ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
В.о. декана юридичного факультету
_____ Т.О. Коломоєць
«____» «_____» 2026

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРПРОСТІР ТА ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ

освітньо-професійної програми «Кібербезпека»
першого (бакалаврського) рівня вищої освіти
за спеціальністю F5 «Кібербезпека та захист інформації»
денної та заочної форм здобуття освіти

ВИКЛАДАЧ: Муцураєва Луїза Асхабівна, PhD, викладач кафедри кримінального права та правоохоронної діяльності

Обговорено та ухвалено.
на засіданні кафедри кримінального права та
правоохоронної діяльності

Протокол № 1 від 28.08.2026 р.
В.о. завідувача кафедри кримінального.
права та правоохоронної діяльності

_____Роман БАРАННІК

Погоджено:
Гарант освітньої програми

_____Олексій КУДІН

2026 рік

Зв'язок з викладачем (викладачами):
Сезн ЗНУ повідомлення:
Телефон: *(095) 619-70-18*
E-mail: *medinaichkeriyskaya@gmail.com*
Кафедра: кримінального права та правоохоронної діяльності. Заняття проводяться дистанційно в Zoom; посилання на конференції — на сторінці дисципліни в Moodle.

1. Опис навчальної дисципліни

Предметом вивчення навчальної дисципліни «Кіберпростір та протидія кіберзлочинності» є правове регулювання відносин у кіберпросторі, кримінально-правова характеристика кіберзлочинів за законодавством України, процесуальні механізми їх розслідування, а також правові межі професійної діяльності фахівця з кібербезпеки.

Програма навчальної дисципліни складається з трьох змістових модулів:

— Кіберпростір як об'єкт правового регулювання.

— Кримінально-правова характеристика кіберзлочинності.

— Протидія кіберзлочинності: процесуальні та практичні аспекти.

Дисципліна належить до циклу професійної підготовки освітньої програми і посідає в структурно-логічній схемі особливе місце: вона є першим освітнім компонентом, що формує в здобувачів правову складову професійної компетентності, та створює основу для подальшого опанування дисциплін «Нормативно-правове забезпечення інформаційної безпеки» і «Інформаційна безпека держави».

Особливість дисципліни полягає в тому, що вона викладається здобувачам технічної спеціальності, які не мають попередньої правової підготовки, і на етапі, коли профільні технічні дисципліни ще не опановані. Тому курс побудований самодостатньо: він не вимагає спеціальних знань ані з права, ані з мережевих технологій, а спирається на аналіз реальних правозастосовних ситуацій.

Основними джерелами вивчення дисципліни є Конституція України, Кримінальний та Кримінальний процесуальний кодекси України, закони України «Про основні засади забезпечення кібербезпеки України» і «Про критичну інфраструктуру», Конвенція Ради Європи про кіберзлочинність та протоколи до неї, акти законодавства Європейського Союзу у сфері мережевої та інформаційної безпеки, а також практика Верховного Суду, матеріали Єдиного державного реєстру судових рішень і офіційна статистика Департаменту кіберполіції, Офісу генерального прокурора, Національного банку України та Держспецзв'язку.

Метою вивчення дисципліни є формування у здобувачів здатності діяти на основі законодавства України та міжнародних стандартів у сфері кібербезпеки, кваліфіковано взаємодіяти з правоохоронними органами під час реагування на кіберінциденти та усвідомлювати правові межі власної професійної діяльності.

Основними цілями вивчення дисципліни є: опанування понятійного апарату законодавства про кібербезпеку; набуття вміння розмежовувати кіберінцидент, кібератаку і кіберзлочин та визначати правові наслідки кожного; формування навичок кваліфікації типових протиправних діянь у кіберпросторі; засвоєння вимог до збирання і збереження цифрових доказів; розуміння правових підстав проведення тестування на проникнення та узгодженого розкриття вразливостей; формування нетерпимого ставлення до протиправного використання професійних знань.

Паспорт навчальної дисципліни

Нормативні показники	денна форма здобуття освіти	заочна форма здобуття освіти
Статус дисципліни	Обов'язкова	
Семестр	3-й	
Кількість кредитів ECTS	-	
Кількість годин	120	
Лекційні заняття	32	
Семінарські / Практичні / Лабораторні заняття	32	
Самостійна робота	56	
Консультації	дистанційні у Zoom — вівторок з 15:00 до 16:00; в інший час за попередньою домовленістю. Посилання на конференцію публікується на сторінці дисципліни в Moodle. *Запис на консультації: Moodle (приватні повідомлення)*	
Вид підсумкового семестрового контролю:	**екзамен**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=18507	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
1	***2***	***3***
КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КЗ 5. Здатність до пошуку, оброблення та аналізу інформації. КЗ 6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства, верховенства права, прав і свобод людини. ФК 1. Здатність застосовувати законодавчу та нормативно-правову базу, державні та міжнародні вимоги, практики і стандарти для здійснення професійної діяльності.	Лекції з елементами проблемного викладу та візуалізацією. Інтерактивні методи: аналіз правових ситуацій, кейс-метод, дискусія, робота в малих групах. Лабораторні заняття як робота з першоджерелами: нормативно-правовими актами, судовими рішеннями,	Поточне оцінювання: — виконання та захист лабораторних робіт; — тестування в СЕЗН Moodle за матеріалами кожного змістового модуля; — розв'язання кваліфікаційних задач (кейсів); — підготовка аналітичних документів. Підсумкове оцінювання: екзамен

ФК 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. ФК 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники. ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел. ПРН 4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач, відповідати за прийняті рішення. ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог стандартів, у тому числі міжнародних. ПРН 8. Готувати пропозиції до нормативних актів щодо забезпечення кібербезпеки. ПРН 9. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти. ПРН 43. Застосовувати національні та міжнародні регулюючі акти для розслідування інцидентів. ПРН 54. Усвідомлювати цінності громадянського суспільства, верховенства права, прав і свобод людини і громадянина в Україні.	офіційною статистикою. Складання процесуальних та організаційних документів за зразками. Самостійна робота із СЕЗН ЗНУ (Moodle).	(тестування та розв'язання кейса).

3. Зміст навчальної дисципліни

Змістовий модуль 1. Кіберпростір як об'єкт правового регулювання

Тема 1. Кіберпростір і кіберзлочинність: понятійний апарат та джерела правового регулювання. Походження та зміст поняття кіберпростору. Легальні дефініції за Законом України «Про основні засади забезпечення кібербезпеки України»: кіберпростір, кібербезпека, кіберзахист, кібератака, кіберінцидент, кіберзлочин. Межі дії закону. Співвідношення інформаційної безпеки і кібербезпеки. Розмежування кіберінциденту, кібератаки та кіберзлочину. Система джерел правового регулювання та їх ієрархія.

