ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ЮРИДИЧНИЙ ФАКУЛЬТЕТ

ЗАТВЕРДЖУЮ
В.о. декана юридичного факультету
_____ Т.О. Коломоєць
«20» 10 2025

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРБЕЗПЕКА ТА УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РЕСУРСАМИ

підготовки бакалаврів
денної та заочної форми здобуття освіти
Освітньо-професійна програма – Правоохоронна діяльність
Спеціальності – 262 Правоохоронна діяльність
Галузь знань – 26 Цивільна безпека

ВИКЛАДАЧ: Рябчинська Олена Павлівна, доктор юридичних наук, професор, професор кафедри кримінального права та правоохоронної діяльності

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

Протокол № 3 від 24.10.2025 р.
В.о. завідувача кафедри кримінального. права та правоохоронної діяльності
_____ Р.В.Бараннік

Погоджено:
Гарант освітньої програми
_____ О.В. Мельковський

2025 рік

ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Силабус навчальної дисципліни
Кібербезпека та управління інформаційними ресурсами

Зв'язок з викладачем (викладачами):
Сезн ЗНУ повідомлення: https://moodle.znu.edu.ua/course/view.php?id=18045
Телефон: *(066) 720-26-28*
E-mail: *ryabchinskaya.olena@gmail.com*
Кафедра: *кримінального права та правоохоронної діяльності, V корпус, ауд.106*

1. Опис навчальної дисципліни

Навчальна дисципліна **«Кібербезпека та управління інформаційними ресурсами»** забезпечує формування цілісного уявлення про міжнародно-правові та національні засади охорони кіберпростору, забезпечення кібербезпеки та нормативно-правові основи управління інформаційними ресурсами.

Під час вивчення дисципліни здобувачі опановують міжнародну та національну нормативно-правову базу, що регламентує діяльність суб'єктів забезпечення кібербезпеки та порядок управління державними інформаційними ресурсами, а також методичні рекомендації Держспецзв'язку (CERT-UA, CSIRT) щодо реагування на інциденти, захисту АСУ/ОТ та збору статистики кібератак. Особлива увага приділяється принципам адміністрування, моніторингу та аудиту інформаційних систем, порядку роботи з інформацією з обмеженим доступом, а також кваліфікації адміністративної та кримінальної відповідальності за правопорушення у сфері використання ЕОМ, автоматизованих систем і мереж електрозв'язку. Окрім того, розглядаються сучасні технічні засоби та правові стратегії запобігання кіберзлочинності для захисту об'єктів критичної інфраструктури та національного інформаційного простору.

Пререквізити: «Вступ до спеціальності», «Спеціальна техніка у правоохоронній діяльності. Профілактика у діяльності правоохоронних органів», «Спеціальна підготовка та оперативна тактика у діяльності правоохоронців», «Професійно-психологічна підготовка правоохоронця».

Постреквізити: «Криміналістика», «Правове регулювання використання та захисту інформації», «Оперативно-розшукова діяльність», «Міжнародна безпека, протидія тероризму, незаконній міграції та торгівлі людьми», «Теорія кваліфікації кримінальних та адміністративних правопорушень».

Навчальна дисципліна спрямована на розвиток поглиблених знань та умінь, необхідних для розв'язання складних задач дослідницького та/або інноваційного характеру у сфері кібербезпеки та протидії кіберзлочинності, а також управління інформаційними ресурсами. Програма курсу розроблена відповідно до вимог освітніх стандартів, сучасного законодавства та міжнародних зобов'язань України у сфері запобігання злочинам та забезпечення прав людини.

Опанування основними положення протидії кіберзлочинності необхідні таких фахівцям в сфері кібербезпеки та захисту інформації як:
Дізнавач (сфера кібербезпеки та захисту інформації)
Експерт-криміналіст (сфера кібербезпеки та захисту інформації)
Експерт-криміналіст судової експертизи (сфера кібербезпеки та захисту інформації)
Слідчий з кіберзлочинів (згідно ДК 003:2010)

Мета вивчення дисципліни: Формування у здобувачів системних знань та практичних навичок щодо правового забезпечення кібербезпеки, ефективного управління інформаційними ресурсами, а також оволодіння інструментарієм запобігання, виявлення та припинення кіберзлочинів для захисту інтересів особи, суспільства та держави, зокрема об'єктів критичної інфраструктури в умовах воєнного стану.

Завдання дисципліни:

Теоретичні: засвоїти правові засади охорони кіберпростору як складової національної безпеки та зрозуміти архітектуру державної системи кіберзахисту;

Управлінські: навчитися організовувати заходи щодо дотримання режиму секретності, захисту інформації з обмеженим доступом та ефективного використання міжвідомчих інформаційно-пошукових систем;
Аналітичні: розвинути здатність критично аналізувати міжнародне та національне законодавство, встановлювати причинно-наслідкові зв'язки у правових явищах та здійснювати пошук інформації для професійних завдань;
Практико-оперативні: оволодіти методикою використання спеціальної техніки, цифрового зв'язку та технологій захисту даних для протидії нелегальній міграції, тероризму та іншим загрозам;
Профілактичні: навчитися здійснювати превентивну діяльність (зокрема у молодіжному середовищі) для запобігання радикалізації та утвердження патріотичних цінностей через цифрові канали комунікації;
Спеціальні: сформувати навички забезпечення правопорядку та життєстійкості громад в умовах надзвичайних ситуацій, воєнного стану та під час охорони об'єктів критичної інфраструктури.

