних атак використовуються сучасними кіберзлочинцями.
66. Технічні підходи здійснення атак через експлойти вразливостей.
67. Популярні вектори атак у сучасному кіберпросторі.
68. Як штучний інтелект і блокчейн можуть бути використані для створення складних кіберзагроз?
69. Новітні технології передбачення та запобігання кіберзагрозам.
70. Як можна проаналізувати та вивчити конкретні випадки сучасних кібератак для розробки ефективних стратегій захисту?
71. Основні принципи технічного захисту інформаційних систем в умовах швидкого технологічного розвитку.
72. Сучасні тенденції технологічного розвитку впливають на кібербезпеку.
73. Яким чином побудувати архітектуру іт-інфраструктури з урахуванням вимог до безпеки?
74. Методи технічного захисту інформаційних систем в хмарних.
75. Основні виклики та рішення для забезпечення безпеки мобільних пристроїв.
76. Поняття кіберзлочинів проти конфіденційності, цілісності та доступності комп’ютерних даних та систем.
77. Ознаки кіберзлочинів проти конфіденційності, цілісності та доступності комп’ютерних даних та систем.
78. Поняття незаконного доступу, незаконного перехоплення, втручання в дані, втручання в систему.
79. Ознаки незаконного доступу, незаконного перехоплення, втручання в дані, втручання в систему.
80. Характеристика складу кіберзлочинів проти конфіденційності, цілісності та доступності комп’ютерних даних та систем.

7. РОЗПОДІЛ БАЛІВ ТА КРИТЕРІЇ ОЦІНЮВАННЯ

Денна форма навчання

Модулі	**Змістовний модуль 1**					**Допуск – 50 балів**	**Диф.залік - 50 балів**	**Загальна оцінка з курсу - 100 балів**
Загальна кількість балів за модулем №1	**20**							
Теми	**Т.1**	**Т.2**	**Т.3**	**Т.4**	**Т.5**			
Практичне заняття	3	3	3	3	3			
Самостійна робота	Оцінювання самостійної роботи здійснюється під час практичних занять та написання контрольної роботи							
Модульна контрольна робота	5							
Модулі	**Змістовний модуль 2**							
Загальна кількість балів за модулем №2	**30**							
Теми	**Т.6**	**Т.7**	**Т.8**	**Т.9**				
Практичне заняття	3	3	3	3				
Самостійна робота	Оцінювання самостійної роботи здійснюється під час практичних занять та написання контрольної роботи							
Модульна контрольна робота	5							
Індивідуально-консультаційна робота	8							
Підсумковий тестовий контроль на порталі дистанційної освіти Moodle	5							

Заочна форма навчання

Модулі	**Змістовний модуль 1**					**Допуск – 50 балів**	**Диф.залік - 50 балів**	**Загальна оцінка з курсу - 100 балів**
Загальна кількість балів за модулем №1	**10**							
Теми	**Т.1**	**Т.2**	**Т.3**	**Т.4**	**Т.5**			
Практичне заняття	-	10	-	-	-			
Самостійна робота	Оцінювання самостійної роботи здійснюється під час практичних занять та написання контрольної роботи							
Модульна контрольна робота	-							
Модулі	**Змістовний модуль 2**							
Загальна кількість балів за модулем №2	**40**							
Теми	**Т.6**	**Т.7**	**Т.8**	**Т.9**				
Практичне заняття	-	10	-	-				
Самостійна робота	Оцінювання самостійної роботи здійснюється під час практичних занять та написання контрольної роботи							
Модульна контрольна робота	15							
Індивідуально-консультаційна робота	10							
Підсумковий тестовий контроль на порталі дистанційної освіти Moodle	5							

Критерії оцінювання роботи на практичних заняттях

Максимальна кількість балів отриманих здобувачем вищої освіти на практичному занятті для денної форми навчання становить 3 бали, а для заочної форми навчання 10 балів (табл. 7.1). Виконання самостійної роботи оцінюється під час проведення практичного заняття у вигляді опитування в тому числі за питаннями, які виносяться на самостійну роботу.

Таблиця 7.1.

Шкала оцінювання роботи здобувачів вищої освіти на практичних заняттях

Критерії оцінювання	Кількість балів	
	ДФН	ЗФН
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	10-8
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	7-5
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	4-1
Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.	0	0

Критерії оцінювання контрольних робіт.

Формою проміжного поточного контролю є контрольні роботи, які проводяться у письмовій формі та кожна з яких оцінюється від 0 до 5 балів для денної форми навчання та від 0 до 15 балів для заочної форми навчання.

Розподіл балів за різні види завдань в межах модульної контрольної роботи (денна форма навчання)

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

Розподіл балів за різні види завдань в межах контрольної роботи (заочна форма навчання)

Вид завдання	Максимальна кількість балів за виконання
Теоретичні питання (2 питання по 2,5)	5
Тестовий блок (закритої форми - 20 по 0,5)	10
Всього	15

Критерії оцінювання індивідуально-консультаційної роботи

Індивідуально-консультаційна робота проводиться у формі тез доповіді, реферату, презентації, статті, проєктів або в інших формах описаних робочою програмою і оцінюється від 0 до 8 балів (табл. 7.3).

Таблиця 7.3.

Шкала оцінювання індивідуально-консультаційної роботи здобувачів вищої освіти

Критерії оцінювання	Кількість балів	
	ДФН	ЗФН
Послідовність, логічність виконання індивідуально-консультаційної роботи, а також підготовлення презентації, її захист, а також виокремлення з різних джерел основних положень, які структурно об'єднанні, проаналізовані та узагальнені висновками**.**	**8-6**	**10-8**
Послідовність, логічність написання індивідуально-консультаційної роботи, але без підготовлення презентації або без захисту.	**5-1**	**7-1**
Не написання індивідуально-консультаційної роботи	**0**	**0**

Підсумкове оцінювання знань здобувачів вищої освіти здійснюється за результатами поточного контролю (від 0 до 50 балів) та підсумкового контролю (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.