Тема 2. Законодавство України про кібербезпеку. Національна система кібербезпеки та її суб'єкти. Принципи державної політики у сфері кібербезпеки. Розмежування компетенції Держспецзв'язку, Національної поліції, Служби безпеки України, Міноборони, розвідувальних

органів, НБУ та МЗС. Національний координаційний центр кібербезпеки. Національна система реагування на кіберінциденти: CERT-UA, галузеві та регіональні CSIRT, приватні команди реагування. Національна система обміну інформацією про кіберінциденти. Критична інформаційна інфраструктура та обов'язки її власників. Підрозділи та керівники з кіберзахисту.

Тема 3. Міжнародно-правові засади протидії кіберзлочинності. Конвенція про кіберзлочинність: матеріально-правові норми, процесуальні повноваження, міжнародне співробітництво. Додаткові протоколи. Конвенція ООН проти кіберзлочинності. Право Європейського Союзу у сфері мережевої та інформаційної безпеки в контексті євроінтеграції України. Застосовність міжнародного права до кібероперацій: суверенітет, застосування сили, атрибуція.

Змістовий модуль 2. Кримінально-правова характеристика кіберзлочинності

Тема 4. Кримінологічна характеристика кіберзлочинності в Україні. Стан, структура і динаміка за офіційною статистикою Департаменту кіберполіції, Офісу генерального прокурора, НБУ та Держспецзв'язку. Латентність та її причини. Класифікації кіберзлочинів. Особа кіберзлочинця. Організовані форми: шахрайські кол-центри, мережі дропів, фішингові угруповання. Віктимологічний аспект: соціальна інженерія як домінуючий чинник збитків.

Тема 5. Кримінальні правопорушення у сфері використання інформаційних систем: розділ XVI Кримінального кодексу України. Загальна характеристика розділу, родовий об'єкт, предмет. Несанкціоноване втручання (ст. 361 КК): об'єктивна сторона, момент закінчення, кваліфікуючі ознаки. Створення та розповсюдження шкідливих програмних чи технічних засобів (ст. 361-1 КК) і проблема засобів подвійного призначення. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом (ст. 361-2 КК). Дії особи, яка має право доступу (ст. 362 КК). Порушення правил експлуатації або порядку захисту інформації (ст. 363, 363-1 КК). Дія кримінального закону в часі за умов частих змін кіберзаконодавства.

Тема 6. Суміжні склади кримінальних правопорушень. Шахрайство з використанням електронно-обчислювальної техніки (ст. 190 КК) і його розмежування зі ст. 361 КК. Незаконні дії з документами на переказ і платіжними картками (ст. 200 КК). Легалізація доходів (ст. 209 КК) та проблема кваліфікації дій дропів. Створення злочинної організації та участь у ній (ст. 255 КК) у справах про кол-центри. Посягання на приватність (ст. 163, 182 КК). Протидія сексуальній експлуатації дітей онлайн. Кібертероризм, кібердиверсія та посягання на критичну інфраструктуру.

Тема 7. Юрисдикція, місце вчинення та транскордонний характер кіберзлочину. Дія закону про кримінальну відповідальність у просторі. Проблема визначення місця вчинення діяння. Конфлікт юрисдикцій і подвійна караність. Дані у хмарних сервісах і територіальність. Анонімізація та атрибуція. Екстрадиція.

Змістовий модуль 3. Протидія кіберзлочинності: процесуальні та практичні аспекти

Тема 8. Реагування на кіберінцидент: обов'язки суб'єктів та взаємодія з правоохоронними органами. Життєвий цикл інциденту та момент виникнення юридичних обов'язків. Обов'язкові повідомлення: адресат, строки, форма. Повідомлення про порушення захисту персональних даних.

Внесення відомостей до ЄРДР. Зміст заяви про кримінальне правопорушення. Дії та бездіяльність, які знищують сліди. Юридичні ризики внутрішнього розслідування.

Тема 9. Цифрові докази у кримінальному провадженні. Належність, допустимість і достовірність доказів. Електронна інформація в системі процесуальних джерел доказів. Тимчасовий доступ до речей і документів. Обшук та особливості вилучення електронних носіїв. Негласні слідчі (розшукові) дії: зняття інформації з електронних комунікаційних мереж та з електронних інформаційних систем. Ланцюг збереження доказів, хешування, робота з волатильними даними. Комп'ютерно-технічна експертиза та постановка питань експертові. Підстави визнання цифрових доказів недопустимими.

Тема 10. Міжнародне співробітництво у розслідуванні кіберзлочинів. Форми міжнародної правової допомоги. Мережа контактних пунктів 24/7. Термінове збереження даних. Прямі запити до іноземних постачальників послуг. Спільні слідчі групи. Взаємодія з Європолом, Інтерполом, Євроюстом. Обмеження, зумовлені захистом персональних даних.

Тема 11. Правові межі діяльності фахівця з кібербезпеки. Тестування на проникнення: обов'язкові умови договору та ризик кваліфікації за ст. 361 КК при виході за межі узгодженого обсягу. Програми пошуку вразливостей за винагороду та узгоджене розкриття вразливостей. Обробка персональних даних фахівцем з безпеки. Моніторинг і логування дій працівників. Професійна етика: конфлікт обов'язку повідомити та обов'язку зберігати конфіденційність. Розмежування дисциплінарної, цивільної, адміністративної та кримінальної відповідальності.

4. Структура навчальної дисципліни

Вид заняття / роботи	**Назва теми**	**Кількість годин**		**Згідно з розкладом**
		о/д.ф.	**з.ф.**	
Лекція 1	Тема 1.Кіберпростір і кіберзлочинність: понятійний апарат та джерела правового регулювання Перелік питань: 1. Кіберпростір як середовище та як правова категорія 2. Легальні дефініції за ст. 1 Закону «Про основні засади забезпечення кібербезпеки України»: кіберпростір, кібербезпека, кіберзахист, кібератака, кіберінцидент, кіберзлочин, кібертероризм, кібершпигунство. 3. Співвідношення понять «інформаційна безпека» і «кібербезпека». 4. Кіберзлочин vs кіберінцидент: не кожен інцидент є злочином, і не кожен злочин породжує інцидент. 5. Система джерел: Конституція, кодекси,	2		*Раз на тиждень*