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	26	6
Семінарські / Практичні / Лабораторні заняття	26	6
Самостійна робота	68	108
Консультації	*особисті – вівторок з 15:00 до 16:00, V корпус, ауд. 106;* *дистанційні – ZOOM, за попередньою домовленістю.* *Запис на консультації: Moodle (приватні повідомлення)*	
Вид підсумкового семестрового контролю:	**залік**	
Посилання на електронний курс у СЕЗН ЗНУ (платформа Moodle)	https://moodle.znu.edu.ua/course/view.php?id=18045	

2. Методи досягнення запланованих освітньою програмою компетентностей і результатів навчання

Компетентності/ результати навчання	**Методи навчання**	**Форми і методи оцінювання**
1	***2***	***3***

ЗК1. Здатність застосовувати знання у практичних ситуаціях. **ЗК2.** Знання та розуміння предметної області та розуміння професійної діяльності. **ЗК4.** Здатність використовувати інформаційні та комунікаційні технології. **ЗК5.** Здатність вчитися і оволодівати сучасними знаннями. **ЗК8.** Здатність приймати обґрунтовані рішення **ЗК11.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя/ **СК2.** Здатність здійснювати нагляд (контроль) за додержанням вимог законодавства у сфері правоохоронної діяльності. **СК3.** Здатність до критичного мислення та системного аналізу правових явищ. **СК4.** Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел. **СК5.** Здатність визначати придатні для юридичного аналізу факти, систематизувати одержані результати, встановлювати причинно-наслідкові зв'язки, формулювати аргументовані висновки та рекомендації. **СК6.** Здатність у межах своєї компетенції забезпечувати законність та правопорядок, безпеку особи та суспільства, протидіяти нелегальній (незаконній) міграції, тероризму та торгівлі людьми, незаконному обігу наркотичних засобів, психотропних речовин, їх аналогів чи прекурсорів. **СК7.** Здатність у межах своєї компетенції ефективно забезпечувати публічну (громадську) безпеку та порядок, у тому числі під час масових правопорушень, запобігати та протидіяти домашньому насильству. **СК8.** Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту	Методи аналізу та рефлексії: кейс-метод, стратегічний аналіз. Практичні методи: виконання тестових завдань, розв'язування кейсів (задач), тощо. Репродуктивні методи (лекція, пояснення, робота з методичними матеріалами); наочні методи (демонстрації та ілюстрації: схеми); метод проблемного викладу (постановка проблем і розкриття доказового шляху їхнього вирішення); дискусійні методи; Метод навчання з використанням Інтернет-технологій (електронне навчання); науково-дослідний (частково пошуковий) метод. Самостійна робота. Консультації (зворотний зв'язок).	Оцінювання здійснюється за накопичувальною системою та включає: Поточний контроль**:** оцінювання результатів практичних занять (вирішення кейсів, робота в малих групах, опитування тощо). Поточне оцінювання здійснюється з метою стимулювати систематичну роботу та відпрацювання практичних навичок. Рефлексивний компонент (оцінюється за здатність студента до самоаналізу. Оцінюється не наявність "правильної" відповіді, а повнота аргументації, критичне ставлення до власних результатів та готовність до корекції навчальної траєкторії Підсумковий контроль: залік (підсумковий тест)

прав і свобод людини, власності, суспільних відносин від протиправних посягань. **СК9.** Здатність надавати правоохоронні послуги. **СК16.** Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури. **СК17.** Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом. **СК18.** Здатність вживати заходів з метою запобігання, виявлення та припинення кримінальних та адміністративних правопорушень, усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення правопорушення. **СК20.** Здатність забезпечувати публічну безпеку та правопорядок в умовах воєнного стану та надзвичайних ситуацій з дотриманням прав і свобод людини, а також сприяти життєстійкості громад і повоєнній відбудові прифронтових територій. **СК21.** Здатність здійснювати превентивну діяльність щодо запобігання правопорушенням у молодіжному середовищі з використанням інструментів державної молодіжної політики та професійної комунікації. **РН8.** Здійснювати пошук інформації у доступних джерелах, аналізувати і оцінювати її для повного та всебічного встановлення обставин, необхідних для виконання професійних завдань. **РН9.** Використовувати інформаційно-комунікаційні системи та інші інформаційні ресурси, у тому числі ті, що мають технічний та криптографічний захист, поштовий зв'язок спеціального призначення, фельд'єгерський зв'язок, системи цифрового зв'язку суб'єктів сектору безпеки і оборони з метою виконання професійних завдань у сфері правоохоронної діяльності. **РН14.** Здійснювати пошук та аналіз новітньої інформації у сфері правоохоронної діяльності, мати навички саморозвитку та самоосвіти протягом життя, підвищення професійної майстерності, вивчення та використання передового досвіду у сфері правоохоронної діяльності. **РН17.** Використовувати методи та засоби забезпечення публічної (громадської) безпеки	Симуляційне моделювання інцидентів: відпрацювання алгоритмів захисту об'єктів критичної інфраструктури та реагування на кіберзагрози в умовах воєнного стану Інтерактивні кейс-студії: аналіз реальних правопорушень у цифровій сфері (витоки даних, тероризм, наркоторгівля) для	

та порядку, протидії злочинності, дотримуватися прав і свобод людини і громадянина, здійснювати заходи щодо попередження та припинення нелегальної (незаконної) міграції та інших загроз національній безпеці держави. **РН18.** Застосовувати вогнепальну зброю та спеціальні засоби (штатне та бойове озброєння), фізичну силу; інформаційні системи та технології, технології захисту даних, методи обробки, накопичення та аналізу інформації, інформаційно-аналітичні системи, бази даних (в тому числі міжвідомчі та міжнародні), криміналістичні та оперативно-технічні засоби, безпілотну авіацію, іншу спеціальну та військову техніку і спорядження. **РН21.** Організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації. **РН23**. Здійснювати заходи із забезпечення публічної безпеки та правопорядку в умовах воєнного стану та надзвичайних ситуацій, зокрема під час обстрілів та евакуації населення, охорони об'єктів критичної інфраструктури, а також у процесі взаємодії з внутрішньо переміщеними особами з дотриманням прав і свобод людини з урахуванням можливості їх дерогації, включно зі сприянням життєстійкості громад та участю у повоєнній відбудові прифронтових територій. **РН24.** Здійснювати превентивні заходи (профілактику) правопорушень у молодіжному середовищі шляхом використання інструментів державної молодіжної політики, комунікації з молодіжними субкультурами, орієнтованої на утвердження громадянських і патріотичних цінностей, запобігання радикалізації та протидію екстремістським проявам.	розробки заходів превенції Проєктно-пошуковий метод: самостійна робота з базами даних та спеціалізованим ПЗ для збору й аналізу правової інформації Тренінги з кібергігієни та режиму секретності: практичне опанування навичок роботи з інформацією з обмеженим доступом та криптографічним захистом тощо.	