Загальний розподіл балів, які здобувач вищої освіти може отримати в межах 100-бальної системи оцінювання, повинен включати обов'язкове комп'ютерне тестування на платформі дистанційного навчання ДПУ Moodle (максимально до 5 балів).

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
8	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	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	

8. **РЕКОМЕНДОВАНА ЛІТЕРАТУРА**

Основна:

1. Конституція України від 28 червня 1996 року № 254к/96. URL: https://zakon.rada.gov.ua
2. Кримінальний кодекс України від 05.04.2001 № 2341-14. URL: http://zakon.rada.gov.ua/laws
3. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI URL: https://zakon.rada.gov.ua/laws
4. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017. № 2163-VIII. URL: http://zakon.rada.gov.ua/law
5. Указ Президента України «Про Національний координаційний центр кібербезпеки» від 07.06.2016 № 242/2016. URL: http://zakon.rada.gov.ua
6. Актуальні питання інформаційного права: навч. посіб. /В. Г. Хахановський, О. В. Корнейко. Київ: Нац. акад. внутр. справ, 2024. 258 с..
7. Анонімність в інтернеті. Цифрові цінності: наук.-прак.посібник /авт.кол.: М.Г. Вербенський, В.О. Криволапчук, Д.В. Смерницький та ін. Київ: «Видавництво Людмила, 2022. 48 с
8. Виявлення та розслідування кіберзлочинів: навчально-методичний посібник. О. А. Самойленко. Одеса: 2020. 112 с.
9. Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навчальний посібник / Майданевич Л. О., Войтович О. П., Шелепало Г. В. Вінниця: ВНТУ, 2025. 109 с.

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. Аніщук В. В., Зицик С. Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. Науковий вісник Ужгородського Національного Університету. Серія : Право. 2024. Вип. 83, Ч. 3. С. 19–23.
4. Бараненко Р. В. Кіберзлочин, комп'ютерний злочин чи кіберправопорушення? Аналіз особливостей застосування термінології. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2021. Вип. 1 (49). С. 85– 90
5. Баранов О. А. Цивілізаційна місія цифрових трансформацій. Інформація і право. 2023. № 3 (46). С. 25–41
6. Бодунова О. М. Кримінологічні засади запобігання злочинності у сфері інформаційних технологій: дис. ... д-ра юрид. наук : 12.00.08 / Мін-во фінансів України, Державний податковий ун-т. Ірпінь, 2023. 433 с
7. Боженко В. В., Кушнерьов О. С., Кільдей А. Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. Економічний форум. 2021. № 4. С. 116–121
8. Галушко П. П. Кіберзлочинність в Україні в умовах війни як об'єкт кримінологічного аналізу // Теоретичні питання юриспруденції і проблеми правозастосування: виклики XXI століття: тези доп. учасників VII Всеукр. наук.-практ. конф. (Харків, 09 черв. 2023 р.), С. 128–131.
9. Галушко П. П. Кіберзлочинність у фокусі кримінолого-феноменологічного аналізу. Вісник Кримінологічної асоціації України. 2024. № 3 (33). С. 884–891
10. Галушко П. П. Кіберзлочинність: поняття та соціально-правова природа. Вісник Кримінологічної асоціації України. 2025. № 1 (34). С. 808–817.
11. Галушко П. П. Особа кіберзлочинця: кримінолого-типологічна характеристика. Вісник Кримінологічної асоціації України. 2025. № 2 (35). Ч. 1. С. 73–85.
12. Деревягін О. О., Пашнєв Д. В., Новицький А. О. Окремі підходи до визначення сучасного портрету професійного кібершахрая. Вісник Кримінологічної асоціації України. 2025. № 1 (34). С. 236–248.
13. Джелілова М. А. Причини та умови організованої злочинності в умовах воєнного стану: регіональний аспект. Протидія злочинності: проблеми практики та науково-методичне забезпечення. 2023. № 2. С. 25–35.
14. Дідківська Г., Шевченко Д. Основоположні принципи протидії кіберзлочинності: міжнародний досвід. Legal Horizons. 2024. № 4 (19). С. 19– 23
15. Думчиков М. О., Каріх І. В. Становлення та генеза кримінальної відповідальності за кримінальні

правопорушення у кіберпросторі на тернах України. Юридичний науковий електронний журнал. 2022. № 5. С. 476–478
16. Корзун С. В. Теоретико-методологічна конструкція державної кримінально-правової політики протидії кіберзлочинності. Економіка, управління та адміністрування. 2024. № 4 (110). С. 145–158.

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).

9. ЛИСТ ОНОВЛЕННЯ ТА ПЕРЕЗАТВЕРДЖЕННЯ

РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

РОЗГЛЯНУТО ТА СХВАЛЕНО
на засіданні кафедри кримінального права та процесу
від _____20__р. № ___

Укладачі: М. МАКСІМЕНЦЕВ, д-р юрид.наук, доцент, професор кафедри кримінального права та процесу

Д. ЛОПАЩУК, канд. юрид. наук, доцент, доцент кафедри кримінального права та процесу

Лист оновлення та перезатвердження робочої програми навчальної дисципліни
(протягом 5 років після затвердження або до затвердження освітньої програми)

Навчальний рік	Дата засідання кафедри	Номер протоколу	Підпис завідувача кафедри	Підпис гаранта ОП