	спеціальні закони, підзаконні акти, міжнародні договори як частина національного законодавства (ст. 9 Конституції). Ієрархія та вирішення колізій.			
Лабораторне заняття 1	Тема 1. Кіберпростір і кіберзлочинність: понятійний апарат та джерела правового регулювання Побудова понятійної карти: студенти зіставляють легальні дефініції з технічною термінологією, якою користуються у фаховій літературі (attack, breach, incident, threat), і фіксують розбіжності. Практична навичка — робота з zakon.rada.gov.ua: пошук акта, визначення чинної редакції, читання картки документа, відстеження змін.	2		*Раз на тиждень*
Самостійна робота	Тема 1. Кіберпростір і кіберзлочинність: понятійний апарат та джерела правового регулювання Опрацювання ст. 1–4 Закону № 2163-VIII у чинній редакції. Складання глосарію з 15 термінів у форматі: термін — легальне визначення — норма — власний приклад.			
Лекція 2-3	Тема 2. Законодавство України про кібербезпеку. Національна система кібербезпеки Перелік питань: 1. Закон № 2163-VIII: сфера дії, принципи, об'єкти кіберзахисту. 2. Суб'єкти забезпечення кібербезпеки та розмежування їх компетенції: Держспецзв'язку, Національна поліція (Департамент кіберполіції), СБУ, Міноборони та Генштаб, розвідувальні органи, НБУ. Національний координаційний центр кібербезпеки при РНБО. 3. CERT-UA: правовий статус, повноваження, порядок звернення. 4. Об'єкти критичної інфраструктури: Закон «Про критичну інфраструктуру», категоризація, особливий режим захисту. 5. Обов'язки власників об'єктів кіберзахисту. Стратегія кібербезпеки України та план її реалізації.	4		*Раз на тиждень*
Самостійна робота	Тема 2. Законодавство України про кібербезпеку. Національна система кібербезпеки та її суб’єкти Опрацювання ст. 4–9-1 Закону № 2163-VIII та ст. 1–3 Закону «Про критичну інфраструктуру». Побудова власної схеми національної системи			

	кібербезпеки із зазначенням норми, що закріплює кожен елемент.			
Лабораторне заняття 2	Тема 2. Законодавство України про кібербезпеку. Національна система кібербезпеки *Кейс: підприємство зазнало атаки. Визначити, чи є воно об'єктом критичної інфраструктури, до якого органу і в які строки зобов'язане звернутися, і скласти повідомлення про кіберінцидент до CERT-UA за встановленою формою.*	2		*Раз на тиждень*
Лабораторне заняття 3	Тема 2. Законодавство України про кібербезпеку. Національна система кібербезпеки *Розробити схему розподілу повноважень суб'єктів національної системи кібербезпеки з посиланнями на конкретні норми.*	2		*Раз на тиждень*
Лекція 4-5	Тема 3. Міжнародно-правові засади протидії кіберзлочинності Перелік питань: 6. Будапештська конвенція 2001 р.: структура, матеріально-правові норми (розділ 1), процесуальні повноваження (розділ 2), міжнародне співробітництво (розділ 3). Україна ратифікувала Конвенцію у вересні 2005 року. Додатковий протокол щодо криміналізації расистських і ксенофобних дій (ратифікований Україною у 2006 р.). 7. Другий додатковий протокол, підписаний Україною 30 листопада 2022 року: пряме співробітництво з провайдерами, прискорене розкриття даних, гарантії захисту персональних даних. 8. Конвенція ООН проти кіберзлочинності, підписана 65 державами в Ханої у жовтні 2025 року: співвідношення з Будапештською конвенцією, дискусія щодо ризиків для прав людини. 9. Право ЄС у контексті євроінтеграції: Директива NIS2, Регламент про кіберстійкість, GDPR у частині повідомлень про витоки. 10. Таллінський посібник 2.0, суверенітет у кіберпросторі, поріг збройного нападу, атрибуція.	4		*Раз на тиждень*
Самостійна робота	Тема 3. Міжнародно-правові засади протидії кіберзлочинності Опрацювання тексту Конвенції про кіберзлочинність. Порівняння двох статей Конвенції з відповідними нормами КК України з висновком про повноту імплементації.			

Лабораторне заняття 4-5	Тема 3. Міжнародно-правові засади протидії кіберзлочинності *1.Порівняльна таблиця складів злочинів за ст. 2–10 Будапештської конвенції та відповідних статей КК України — виявлення прогалин імплементації.* *2. Аналіз ситуації: чи є конкретна кібероперація порушенням суверенітету, втручанням чи збройним нападом; аргументація на основі критеріїв Таллінського посібника.*	4		*Раз на тиждень*
Лекція 6	Тема 4. Кримінологічна характеристика кіберзлочинності 1. Стан, структура і динаміка кіберзлочинності в Україні за офіційною статистикою Офісу Генерального прокурора. 2. Латентність та її причини: небажання потерпілих заявляти, репутаційні втрати, транскордонність. 3. Класифікації: злочини проти комп'ютерних систем vs злочини, вчинені з використанням комп'ютерних систем. 4. Особа кіберзлочинця: типології, мотивація, вік. 5. Кіберзлочинність як бізнес-модель: crime-as-a-service, RaaS, партнерські програми, «дропи», відмивання через криптоактиви. 6. Віктимологічний аспект: чому соціальна інженерія працює.	2		*Раз на тиждень*
Самостійна робота	Тема 4. Кримінологічна характеристика кіберзлочинності в Україні Опрацювання річного звіту Департаменту кіберполіції та огляду НБУ щодо платіжного шахрайства за останній рік. Підготовка аналітичної довідки на одну сторінку.			
Лабораторне заняття 6	Тема 4. Кримінологічна характеристика кіберзлочинності *Робота зі статистичними даними: вивантажити показники за розділом XVI КК за кілька років, побудувати динаміку і сформулювати гіпотези щодо розриву між кількістю зареєстрованих проваджень та кількістю обвинувальних актів.*	2		*Раз на тиждень*
Лекція 7-8	Тема 5. Кримінальні правопорушення у сфері використання ЕОМ: розділ XVI КК України 1. Загальна характеристика розділу XVI, родовий об'єкт, предмет. 2. Ст. 361 — несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних,	4		*Раз на тиждень*

	інформаційно-комунікаційних систем, електронних комунікаційних мереж: об'єктивна сторона, момент закінчення, кваліфікуючі ознаки. 3. Ст. 361-1 — створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. Проблема dual-use: коли інструмент пентестера стає предметом злочину. 4. Ст. 361-2 — несанкціоновані збут або розповсюдження інформації з обмеженим доступом. 5. Ст. 362 — несанкціоновані дії з інформацією особою, яка має право доступу (інсайдер). 6. Ст. 363 — порушення правил експлуатації або порядку чи правил захисту інформації; ст. 363-1 — перешкоджання роботі шляхом масового розповсюдження повідомлень. 7. Суб'єктивна сторона, вік відповідальності, співучасть.			
Самостійна робота	Тема 5. Кримінальні правопорушення у сфері використання інформаційних систем (розділ XVI КК України) Опрацювання ст. 361–363-1 КК України у чинній редакції та постанови ККС ВС від 19.09.2024 у справі № 735/739/20. Складання таблиці елементів складу за кожною статтею розділу XVI.			
Лабораторне заняття 7-8	Тема 5. Кримінальні правопорушення у сфері використання ЕОМ: розділ XVI КК України *1.Кваліфікаційний практикум: 8–10 фабул, за кожною визначити статтю, частину, обґрунтовати кожну ознаку складу і вказати момент закінчення.* *2.Пошук у Єдиному державному реєстрі судових рішень вироку за заданою статтею, аналіз доказової бази.*	4		*Раз на тиждень*
Лекція 9-10	Тема 6. Суміжні склади: кібершахрайство, платіжні інструменти, кібертероризм, критична інфраструктура Перелік питань: 1. Ст. 190 КК — шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Розмежування зі ст. 361: коли фішинг є шахрайством, коли — втручанням, коли — сукупністю.	4		*Раз на тиждень*