3. Зміст навчальної дисципліни

Змістовий модуль 1.
ПРАВОВЕ РЕГУЛЮВАННЯ ТА ДЕРЖАВНЕ УПРАВЛІННЯ В СФЕРІ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Тема 1: Міжнародно-правові стандарти в сфері кібербезпеки та протидії кіберзлочинності

Конвенція про кіберзлочинність. Імплементація положень Конвенції в кримінальне законодавство України щодо криміналізації: умисного доступу до цілої комп'ютерної системи або її частини без права на це; умисного перехоплення технічними засобами, без права на це, передачі комп'ютерних даних, які не є призначеними для публічного користування; втручання у дані; втручання у систему; зловживання пристроями; підробки, пов'язаної з комп'ютерами; шахрайства, пов'язаного з комп'ютерами; правопорушень, пов'язаних з порнографією; правопорушень, пов'язаних з порушенням авторських та суміжних прав. Відповідальність юридичних осіб за кіберзлочини. Директива щодо мережевої та інформаційної безпеки (NIS). Проблеми виконання своїх міжнародних зобов'язань та вдосконалення законодавства в сфері кібербезпеки. Інші універсальні міжнародно-правові документи (Директива ЄС щодо протидії кібератакам на інформаційні системи 2013 р.; Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет 2017 р.). Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Інституційний механізм міжнародно-правового регулювання глобального інформаційного суспільства. Міжнародне співробітництво в сфері протидії кіберзлочинності.

Тема 2: Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.

Кібербезпека як частина національної безпеки України**.** Програмний рівень політики у сфері кібербезпеки в Україні. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. Виклики та загрози для України у сфері кібербезпеки. Засади побудови національної системи кібербезпеки. Пріоритети забезпечення кібербезпеки України. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки. Суб'єкти формування та реалізації політики у сфері кібербезпеки. Поняття кібербезпеки та кіберзахисту. Об'єкти кібербезпеки та кіберзахисту. Суб'єкти національної системи кібербезпеки. Класифікація суб'єктів діяльність спрямованих на забезпечення кібербезпеки. Розмежування повноважень між органами, відповідальними за кібербезпеку в Україні.

Тема 3. Управління державними інформаційними ресурсами

Поняття інформаційного ресурсу та його класифікація. Правовий режим доступу до публічної інформації та інформації з обмеженим доступом (таємна, службова, конфіденційна). Державний контроль за обігом інформації та роль регуляторів у сфері захисту даних. Правовий статус державних інформаційних систем та реєстрів у сфері правопорядку. Особливості обробки персональних даних у правоохоронній діяльності. Використання засобів електронної ідентифікації (КЕП) у службовому документообігу.

Тема 4. Режим секретності та технічний захист інформації

Організація документообігу з грифом «Таємно» та «ДСК». Криптографічний захист зв'язку. Правила роботи з фельд'єгерським та спеціальним зв'язком. Комплексна система захисту інформації (КСЗІ). Поняття та види технічних каналів витоку інформації. Допуск та доступ до державної таємниці. Особливості режиму секретності в умовах воєнного стану.

Змістовний модуль 2
ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ

Тема 5. Спеціалізовані інформаційні системи та бази даних.

Робота з інтегрованими системами МВС (АРМ «Поліція», «Гарпун», «Цунамі»). Доступ до міжвідомчих та міжнародних баз даних (SIS II, бази даних ДПСУ). Інформаційно-пошукові та довідкові системи криміналістичного обліку. Порядок роботи з базами даних біометричної ідентифікації (ДНК, дактилоскопія), обліку зброї («Єдиний реєстр зброї») та викрадених культурних цінностей. Системи автоматизованої відеоаналітики та розпізнавання об'єктів («Безпечне місто»).

Тема 6. Методологія пошуку та аналізу інформації (OSINT).

Пошук інформації у відкритих джерелах, реєстрах та соціальних мережах. Перевірка достовірності даних та виявлення прихованих зв'язків між суб'єктами. Методи ідентифікації осіб та локацій за метаданими та цифровими слідами. Використання OSINT-інструментів для моніторингу соціальних мереж та месенджерів. Основи роботи з Darknet та специфіка збору даних в анонімних мережах. Спеціалізоване програмне забезпечення для візуалізації та аналізу зв'язків. Етичні та правові межі використання результатів OSINT у кримінальному провадженні.

Тема 7. Використання безпілотної авіації та геоінформаційних систем (ГІС).

БПЛА як мобільний елемент інформаційної системи правоохоронних органів. Кібербезпека каналів керування та передачі даних БПЛА. Управління великими масивами геопросторових даних. Використання ГІС-технологій для візуалізації та аналізу оперативної інформації. Цифрова криміналістика безпілотних апаратів. ехнічні та програмні методи протидії «інформаційним диверсіям» із застосуванням БПЛА.

Змістовний модуль 3
ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ

Тема 8. Поняття та види кіберзлочинів

Поняття кіберзлочинності. Співвідношення з поняттями «злочинність у сфері використання електронно-обчислювальних машин», «комп'ютерна злочинність», «злочинність у віртуальному просторі», «злочинність у сфері інформаційних технологій», «злочинність у сфері ІТ - технологій» тощо. Ознаки кіберзлочинності. Класифікація кіберзлочинів. Кримінологічна характеристика кіберзлочинів: динаміка, рівень, географія, тенденції, ціна кіберзлочинності. Кримінологічна характеристика особи кіберзлочинця. Національний індекс кібербезпеки.

Тема 9. Основні суб'єкти протидії (запобігання) кіберзлочинам.

Поняття спеціалізованого та неспеціалізованого суб'єкта запобігання вчиненню кримінальних правопорушень. Основні суб'єкти протидії кіберзлочинності, органи, що реалізують державну політику в сфері протидії кіберзлочинності. Державна служба спеціального зв'язку та захисту інформації України. Національна поліція України. Департамент кіберполіції Національної поліції України. Служба безпеки України. Міністерство оборони України. Генеральний штаб Збройних сил України. Розвідувальні органи України. Національний банк України. Рада національної безпеки і оборони України.

Тема 10. Протидія кібершахрайству та деструктивним впливам у мережі.

Психологічні аспекти кіберзлочинності: механізми маніпуляції в соціальній інженерії. Технології фішингу: класичний фішинг, Clone Phishing, смішинг, вішинг та Evil Twin («Злий двійник»). Методика ідентифікації шахрайських ресурсів: ознаки підроблених сайтів, платіжних систем та електронних листів. Кібербулінг та онлайн-радикалізація: види деструктивного впливу (хейтинг, доксинг, тролінг). Превентивні заходи правоохоронців у молодіжному середовищі. Алгоритм допомоги потерпілим: першочергова фіксація доказів кібершахрайства, блокування транзакцій та маршрутизація заяв.

Тема 11. Кібергігієна та захист персональних даних у правоохоронній діяльності

Персональна кібергігієна як елемент національної безпеки: створення та менеджмент надійних паролів, двофакторна автентифікація (2FA). Технічні засоби самозахисту: антивірусне ПЗ, використання VPN, безпечне використання публічних Wi-Fi мереж. Цифрова безпека правоохоронця: ризики використання соціальних мереж, контроль метаданих у фотознімках, небезпека геолокації під час виконання

службових завдань. Захист конфіденційної інформації та персональних даних громадян: правові аспекти доступу правоохоронців до приватної інформації. Аналіз типових помилок користувачів: вразливості «людського фактора» та способи їх мінімізації.

Змістовний модуль 4.
НАЦІОНАЛЬНА БЕЗПЕКА В ЦИФРОВОМУ СЕРЕДОВИЩІ ТА ІННОВАЦІЙНИЙ РОЗВИТОК

Тема 12: Кібербезпека об’єктів критичної інфраструктури та превенція екстремізму

Захист критичної інформаційної інфраструктури (КІІ): класифікація об’єктів (енергетика, водопостачання, транспорт) та їх вразливості до кібердиверсій. Алгоритми дій правоохоронців при техногенних та кіберінцидентах: охорона об'єктів та підтримання порядку при відключенні зв’язку чи атаках на держреєстри. Моніторинг деструктивних субкультур у мережі: виявлення ознак радикалізації молоді та підготовки до терористичних актів/диверсій. Профілактика екстремізму та онлайн-вербування: інструменти державної молодіжної політики у протидії поширенню радикальних ідеологій.

Тема 13. Гібридні загрози та протидія інформаційно-психологічним операціям (ІПСО)

Інструментарій гібридної війни: роль дезінформації, фейків та маніпуляцій у дестабілізації публічного порядку. Методика розпізнавання ІПСО: аналіз ботоферм, пропагандистських наративів та технік емоційного маніпулювання. Забезпечення інформаційного суверенітету держави: роль правоохоронних органів у протидії ворожим впливам та паніці серед населення. Взаємодія з внутрішньо переміщеними особами (ВПО) та громадами: запобігання конфліктам, що провокуються через цифрові канали зв’язку.

4. Структура навчальної дисципліни

Вид заняття / роботи	Назва теми	Кількість годин		Згідно з розкладом
		о/д.ф	з.ф.	
Лекція 1	**Тема 1: Міжнародно-правові стандарти в сфері кібербезпеки та протидії кіберзлочинності**	2	0,5	*1 тиждень*
Практичне заняття 1 *Робота в*	**Тема 1: Міжнародно-правові стандарти в сфері кібербезпеки та протидії кіберзлочинності** *Перелік питань*: 1. Поняття кібербезпеки та кіберпростору.	2	0,5	*1 тиждень*

малих групах, рефлексія	2. Тріада інформаційної безпеки (CIA) 3. Будапештська конвенція як «Конституція» кіберпростору: 4. Інші універсальні міжнародно-правові документи (Директива ЄС щодо протидії кібератакам на інформаційні системи 2013 р.; Директива Єврокомісії щодо боротьби з шахрайством та іншими фінансовими злочинами в мережі Інтернет 2017 р.). ***Завдання для малих груп:*** Використовуючи структуру Будапештської конвенції, визначте, до якої з чотирьох груп належить кожен випадок: 1) DDoS-атака на сайт суду; 2) розсилка фішингових листів; 3) піратський стрімінг фільмів; 4) поширення дитячої порнографії; 5) створення шкідливого програмного забезпечення. ***Кейс «Гібрідна атака»:*** Під час масованої гібридної атаки на інформаційну інфраструктуру України постраждав умовний державний реєстр. Слідство встановило три факти: 1. Дані про місце проживання держслужбовців з'явилися в анонімних Telegram-каналах. *2.* У реєстрі нерухомості право власності на об'єкт критичної інфраструктури було переписано на підставну особу шляхом несанкціонованої зміни запису в базі. *3.* Вебпортал надання державних послуг перестав відповідати на запити користувачів через перевантаження трафіком із закордонних IP-адрес. **Питання до кейсу**: Спираючись на розділ Конвенції "Злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем", визначте: Яка стаття описує правопорушення витік персональних даних, якщо воно було здійснено через незаконний доступ до сервера? Чому зміна власника в реєстрі є порушенням Статті 4, а не просто фінансовим шахрайством? У чому полягає різниця між "втручанням у дані" та "комп'ютерним шахрайством" (Стаття 8)? Чи підпадає перевантаження трафіком із закордонних IP-адрес під дію **Статті 5**, якщо перевантаження трафіком було спричинене не шкідливим кодом, а використанням законних мережевих протоколів (DDoS)?			
Самостійна робота	**Тема 1: Міжнародно-правові стандарти в сфері кібербезпеки та протидії кіберзлочинності** *Питання для розгляду:*	5	8	*1 тиждень*