	2. Ст. 200 КК — незаконні дії з документами на переказ, платіжними картками. Скімінг, кардинг, дроп-схеми. 3. Посягання на приватність: ст. 163 (порушення таємниці листування та інших повідомлень), ст. 182 (порушення недоторканності приватного життя). Незаконний доступ до персональних даних. 4. Ст. 301-1, 301-2 КК — протидія дитячій порнографії та сексуальній експлуатації дітей онлайн; ст. 156-1 — грумінг. 5. Кібертероризм і кібердиверсія: ст. 258, ст. 113 КК. Кібератаки на об'єкти критичної інфраструктури в умовах збройної агресії; співвідношення з воєнними злочинами (ст. 438 КК). 6. Порушення авторського права та суміжних прав в мережі (ст. 176 КК).			
Самостійна робота	Тема 6. Суміжні склади кримінальних правопорушень Опрацювання ст. 190, 200, 209, 255 КК України. Аналіз обвинувального акта у справі про шахрайський кол-центр із поясненням, чому застосовано сукупність статей.			
Лабораторне заняття 9-10	Тема 6. Суміжні склади: кібершахрайство, платіжні інструменти, кібертероризм, критична інфраструктура *Розмежувальні задачі: фабули на межі двох-трьох складів, де студент має обрати кваліфікацію та письмово аргументувати відмову від альтернативної. Складання схеми «атака → етапи → статті КК» для сценарію ransomware-атаки з ексфільтрацією даних та вимогою викупу.*	4		*Раз на тиждень*
Лекція 11	Тема 7. Юрисдикція, місце вчинення та транскордонний характер кіберзлочину Принципи дії закону про кримінальну відповідальність у просторі (ст. 6–8 КК) стосовно кіберзлочинів. Місце вчинення: місцезнаходження суб'єкта, обладнання, сервера, потерпілого? Конфлікт юрисдикцій і подвійна караність. Проблема «даних у хмарі»: територіальність зберігання, кейси транскордонного доступу. Роль VPN, Tor, анонімізації для атрибуції та доказування. Екстрадиція.	2		*Раз на тиждень*
Самостійна робота	Тема 7. Юрисдикція, місце вчинення та транскордонний характер кіберзлочину Опрацювання ст. 6–8 КК України. Аналіз			

	реальної справи про кол-центр, орієнтований на іноземних потерпілих, із визначенням застосовного права.			
Лабораторне заняття 11	Тема 7. Юрисдикція, місце вчинення та транскордонний характер кіберзлочину *Кейс із трьома-чотирма державами: визначити, які держави мають юрисдикцію, за яким принципом, і які колізії виникнуть; запропонувати механізм вирішення.*	2		*Раз на тиждень*
Лекція 12	Тема 8. Реагування на кіберінцидент: обов'язки суб'єктів та взаємодія з правоохоронними органами Життєвий цикл інциденту та точки, у яких виникають юридичні обов'язки. Обов'язкове повідомлення: кому, у які строки, у якій формі. Повідомлення про витік персональних даних. Момент, коли інцидент стає підставою для внесення відомостей до ЄРДР. Заява потерпілого: зміст, додатки, типові помилки. Що адміністратор системи має зробити і чого категорично не має робити у перші години, щоб не знищити сліди. Юридичні ризики «внутрішнього розслідування».	2		*Раз на тиждень*
Самостійна робота	Тема 8. Реагування на кіберінцидент: обов’язки суб’єктів та взаємодія з правоохоронними органами Опрацювання ст. 9-1 Закону № 2163-VIII та ст. 214 КПК України. Складання чек-листа першочергових дій відповідальної особи в перші три години після виявлення інциденту.			
Лабораторне заняття 12	Тема 8. Реагування на кіберінцидент: обов'язки суб'єктів та взаємодія з правоохоронними органами *За фабулою інциденту скласти пакет документів: внутрішній акт фіксації, повідомлення регулятору, заяву до Кіберполіції з переліком додатків.*	2		*Раз на тиждень*
Лекція 13-14	Тема 9. Цифрові докази у кримінальному провадженні Перелік питань: 1. Поняття та властивості доказу за КПК: належність, допустимість, достовірність. Місце електронної інформації в системі процесуальних джерел доказів. 2. Тимчасовий доступ до речей і документів; тимчасове вилучення та арешт майна. Обшук і особливості вилучення електронних носіїв: коли вилучається носій, а коли лише копіюється інформація.	4		*Раз на тиждень*

	3. Негласні слідчі (розшукові) дії: зняття інформації з електронних комунікаційних мереж (ст. 263 КПК), зняття інформації з електронних інформаційних систем (ст. 264 КПК); підстави та санкціонування. 4. Ланцюг збереження доказів (chain of custody), хешування, образи носіїв, робота з волатильними даними. 5. Експертиза: види комп'ютерно-технічних експертиз, коректна постановка питань експертові. 6. Типові підстави визнання цифрових доказів недопустимими у практиці судів.			
Самостійна робота	Тема 9. Цифрові докази у кримінальному провадженні Опрацювання ст. 84–94, 159–166, 234–236, 263–264 КПК України. Пошук в ЄДРСР та аналіз одного рішення, у якому вирішувалося питання допустимості цифрового доказу.			
Лабораторне заняття 13-14	Тема 9. Цифрові докази у кримінальному провадженні *1.Розбір реального вироку або ухвали, де цифровий доказ був визнаний недопустимим — встановити, на якому етапі допущено помилку та як її можна було уникнути.* *2.Формулювання переліку питань для комп'ютерно-технічної експертизи за заданою фабулою.*	4		*Раз на тиждень*
Лекція 15	Тема 10. Міжнародне співробітництво у розслідуванні кіберзлочинів Форми міжнародного співробітництва за розділом IX КПК: запит про правову допомогу, його реквізити та строки. Мережа контактних пунктів 24/7 за ст. 35 Будапештської конвенції. Термінове збереження даних (expedited preservation) як механізм, що випереджає формальний запит. Прямі запити до іноземних провайдерів: Google, Meta, Microsoft, їх політики розкриття та transparency reports. Спільні слідчі групи. Взаємодія з Європолом (ЕС3), Інтерполом, Євроюстом. Обмеження, зумовлені захистом персональних даних у ЄС.	2		*Раз на тиждень*
Самостійна робота	Тема 10. Міжнародне співробітництво у розслідуванні кіберзлочинів Опрацювання розділу IX КПК України та ст. 29–35 Конвенції про кіберзлочинність. Аналіз звіту прозорості одного великого постачальника послуг.			
Лабораторне заняття	Тема 10. Міжнародне співробітництво у розслідуванні кіберзлочинів	2		*Раз на тиждень*