	1. Проблеми виконання своїх міжнародних зобов'язань та вдосконалення законодавства в сфері кібербезпеки. 2. Чому для боротьби з кіберзлочинністю недостатньо законів однієї країни? Як міжнародний стандарт допомагає українському поліцейському отримати дані з сервера, що знаходиться в США?» Виконати тест № 1 до теми № 1.			
Лекція 2	**Тема 2: Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.**	2	0,5	*2 тиждень*
Самостійна робота	**Тема 2: Основні цілі, напрями та принципи державної політики у сфері кібербезпеки**. *Перелік питань для розгляду*: 1) Напрями зовнішньополітичної діяльності України у сфері кібербезпеки. 2) співпраця у сфері кібербезпеки з іноземними партнерами (Сполученими Штатами Америки, Сполученим Королівством Великої Британії і Північної Ірландії, Федеративною Республікою Німеччина, Королівством Нідерланди, Японією тощо); 3) співробітництво з ЄС та НАТО	5	8	*2 тиждень*

Практичне заняття 2 *Інтерактивна кейс-студія: «Стратегія в дії», рефлекція*	**Тема 2: Основні цілі, напрями та принципи державної політики у сфері кібербезпеки.** *Перелік питань:* 1) Кібербезпека як частина національної безпеки України**;** 2) Програмний рівень політики у сфері кібербезпеки в Україні. 3) Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. 4) Суб'єкти формування та реалізації політики у сфері кібербезпеки. ***Кейс-сценарій: «Фінансовий параліч»*** *Сюжет:* П'ятниця, 16:00. Провідні державні та приватні банки України зазнають масованої DDoS-атаки у поєднанні з впровадженням вірусу-шифрувальника в систему міжбанківських платежів. *Наслідки:* Картки не працюють, банкомати порожні, мобільні додатки «лежать». *Загроза:* У соцмережах поширюється фейк про те, що «всі гроші українців вкрадено хакерами», що провокує масову паніку та штурм закритих відділень банків. **Завдання:** «Пошук стратегічного рішення» Ознайомтеся з текстом Стратегії кібербезпеки України та знайдіть ключові напрями подолання цієї кризи? **Питання для рефлекції:** Якби ви були керівником підрозділу кіберполіції в цій ситуації, куди б ви спрямували обмежені людські ресурси в першу чергу: на технічну допомогу банкам у розблокуванні серверів чи на виявлення та блокування першоджерел панічних фейків у соцмережах? Обґрунтуйте пріоритетність згідно зі Стратегією».	2	0,5	*2 тиждень*
Лекція 3	**Тема 3: Управління державними інформаційними ресурсами**	2	0,5	*3 тиждень*
Самостійна робота	Тема 3: Управління державними інформаційними ресурсами *Перелік питань:* *1.* Обґрунтуйте, у яких випадках правоохоронні органи мають право обробляти персональні дані особи без її згоди згідно із Законом України «Про захист персональних даних». *2.* Наведіть 2-3 приклади інформації, яка в поліції вважається просто «службовою» (ДСК), а яка — «державною таємницею». У чому головна різниця в роботі з ними? *3.* Що загрожує співробітнику поліції за	*5*	8	*3 тиждень*

	«цікавість» — наприклад, якщо він перевірив по базах сусіда або родича без службової потреби? *4.* Чому не можна передавати свій електронний ключ або пароль від нього колегам, навіть якщо це потрібно «для термінової роботи»? *5.* Хто в Україні має право перевірити, чи правильно правоохоронці зберігають та використовують інформацію про громадян? *6.* У яких ситуаціях правоохоронець може збирати дані про людину (адресу, номер телефону, фото), не питаючи її дозволу?			
Практичне заняття 3 *Робота в малих групах, інтерактивний кейс, рефлексія*	**Тема 3. Управління державними інформаційними ресурсами** *Питання до розгляду:* 1.Поняття інформаційного ресурсу та його класифікація. 2.Правовий режим доступу до публічної інформації та інформації з обмеженим доступом (таємна, службова, конфіденційна). 3. Державний контроль за обігом інформації та роль регуляторів у сфері захисту даних. 4. Правовий статус державних інформаційних систем та реєстрів у сфері правопорядку. 5. Особливості обробки персональних даних у правоохоронній діяльності. 6.Використання засобів електронної ідентифікації (КЕП) у службовому документообігу. ***Завдання для малих груп:*** Класифікуйте кожен ресурс та визначити його правовий режим (відкрита, службова (ДСП), таємна чи конфіденційна персональна інформація? (*декларація доброчесності судді, декларація родинних зав'язків прокурора, декларація депутата, витяг з реєстру прав на нерухоме майно, запис з бодікамери патрульного поліцейського, запис з камери відеоспостереження «Безпечне місце», відео з камери охорони приватного будинку, домашня адреса потерпілої особи, результати судово-медичної експертизи в кримінальному провадженні*). **Інтерактивний кейс: «Запит на інформацію vs Персональні дані».** **Ситуація:** кримінальне провадження щодо ОСОБА_1 було закрито у зв'язку з відсутністю складу кримінального правопорушення. Коли будуть видалені його персональні дані, які знаходяться в інформаційно-комунікативній системі Національної поліції?	2	0,5	*3 тиждень*

	Завдання: яким чином ОСОБА_1 може перевірити наявність/відсутність своїх персональних даних у реєстрах МВС? ***Рефлексія з питань:*** 1.Що є вищим пріоритетом для правоохоронної системи: цілісність державних архівів (пам'ятати все) чи право людини на новий старт без цифрового шлейфу закритих справ?» 2.Чи відповідає стандартам ЄСПЛ практика автоматичного зберігання інформації про всі інциденти в єдиній базі, чи держава зобов'язана запровадити диференційовані строки зберігання залежно від тяжкості злочину та результатів розслідування?			
Лекція 4	**Тема 4. Режим секретності та технічний захист інформації**	**2**	0,5	*4 тиждень*
Практичне заняття 4 *Опитування* *Рефлексія*	**Тема 4. Режим секретності та технічний захист інформації** *Перелік питань:* 1.Організація документообігу з грифом «Таємно» та «ДСК». 2.Криптографічний захист зв'язку. 3.Правила роботи з фельд'єгерським та спеціальним зв'язком. 4.Комплексна система захисту інформації (КСЗІ). 5.Поняття та види технічних каналів витоку інформації. 6.Допуск та доступ до державної таємниці. 7. Особливості режиму секретності в умовах воєнного стану. ***Рефлексія з питання:*** «Приватність проти безпеки: чи має право сучасний правоохоронець на активне життя в соцмережах та використання персональних гаджетів під час виконання бойових чи спеціальних завдань?»	2	0,5	*4 тиждень*
Самостійна робота	Тема 4. Режим секретності та технічний захист інформації *Перелік питань:* 1.Поясніть різницю між поняттями допуск та доступ до документів двома. Чи може поліцейський, який має допуск до таємниці, самовільно отримати доступ до будь-якої секретної справи свого відділу? 2. Чому заборонено фотографувати секретні документи або бойові розпорядження на особистий смартфон, навіть якщо ви хочете переслати їх колезі через «захищений» месенджер (приміром WhatsApp)? 3. Як має діяти правоохоронець із секретними	*5*	8	*4 тиждень*