15	*Складання проєкту запиту про термінове збереження даних та переліку відомостей, які реально можна отримати від конкретного провайдера, з посиланням на його опубліковану політику.*			
Лекція 16	Тема 11. Правові межі діяльності фахівця з кібербезпеки 1. Тестування на проникнення: чому усної згоди недостатньо. Обов'язкові елементи договору — scope, часові рамки, дозволені техніки, порядок дій при виявленні стороннього доступу, конфіденційність. Ризик кваліфікації за ст. 361 при виході за межі scope. 2. Bug bounty та safe harbour: правова природа публічної обіцянки винагороди, межі захисту дослідника. 3. Відповідальне розкриття вразливостей: узгоджені строки, ризики публікації PoC, ст. 361-1 щодо шкідливих засобів. 4. OSINT і межі законного збору інформації; персональні дані у відкритих джерелах. 5. Обробка персональних даних фахівцем з безпеки: мінімізація, законні підстави, логування та моніторинг працівників. 6. Професійна етика: конфлікт між обов'язком повідомити і обов'язком зберігати конфіденційність; свідчення у справі; whistleblowing. 7. Дисциплінарна, цивільна, адміністративна та кримінальна відповідальність — розмежування.	2		*Раз на тиждень*
Самостійна робота	Тема 11. Правові межі діяльності фахівця з кібербезпеки Опрацювання ч. 7 ст. 8 Закону № 2163-VIII та Закону України «Про захист персональних даних». Складання переліку обов’язкових умов договору на тестування на проникнення.			
Лабораторне заняття 16	Тема 11. Правові межі діяльності фахівця з кібербезпеки *1.Аналіз договору на проведення пентесту.* *2.Етична дилема з обґрунтуванням рішення та посиланням на норми.*	2		*Раз на тиждень*

5. Види і зміст контрольних заходів

Вид заняття/роботи	Вид поточного контрольного заходу	Зміст контрольного заходу*	Критерії оцінювання та термін виконання*	Усього балів
Поточний контроль				

Лабораторне заняття №1-16	Опитування	З переліку питань до лабораторного заняття та самостійної роботи;	Самостійність, правильність, повнота — 1 бал Неправильна – 0 балів	**1**
	тест	десять питань з переліку питань до лабораторного заняття та самостійної роботи	Кількість правильних відповідей (1 питання – **0,1** балів) – усього 10 питань	**1**
	вирішення практичного завдання	фабули яких містяться на сторінці дисципліни в Moodle	Самостійність, правильність, повнота, рівень засвоєння навчального матеріалу: Правильна повна **– 1** бал	**1**
Разом за 16 лабораторних занять			16 занять × 3 бали	48
	Модульне тестування № 1	Тестування в СЕЗН Moodle	За матеріалами змістового модуля 1 (теми 1–3). 20 рівнозначних питань, правильна відповідь — 0,2 бала	4
	Модульне тестування № 2	Тестування в СЕЗН Moodle	За матеріалами змістового модуля 2 (теми 4–7). 20 рівнозначних питань, правильна відповідь — 0,2 бала	4
	Модульне тестування № 3	Тестування в СЕЗН Moodle	За матеріалами змістового модуля 3 (теми 8–11). 20 рівнозначних питань, правильна відповідь — 0,2 бала	4
Разом за модульні тестування			3 × 4 бали	12
Усього за поточний контроль				**60**
Підсумков. семестр. контроль	Тестування	Тестові питання за матеріалами всіх тем курсу. Кількість рівнозначних питань — 40; правильна відповідь оцінюється у 0,5 бала	20	**40**
	Розв’язання кейсу	Кваліфікація діяння за фабулою з	20	

		обґрунтуванням кожної ознаки складу, зазначенням норми та розмежуванням із суміжними складами		
Усього				**100**

Критерії оцінювання кейсу

— 18–20 балів — кваліфікацію визначено правильно, обґрунтовано кожну ознаку складу, наведено норму з точним посиланням, аргументовано відмову від альтернативної кваліфікації.

— 14–17 балів — кваліфікація правильна, обґрунтування повне, але бракує розмежування із суміжними складами.

— 10–13 балів — кваліфікація правильна, обґрунтування фрагментарне або посилання на норми неточні.

— 5–9 балів — кваліфікацію визначено частково правильно, наявні суттєві помилки в обґрунтуванні.

— 1–4 бали — кваліфікацію визначено неправильно.

— 0 балів — відповідь відсутня.

РОЗПОДІЛ БАЛІВ ПОТОЧНОГО ТА ПІДСУМКОВОГО КОНТРОЛЮ

Шкала оцінювання ЗНУ: національна та ECTS

За шкалою ECTS	За шкалою університету	За національною шкалою	
		Екзамен	Залік
A	90 – 100 (відмінно)	5 (відмінно)	Зараховано
B	85 – 89 (дуже добре)	4 (добре)	
C	75 – 84 (добре)		
D	70 – 74 (задовільно)	3 (задовільно)	
E	60 – 69 (достатньо)		
FX	35 – 59 (незадовільно – з можливістю повторного складання)	2 (незадовільно)	Не зараховано
F	1 – 34 (незадовільно – з обов'язковим повторним курсом)		

6. Основні навчальні ресурси: Рекомендована література

Нормативно-правові акти:

1. Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III. URL : https://zakon.rada.gov.ua/laws/show/2341-14.
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021
3. Про інформацію: Закон України від 02.10.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

4. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI URL : https://zakon.rada.gov.ua/laws/show/2297-17
5. Про електронні довірчі послуги: Закон України від 05.10.2017 р. № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL : https://zakon.rada.gov.ua/laws/show/2163-19#Text
7. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII URL : https://zakon.rada.gov.ua/laws/show/2469-19#Text
8. Про кіберзлочинність: Конвенція ратифікована із застереженнями і заявами Законом № 2824- IVвід 07.09.2005, URL : https://zakon.rada.gov.ua/laws/show/994_575#Text
9. Про критичну інфраструктуру: Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20
10.План заходів на 2025 рік з реалізації Стратегії кібербезпеки України. Затверджений розпорядженням Кабінету Міністрів України від 7 березня 2025 р. № 204-р. https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text
11. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24.03.22 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-IX#Text
12.Про внесення змін до Кримінального процесуального кодексу України щодо удосконалення порядку здійснення кримінального провадження в умовах воєнного стану: Закон України від 14.04.22 р. № 2201-IX. URL: https://zakon.rada.gov.ua/laws/show/2201-20#Text
13.Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 27.03.2025 № 4336-IX.
13. Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Постанова КМ № 299 від 4 квітня 2023 року. URL: https://zakon.rada.gov.ua/laws/show/299-2023-п#Text
14. Про затвердження Положення про організаційно-технічну модель кіберзахисту: постанова Кабінету Міністрів України від 29.12.2021 р. № 1426 (у редакції від 26.12.2024, постанова КМУ № 1468). URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п
15. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19.06.2019 р. № 518 (у редакції постанови КМУ від 13.11.2025 р. № 1470). URL: https://zakon.rada.gov.ua/laws/show/518-2019-п
16. Положення про Департамент кіберполіції Національної поліції України, затверджене наказом Національної поліції України № 85 : від 10.11.2015, в редакції наказу Національної поліції України від 07 листопада 2019 року № 1136 «Про внесення змін до Положення про Департамент кіберполіції Національної поліції України». К. : Національна поліція України, 2019. 11 с.
17. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. Офіційний сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text
18. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17
19. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27.03.2025 р. № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20
20. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20
21. Про захист інформації в інформаційно-комунікаційних системах: Закон України від