	документами у разі реальної загрози захоплення будівлі чи території ворогом? 4. Проаналізуйте ризики публікації фото з робочого місця в Instagram: які деталі на задньому плані (карти, списки, спеціальне обладнання) можуть видати державну таємницю? 5. Ви отримали новий робочий комп'ютер для роботи з секретною базою даних. На ньому встановлено Комплексну систему захисту інформації (КСЗІ). Поясніть, чому на такий комп'ютер категорично заборонено самостійно встановлювати будь-які програми (наприклад, браузери чи плеєри) або підключати власні флешки? *6.* За які дії правоохоронця можуть позбавити допуску до державної таємниці?			
Лекція 5	**Тема 5. Спеціалізовані інформаційні системи та бази даних.**	2	0,5	*5 тиждень*
Практичне заняття 5 *Брейнстормінг у поєднанні з Інтерактивним кейсом.*	**Тема 5. Спеціалізовані інформаційні системи та бази даних**. *Перелік питань:* 1.Робота з інтегрованими системами МВС (АРМ «Поліція», «Гарпун», «Цунамі»). 2. Доступ до міжвідомчих та міжнародних баз даних (SIS II, бази даних ДПСУ). 3. Інформаційно-пошукові та довідкові системи криміналістичного обліку. 4.Порядок роботи з базами даних біометричної ідентифікації (ДНК, дактилоскопія), обліку зброї («Єдиний реєстр зброї») та викрадених культурних цінностей. 5.Системи автоматизованої відеоаналітики та розпізнавання об’єктів («Безпечне місто»). **Вхідні дані (Фабула):** Ви зупинили авто на блокпосту. Система **«Гарпун»** видає повідомлення: *"Помилка запиту: Тимчасова відсутність зв'язку з сервером"*. Водій помітно нервує, уникає зорового контакту та заявляє, що «дуже поспішає», відмовляючись виходити з авто. Документи на транспортний засіб виглядають новими, але серійний номер техпаспорта викликає сумнів (можлива підробка). ***Завдання для брейнстормінгу (малі групи):*** Протягом 5 хвилин виробити план ідентифікації через інші системи, що працюють автономно або через інші канали зв'язку.	2	0,5	*5 тиждень*
Самостійна робота	**Тема 5. Спеціалізовані інформаційні системи та бази даних.** *Перелік питань:*	5	8	*5 тиждень*

	1.Опишіть покроково, які дані про транспортний засіб ви отримаєте через систему «Гарпун», якщо камера зафіксувала номер авто, що перебуває в розшуку. Якими мають бути ваші перші дії? 2. Поясніть процесуальний порядок відбору зразків ДНК або відбитків пальців. У яких випадках ці дані вносяться до баз даних примусово, а в яких — за згодою особи? 3. Як працює база даних викрадених предметів мистецтва? Які ознаки (клейма, підписи, дефекти) є ключовими для їх ідентифікації та внесення в систему розшуку? 4. Які переваги дає перехід на електронний облік зброї для дільничного офіцера поліції під час перевірки умов зберігання мисливської зброї за місцем проживання власника? 5. Опишіть ситуацію, коли патрульному поліцейському необхідно отримати дані з баз Державної прикордонної служби. Яку саме інформацію про перетин кордону особою чи автомобілем він може отримати в режимі реального часу?			
Лекція 6	**Тема 6. Методологія пошуку та налізу інформації (OSINT)**	2	0,5	*6 тиждень*
Практичне заняття 6 *Ситуаційний кейс*	**Тема 6. Методологія пошуку та аналізу інформації (OSINT).** *Перелік питань:* 1.Пошук інформації у відкритих джерелах, реєстрах та соціальних мережах. 2.Перевірка достовірності даних та виявлення прихованих зв'язків між суб'єктами. 3.Методи ідентифікації осіб та локацій за метаданими та цифровими слідами. 4.Використання OSINT-інструментів для моніторингу соціальних мереж та месенджерів. 5.Основи роботи з Darknet та специфіка збору даних в анонімних мережах. 6.Спеціалізоване програмне забезпечення для візуалізації та аналізу зв’язків. 7.Етичні та правові межі використання результатів OSINT у кримінальному провадженні. **Ситуаційний кейс: «**Боржник в Instagram» В Instagram фігуранта знайдено фото розкішного авто, хоча за реєстрами він «безробітний боржник». Цю інформацію аналізують двоє: колишня дружина (через адвоката) та детектив поліції/НАЗК. *Питання для студентів:* «Проаналізуйте дії обох суб’єктів. Чи будуть відмінності в їхніх підходах до збору, верифікації та	2	0,5	*6 тиждень*

	використання цієї інформації? Дайте відповідь на наступні пункти: Які додаткові бази (ДПСУ, реєстри майна, банківські виписки) доступні правоохоронцю, але закриті для цивільної особи? Чим відрізняється доведення "спроможності платити аліменти" (цивільний процес) від доведення "незаконного збагачення" (кримінальний/адміністративний процес)? Як правоохоронець перетворить скріншот на "результат оперативно-розшукової діяльності", а дружина — на "доказ у сімейному спорі"?»			
Самостійна робота	Тема 6. Методологія пошуку та аналізу інформації (OSINT). *Перелік питань:* 1.Складіть перелік відкритих реєстрів України (наприклад, Опендатабот, реєстр судових рішень), які дозволяють за ПІБ особи встановити її зв'язки з бізнесом або наявність боргів. 2. Чи можна використати скріншот сторінки у Facebook як прямий доказ у суді? Які вимоги висуваються до фіксації такої інформації, щоб вона не була визнана недопустимим доказом? 3. Як встановити місце зйомки відео, якщо на ньому немає відомих пам'яток чи табличок з адресами? 4. Опишіть методи візуального аналізу для виявлення згенерованих нейромережами облич або голосів.	5	8	*6 тиждень*
Лекція 7	**Тема 7. Використання безпілотної авіації та геоінформаційних систем (ГІС).**	2	0,5	*7 тиждень*
Практичне заняття 7 рефлекція	**Тема 7. Використання безпілотної авіації та геоінформаційних систем (ГІС).** *Перелік питань:* 1.БПЛА як мобільний елемент інформаційної системи правоохоронних органів. 2.Кібербезпека каналів керування та передачі даних БПЛА. 3. Використання ГІС-технологій для візуалізації та аналізу оперативної інформації. 4. Цифрова криміналістика безпілотних апаратів. ехнічні та програмні методи протидії «інформаційним диверсіям» із застосуванням БПЛА. ***Рефлексія щодо питання:*** «Ви використовуєте дрон для пошуку викраденого авто у приватному секторі. Випадково камера зафіксувала на подвір'ї іншого будинку інше правопорушення (наприклад, вирощування	2	0,5	*7 тиждень*

	конопель). Чи буде це відео законним доказом, якщо дрон "залетів" у приватний простір без ухвали суду?»			
Самостійна робота	**Тема 7. Використання безпілотної авіації та геоінформаційних систем (ГІС).** *Перелік питань:* 1.За яких умов правоохоронні органи мають право здійснювати аерофотозйомку приватної власності без згоди власника? 2. Які переваги має використання безпілотників при документуванні наслідків масштабних ДТП або місць воєнних злочинів? 3. Які законні методи мають правоохоронці для примусової посадки або перехоплення приватного дрона, що порушує межі режимного об'єкта чи загрожує безпеці громадян? 4. Яких правил безпеки (шифрування каналів, режим радіомовчання) має дотримуватися оператор поліцейського БПЛА? 5. Поясніть, чому наявність автоматично згенерованих EXIF-даних (GPS-координати, час, висота) є критично важливою при фіксації прильотів у Запорізькій області. Як ці дані допомагають експертам-артилеристам чи вибухотехнікам встановити точне місце запуску ворожої ракети? 6. Тактичні особливості екстреної фіксації воєнних злочинів в умовах активних бойових дій та загрози повторних ударів (на прикладі Запорізької агломерації та прифронтових громад)?	5	8	*7 тиждень*
Лекція 8	**Тема 8: Поняття кіберзлочинів та їх види**	2	0,5	*8 тиждень*
Практичне заняття 8 *Вирішення ситуаційних кейсів*	**Тема 8: Поняття кіберзлочинів та їх види** *Перелік питань:* 1) Поняття кіберзлочинності; 2) Співвідношення з поняттями «злочинність у сфері використання електронно-обчислювальних машин», «комп'ютерна злочинність», «злочинність у віртуальному просторі», «злочинність у сфері інформаційних технологій», «злочинність у сфері ІТ - технологій» тощо; 3) Класифікація кіберзлочинів. **Кейс №1: «Дзвінок з "безпеки банку"»** **Ситуація:** Пенсіонерці зателефонував чоловік, який представився співробітником служби безпеки відомого банку. Він повідомив, що з її картки прямо зараз намагаються списати кошти в іншому місті. Щоб «заблокувати операцію», він попросив назвати	2	0,5	

	термін дії картки та три цифри з обороту (CVV), а також код, що прийде в SMS. Жінка все назвала, і з її рахунку зникло 15 000 грн. *Питання:* Чому цей злочин називають «кіберзлочином», хоча злочинець просто розмовляв по телефону? Яку роль тут відіграє цифрова інструментарія (підміна номера, онлайн-банкінг)? Потерпіла заявила про вченене діяння через 2 години після події. Яку першу цифрову дію ви порадите їй зробити (крім написання заяви), щоб зупинити рух грошей? **Кейс №2: «Цифрова пастка: Шантаж у шкільному чаті»** Ситуація: 14-річна школярка отримала в Instagram повідомлення від "подруги" з проханням: *«Привіт! Голосуй за мене в конкурсі, ось посилання»*. Дівчина перейшла за посиланням і ввела свої дані для входу. Вже через годину доступ до акаунту було втрачено. Згодом у Telegram їй написав анонім, який надіслав скріншоти її приватних фото з Direct (у тому числі особистого характеру). Шахрай вимагає 3 000 грн, погрожуючи, що в разі відмови розішле ці фото у загальний чат класу та батькам. Уявіть, що до вас як до чергового офіцера звернулася неповнолітня особа, яка стала жертвою кібершантажу (погроза поширення інтимних фото). Яким має бути ваш покроковий алгоритм дій згідно із законом та відомчими інструкціями, щоб одночасно забезпечити захист прав дитини та не втратити цифрові докази злочину?» **Кейс: «Цифровий оператор АЗС»** **Ситуація:** Системний адміністратор мережі автозаправних станцій (АЗС) створив приховану програму-доповнення до офіційного софту, який контролює налив пального. Ця програма під час кожного заправлення на 40 літрів непомітно недоливала в бак **клієнта 200 мл** пального. При цьому на екрані колонки та в чеку відображалися повні 40 літрів. «Зекономлене» пальне накопичувалося як надлишок у резервуарах, який адмін потім списував через систему як «випаровування» та перепродував «наліво».			