05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80
22. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.2016 р. № 242/2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016

Підручники, навчальні посібники та ін.:

1. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. Brussels, 7.2.2013. Join (2013) URL: http://www.enisa.europa.eu.
2. Nizovtsev, Yuriy; Parfylo, Oleg; Barabash, Olha; Kyrenko, Sergij; Smetanina, Nataliia. Mechanisms of money laundering obtained from cybercrime: the legal aspect. *Journal of Money Laundering Control.* Volume 25, Issue 2, Pages 297–305. 21 April 2022. https://www.emerald.com/insight/content/doi/10.1108/JMLC-02-2021-0015/full/html.
3. Апетик А. М., Дьякова А. Д., Ковальова О. В., Козлова А. Г., Манжай О. В., Мердова О. М., Мілорадова Н. А., Пашко Н. А., Юртаєва К. В., Філоненко В. Підготовка поліцейських підрозділів превентивної діяльності, слідства, та дізнання, кіберполіцейських з питань убезпечення дітей у кіберпросторі: навчально-методичний посібник / за заг. ред. Т. В. Журавель, О. В. Ковальової. Київ: ГО Волонтер, 2023.
4. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2014. № 4. С. 27-30.
5. Бабенко А.М. Кіберзлочинність як чинник негативного впливу на криміногенну ситуацію у регіонах. *Безпека інформації*. 2013. Т. 19. № 2. С. 112-117.
6. Бєлкін Л.М., Юринець Ю.Л., Бєлкін М.Л., Криволап Є.В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law»*. 2022. № 3 (64). С. 78–86.
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. Бондаренко О. С., Рєпін Д. А. Кіберзлочинність в Україні : причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246– 248.
9. Бугера О.І. Загальна кримінологічна характеристика мережі Інтернет та запобігання злочинності. *Право і суспільство*. 2018. № 5. С. 177–181.
10. Вейц А.М. Особливості розслідування кіберзлочинів, вчинених у військовому середовищі. *Інформація і право*. 2024. № 4 (51). С. 233-242.
11. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. К., 2017. 148 с. Манжай О. В. Особливості огляду засобів комп'ютерної техніки. *Вісник Харківського національного університету внутрішніх справ.* 2016. № 3 (74). С. 111-120.
12. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і Безпека.* 2011. № 4. С. 107-112.
13. Воронов І.О. Криміналістичний аналіз кримінальних правопорушень у сфері використання комп'ютерів. *Юридичний бюлетень*. 2022. № 4. С. 180-186.
14. Галак М. Кіберзлочини: Методи, суб'єкти та вимоги для доказу. К.: Видавництво "Юрінком Інтер", 2018. 224 с.
15. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права*. 2014. № 4. С. 312-317.

16. Гуржій С.В. Засади інституціонально-функціонального забезпечення кібербезпеки в сучасних умовах. Інформація і право. 2021. № 2 (37). С. 103-104.
17. Гуцалюк М.В. Особливості протидії кіберзлочинності під час воєнного стану. *Інформація і право.* 2023. № 3 (46). С. 108-117.
18. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі «Даркнет». *Інформація і право*. 2018. № 3 (26). С. 102-108.
19. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1(28). С. 118-128.
20. Діброва Т.А., Пісенко Д.О., Сметаніна Н.В. Кіберзлочинність та кібершахрайство в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2022. № 11. С.546-549.
21. Єрема М., Борисенко А., Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. Офіційний сайт «LIGAЗакон». URL: https://jurliga.ligazakon.net/ analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix
22. Забара І. М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. *Часопис Академії адвокатури України*. 2012. № 17. С. 1-68.
23. Іванченко О.І. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 172-177.
24. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. *Актуальні проблеми міжнародних відносин*. 2015. Випуск 126 (частина ІІ). С. 77-90.
25. Кирилюк О. В. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. Актуальні проблеми міжнародних відносин. 2015. Випуск 126 (частина ІІ). С. 77-9016.
26. Кіберзлочинність та електронні докази: навч. посіб. / Б.М. Головкін, О.І. Денькович, В.В. Луцик, Д.М. Цехан. Львів: ЛНУ ім. Івана Франка, 2022. 298 с. URL: https://nlu.edu.ua/wpcontent/uploads/2023/09/cybercrime-and-digital-evidence.pdf
27. Кіберзлочинність та електронні докази. Cybercrime and digital evidence : навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельце. Львів. Львівськ. Ун-т ім. Івана Франка. 2022. 298 с.
28. Климчук О. О. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 3. С. 75–83.
29. Колосовський В.Ю. Сучасний стан кібербезпеки україни в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402-405.
30. Коршенко В.А. Судова телекомунікаційна експертиза як джерело доказів під час розслідування кіберзлочинів. *National law journal: theory and practice*. 2017. № 2 (24). С. 192-194.
31. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: 12.00.08 / Харків. нац. ун-т внутр. справ. Харків, 2016. 16 с.
32. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України*. 2018. № 2 (19). С. 155-166.
33. Красніков С.А. Кібергігієна як чинник запобігання кіберзагрозам. *Нове українське право*. 2024. Вип. 6. С. 57-62.
34. Кравцова М.О. Фактори детермінації кіберзлочинності в сучасній кримінологічній теорії. *Юридичний науковий електронний журнал*. 2014. № 5. С. 110–113.
35. Кримінологія: підручник / Б. М. Головкін, В. В. Голіна, О.Ю. Шостко та ін; за ред. Б. М.

Головкіна. Харків : Право, 2020. 384 с.

36. Манжай О. В. Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів. *Протидія кіберзагрозам та торгівлі людьми* (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2019. С. 178–180.
37. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і Безпека.* 2015. № 2. С. 107-113.
38. Методика розслідування створення та поширення контенту з вмістом дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій: науково-методичні рекомендації / С.О. Книженко, О.В. Салманов, О.В. Манжай, В.В. Кікінчук, В.В. Романюк. Х. : ХНУВС, 2022. 68 с.
39. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304-307.
40. Носов В. В., Манжай І. А. Окремі аспекти аналізу криптовалютних трансакцій під час попередження та розслідування злочинів. *Право і безпека*. 2021. № 1(80). С. 93-100.
41. Носов В. В., Манжай О. В., Панченко Є. В. Аналіз етеріум-трансакцій під час попередження та розслідування кримінальних правопорушень. *Право і безпека*. 2022. № 4 (87). С. 108-124.
42. Ньюман М. Історія кіберзлочинності: Від комп'ютерних вайрусів до кібервійн. К.: Видавництво «Наукова думка». 2019. 368 с.
43. Орлов О.В., Онищенко Ю. М. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. *Теорія та практика державного управління*. 2013. Вип. 4 (43). С. 1-610.
44. Орловський Б.М. Детермінанти кіберзлочинності у кримінологічній науці. *Правовий вимір конституційної та кримінальної юрисдикції в Україні та світі.* Одеський національний університет імені Мечникова. 2024. С. 137-139.
45. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
46. Особливості розслідування кримінальних правопорушень, пов'язаних із доведенням до самогубства неповнолітніх із використанням соціальних мереж в Інтернеті: науково-методичні рекомендації / О.В. Манжай, В.В. Кікінчук, В.В. Корнієнко, В.С. Гнатенко, О.М. Рвачов. Х. : ХНУВС, 2022. 57 с.
47. Пивоваров В. В., С. Ю. Лисенко. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3. Ч. 2. С. 177–182.
48. Пошук та фіксація фактичних даних про протиправні діяння, які вчинені з використанням інформаційно-телекомунікаційних систем або технологій при розслідуванні фактів збуту наркотичних засобів: науково-методичні рекомендації / В.В. Кікінчук, Т.П. Матюшкова, А.В. Піддубна, О.В. Манжай, В.В. Носов. Х. : ХНУВС, 2022. 69 с.
49. Прикладний кримінальний аналіз на базі інформаційно-аналітичної системи «RICAS»: методичні рекомендації щодо аналітичної діяльності та кримінального аналізу на базі інформаційно-аналітичної системи «RICAS». Харків : Юрайт, 2018. 92 с.
50. Розвиток навичок кібергігієни. URL: https://ua.issp.com/_files/ugd/2d3fc0_8dc46933eb064737aea6b2bda0b01821.pdf
51. Романенко Т. Способи вчинення шахрайств із використанням електронно-обчислювальної техніки як елемент їх криміналістичної характеристики. *Knowledge, Education, Law, Management.* 2020. № 3 (31), vol. 2. С. 144-148.
52. Саєнко М.І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2021. Випуск 64. С. 386-391.
53. Салманов О.В. Кіберзлочинність і протидія їй в умовах воєнного стану в україні. Злочинність

і протидія їй в умовах війни та у повоєнній перспективі: міждисциплінарна панорама. Вінниця, 2024. С. 313-318.

54. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса. 2020. 112 с.
55. Самойленко О. А. Діяльність правоохоронних органів у протидії кіберзлочинності [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса. 2020. 133 с.
56. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса: ТЕС, 2020. 372 с.
57. Самойленко О.А. Виявлення та розслідування кіберзлочинів. Одеса, 2020.112 с.
58. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Актуальна юриспруденція. зб. матеріалів інтернет-конференції. Київ. 2018. С.77-80.
59. Сметаніна Н. В. Національний і міжнародний досвід визначення та розрахунку ціни кіберзлочинності. *Міжнародні стандарти з кібербезпеки та їх застосування в Україні* : матеріали «круглого столу» (м. Харків, 19 квіт. 2016 р.). Харків, 2016. С. 59–61.
60. Спроби впровадження міжнародного контролю за діяльністю в Інтернеті під егідою ООН: нові можливості реалізації Україною інформаційного суверенітету: аналітична записка / Національний інститут стратегічних досліджень. URL: http://www.niss.gov.ua/articles/1093/
61. Таволжанський О. В. Кримінологічні аспекти кіберзлочинності у сучасних умовах. *Журнал східноєвропейського права.* 2016. №. 31. С. 80– 86.
62. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія: Право.* 2018. Вип. 6. С. 154–163.
63. Таволжанський О. В. Питання визначення кіберзлочинності в умовах розбудови інформаційного суспільства. *Журнал східноєвропейського права.* 2017. Вип. 45. С. 97-103.
64. Федушко С. Сучасні підходи до дослідження кібербезпеки та кібергігієни в умовах цифрової трансформації суспільства. *Вісник Хмельницького національного університету*. 2023. № 3 (321). С. 210–213.
65. Федюк В.В. Кримінальна відповідальності за кібершпигунство: проблеми нормативної регламентації: тези доповідей VI Міжнародної науково-практичної конференції Кримінально-правова охорона інформаційної безпеки, м. Харків 12 трав. 2022 р. Харків: Право. С. 260-263.
66. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2. С. 162–169
67. Харитоненко І.О. Причини та умови вчинення кіберзлочинів. *Економіка. Фінанси. Право*. 2023. № 7. С.67-72.
68. Хілько В. І. Кіберзахист: Теорія і практика. К.: Видавництво "Логос", 2020. 288 с.
69. Холлінс Т. Ж. Кіберзлочинність і кібербезпека: Основи, виклики та рішення. Дніпро: Видавництво «Ліга-Прес», 2021. 416 с.
70. Шестак Я. І. Кібергігієна у інформаційному просторі в умовах воєнного стану. Інформаційна безпека та комп'ютерні технології. Ценральноукраїнський національний технічний університет, Кропивницький, 2022. С. 5–6. 14.

Інтернет-ресурси:

1. URL: http://www.president.gov.ua/ - Офіційний сайт Президента України;
2. URL: http://www.rada.gov.ua/ – Офіційний портал Верховної ради України;
3. URL: http://www.kmu.gov.ua/ – Офіційний портал Кабінету міністрів України;
4. URL: http://vkksu.gov.ua/ – Офіційний сайт Вищої кваліфікаційної комісії суддів України;
5. URL: http://reyestr.court.gov.ua – Офіційний сайт єдиного державного реєстру судових рішень

України";
6. URL: http://www.rada.kiev.ua/laws/pravo/all/sites.htm – перелік серверів державних органів на сайті Верховної Ради України;
7. URL: https://supreme.court.gov.ua/supreme/ – Офіційний сайт Верховного Суду;
8. URL: http://www.minjust.gov.ua/ – Офіційний сайт Міністерства юстиції України;
9. URL: https://cyberpolice.gov.ua/news/zvit-pro-rezultaty-roboty-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-4792/ - Офіційний сайт Департаменту кіберполіції України
10. URL: http://anticyber.com.ua - Кіберзлочинність: проблеми боротьби і прогнози. Антикібер Національне антикорупційне бюро.

7. Регуляції і політики курсу

Відвідування занять. Регуляція пропусків

Заняття проводяться дистанційно у Zoom. Відвідування лекційних і лабораторних занять є обов'язковим. Здобувач приєднується до конференції під власним прізвищем та ім'ям і вмикає камеру на час опитування, захисту завдання та контрольних заходів. Якість участі оцінюється за критеріями: участь у дискусіях, аналіз правових ситуацій, виконання завдань у межах заняття. Присутність у конференції без участі в роботі не враховується як повноцінна участь. Технічні проблеми зі зв'язком не є підставою для незарахування заняття, якщо здобувач повідомив про них викладача та відпрацював завдання у встановлений строк.

Завдання лабораторних робіт виконуються у встановлені строки. Несвоєчасне подання без поважних причин тягне зниження оцінки. У разі об'єктивних обставин здобувач має завчасно повідомити викладача та погодити нові строки.

Відпрацювання пропущених занять

Пропущені заняття підлягають обов'язковому відпрацюванню у встановлений викладачем термін — у формі індивідуального опитування, письмової роботи або виконання завдання лабораторної роботи. Без відпрацювання здобувач не допускається до підсумкового контролю.

Порядок складання екзамену

Екзамен складається дистанційно: тестування виконується в СЕЗН ЗНУ (Moodle), розв'язання кейсу — під час відеоконференції Zoom з увімкненою камерою. Участь здобувача в конференції у визначений час є обов'язковою. У разі неможливості з поважних причин, підтверджених документально, здобувач зобов'язаний повідомити про це не пізніше ніж за добу; йому призначається індивідуальний день складання. Відсутність технічної можливості (несправність обладнання, відсутність зв'язку) не є поважною причиною, якщо про неї не повідомлено завчасно.

Політика академічної доброчесності

Усі письмові роботи перевіряються на наявність плагіату за допомогою спеціалізованого програмного забезпечення StrikePlagiarism. Плагіатом вважається копіювання чужої роботи та оприлюднення результату під своїм іменем, створення суміші власного та запозиченого тексту без

належного цитування, а також перефразування чужої праці без згадування автора. Роботи з ознаками плагіату не приймаються.

Специфічна вимога цієї дисципліни: посилання на нормативно-правовий акт має містити повні реквізити — структурний елемент, назву акта, дату і номер, а також зазначення редакції, чинної на дату аналізованих подій. Посилання на реферативні бази та Wikipedia є неприпустимими. Використання генеративних систем штучного інтелекту для формулювання правових висновків без перевірки за першоджерелом розглядається як недобросовісне виконання завдання.

Робота з персональними даними в судових рішеннях

Тексти судових рішень у Єдиному державному реєстрі є знеособленими. Здобувачам забороняється вчиняти дії, спрямовані на встановлення особи учасників судового процесу за непрямими ознаками. Порушення цієї вимоги є підставою для незарахування роботи.

Використання комп'ютерів і телефонів на занятті

Заняття проводяться за комп'ютером, і робота з нормативно-правовими базами та реєстрами є їх основним змістом. Під час контрольних заходів дозволено користуватися лише тими ресурсами, які прямо визначені викладачем у завданні; використання сторонньої допомоги, обмін відповідями та робота з чужого облікового запису розглядаються як порушення академічної доброчесності, а роботу буде анульовано. Під час тестування в Moodle здобувач перебуває у конференції Zoom з увімкненою камерою.

Комунікація

Основними платформами є СЕЗН ЗНУ (Moodle) для матеріалів, завдань і тестування та Zoom для проведення занять і консультацій. Важливі повідомлення розміщуються на форумі курсу; для персональних запитів використовується сервіс приватних повідомлень Moodle. Посилання на конференції публікуються на сторінці дисципліни завчасно.

Визнання результатів неформальної/інформальної освіти

Процедура врахування результатів, отриманих здобувачем за рахунок неформальної/інформальної освіти визначена у Положенні Запорізького національного університету про порядок визнання результатів навчання, здобутих шляхом неформальної та/або інформальної освіти від 29.06.2022 р. №154 (URL: http://surl.li/xogolg).

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ НА 2026-2027 н.р. доступний за адресою: http://surl.li/afeagu

НАВЧАННЯ ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОСВІТИ. Перевірка набутих студентами знань, навичок та вмінь є невід'ємною складовою системи забезпечення якості освіти і проводиться відповідно до Положення про організацію та методику проведення поточного та підсумкового семестрового контролю навчання студентів ЗНУ: https://tinyurl.com/y9tve4lk.

ПОВТОРНЕ ВИВЧЕННЯ ДИСЦИПЛІН. Наявність академічної заборгованості до 6 навчальних дисциплін (у тому числі проходження практики чи виконання курсової роботи) за результатами однієї екзаменаційної сесії є підставою для надання студенту права на повторне вивчення зазначених навчальних дисциплін. Процедура повторного вивчення визначається Положенням про

порядок повторного вивчення навчальних дисциплін та повторного навчання у ЗНУ: https://tinyurl.com/y9pkmmp5.

ВИРІШЕННЯ КОНФЛІКТІВ. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, регламентуються Положенням про порядок і процедури вирішення конфліктних ситуацій у ЗНУ: https://tinyurl.com/57wha734.
Конфліктні ситуації, що виникають у сфері стипендіального забезпечення здобувачів вищої освіти, вирішуються стипендіальними комісіями факультетів, коледжів та університету в межах їх повноважень, відповідно до: Положення про порядок призначення і виплати академічних стипендій у ЗНУ: https://tinyurl.com/yd6bq6p9; Положення про призначення та виплату соціальних стипендій у ЗНУ: https://tinyurl.com/y9r5dpwh.

ПСИХОЛОГІЧНА ДОПОМОГА. Телефон довіри практичного психолога **Марті Ірини Вадимівни** (061) 228-15-84, (099) 253-78-73 (щоденно з 9 до 21).

УПОВНОВАЖЕНА ОСОБА З ПИТАНЬ ЗАПОБІГАННЯ ТА ВИЯВЛЕННЯ КОРУПЦІЇ Запорізького національного університету: **Банах Віктор Аркадійович**
Електронна адреса: v_banakh@znu.edu.ua
Гаряча лінія: тел. (061) 227-12-76, факс 227-12-88

РІВНІ МОЖЛИВОСТІ ТА ІНКЛЮЗИВНЕ ОСВІТНЄ СЕРЕДОВИЩЕ. Центральні входи усіх навчальних корпусів ЗНУ обладнані пандусами для забезпечення доступу осіб з інвалідністю та інших маломобільних груп населення. Допомога для здійснення входу у разі потреби надається черговими охоронцями навчальних корпусів. Спеціалізована допомога: (061) 228-75-11 (начальник охорони). Порядок супроводу (надання допомоги) осіб з інвалідністю та інших маломобільних груп населення у ЗНУ: https://tinyurl.com/ydhcsagx.

РЕСУРСИ ДЛЯ НАВЧАННЯ

НАУКОВА БІБЛІОТЕКА: http://library.znu.edu.ua. Графік роботи абонементів: понеділок-п`ятниця з 08.00 до 16.00; вихідні дні: субота і неділя.

СИСТЕМА ЕЛЕКТРОННОГО ЗАБЕЗПЕЧЕННЯ НАВЧАННЯ ЗАПОРІЗЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ (СЕЗН ЗНУ): https://moodle.znu.edu.ua.
Посилання для відновлення паролю: https://moodle.znu.edu.ua/mod/page/view.php?id=133015.

ЦЕНТР ІНТЕНСИВНОГО ВИВЧЕННЯ ІНОЗЕМНИХ МОВ: http://sites.znu.edu.ua/child-advance/