	Дайте кримінально-правову оцінку діям системного адміністратора.			
Самостійна робота	**Тема 8: Поняття кіберзлочинів та їх кримінологічна характеристика** *Перелік питань:* 1. Проаналізуйте основні групи злочинів згідно з Конвенцією про кіберзлочинність (злочини проти конфіденційності, комп'ютерні злочини, злочини, пов'язані з контентом). Які з них є найбільш поширеними в Україні за останній рік? 2. Як змінилася структура кіберзлочинності в Україні з 2022 року? Проаналізуйте зростання кількості фішингових атак, пов'язаних із «виплатами допомоги від ООН» або «зборами на ЗСУ», та використання кіберінструментів для координації ракетних ударів. 3. Чому значна частина кіберзлочинів (наприклад, злам особистих поштових скриньок або невеликі крадіжки з криптогаманців) залишається поза статистикою МВС? Які фактори заважають потерпілим звертатися до поліції? 4. Чи визнається предметом злочину, пов'язаного зі зберіганням дитячої порнографії зображення, згенероване штучним інтелектом? 5. Які саме технічні або програмні властивості роблять програму «шкідливою» з юридичної точки зору? Проаналізуйте різницю між програмою-вірусом та легітимним програмним забезпеченням для віддаленого адміністрування, яке було використане зловмисником без дозволу власника. 6. Зловмисник створив фейковий сайт для 'виплат допомоги від ООН', де користувачі самі вводили дані карток. За якою частиною статті 190 КК України найімовірніше будуть кваліфіковані ці дії в умовах воєнного стану? 7. У чому полягає юридична різниця між заволодінням коштами через фішинг (де жертва сама вводить дані) та автоматизованим викраденням грошей через вразливість банківської системи? Поясніть, чому використання комп'ютерної техніки є обтяжуючою обставиною за ч. 3 та 4 ст. 190 КК України. 8. Як саме кваліфікуються дії особи, яка створює клон сторінки відомого благодійного фонду для збору коштів нібито на ЗСУ?	5	8	*8 тиждень*
Лекція 9	**Тема 9. Основні суб'єкти протидії (запобігання) кіберзлочинам та забезпечення кібербезпеки.**	2	0,25	*9 тиждень*

Практичне заняття 9	**Тема 9. Основні суб'єкти протидії (запобігання) кіберзлочинам та забезпечення кібербезпеки.** *Перелік питань:* 1.Поняття спеціалізованого та неспеціалізованого суб'єкта запобігання вчиненню кіберзлочинів. 2.Основні суб'єкти протидії кіберзлочинності та органи, що реалізують державну політику в сфері протидії кіберзлочинності. Державна служба спеціального зв'язку та захисту інформації України. Національна поліція України. Департамент кіберполіції Національної поліції України. Служба безпеки України. Міністерство оборони України. Генеральний штаб Збройних сил України. Розвідувальні органи України. Національний банк України. Рада національної безпеки і оборони України.	2	0,25	
Самостійна робота	**Тема 9. Суб'єкти протидії (запобігання) кіберзлочинам** *Перелік питань до розгляду:* 1. Яким чином здійснюється координація між різними суб'єктами (МВС, СБУ, Міноборони) під час масштабних кібератак на державні реєстри? 2. Визначте специфіку роботи контррозвідувального захисту інтересів держави у кіберпросторі. Які саме об'єкти критичної інфраструктури (наприклад, ДніпроГЕС у Запоріжжі) перебувають під прямим наглядом СБУ у контексті кібербезпеки? 3. Поясніть роль Державної служби спеціального зв'язку та захисту інформації. Що таке команда CERT-UA і яким є алгоритм її взаємодії з приватними підприємствами у разі виявлення вразливостей у їхніх мережах? 4. Проаналізуйте правові підстави діяльності кіберпідрозділів у структурі ЗСУ. Яка різниця між "кібероборoною" (захистом військових мереж) та "кібероперaціями" у контексті сучасної війни? 5. Опишіть роль приватного сектору (провайдерів, антивірусних компаній) у забезпеченні національної кібербезпеки. Як правоохоронні органи залучають цивільних IT-спеціалістів до розслідування складних кіберзлочинів? 6. Проаналізуйте основні завдання CERT-UA – спеціалізованого структурного підрозділу Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації; 7. Яким чином НБУ забезпечує захист банківської системи та платіжних сервісів від	5	8	*9 тиждень*

	фішингових атак та маніпуляцій з електронними грошима? Роль Центру кіберзахисту НБУ (CSIRT-NBU). 8. Які функції виконують міжнародні інституції (Europol, Interpol) у підтримці українських правоохоронців? 9. Ззнайомтеся з підходами щодо формування системи підготовки кадрів у сфері кібербезпеки та оцініть стандарти підготовки фахівців з кібербезпеки в Україні.			
Лекція 10	**Тема 10. Протидія кібершахрайству та деструктивним впливам у мережі**	2	0,25	*10 тиждень*
Практичне заняття 10	**Тема 10. Протидія кібершахрайству та деструктивним впливам у мережі.** *Перелік питань:* 1.Психологічні аспекти кіберзлочинності: механізми маніпуляції в соціальній інженерії. 2.Технології фішингу: класичний фішинг, Clone Phishing, смішинг, вішинг та Evil Twin («Злий двійник»). 3.Методика ідентифікації шахрайських ресурсів: ознаки підроблених сайтів, платіжних систем та електронних листів. 4.Кібербулінг та онлайн-радикалізація: види деструктивного впливу (хейтинг, доксинг, тролінг). 5.Превентивні заходи правоохоронців у молодіжному середовищі. 6.Алгоритм допомоги потерпілим: першочергова фіксація доказів кібершахрайства, блокування транзакцій та маршрутизація заяв. **Кейс: «Атомний фейк: протидія радіаційній паніці»** Сценарій: У місцевих Telegram-каналах та Viber-чатах міста (яке знаходиться за 100 км від Енергодара) починає масово поширюватися повідомлення: *«Терміново! На ЗАЕС стався викид. Радіаційна хмара рухається на нас. Влада мовчить, щоб не сіяти паніку. Пийте йод, зачиняйте вікна, виїжджайте негайно!»*. До повідомлення додано скріншот карти з «моделлю розповсюдження радіації», яка виглядає дуже реалістично (створена за допомогою ШІ). Люди в паніці кидаються до аптек за йодом та на заправки, блокуючи основні виїзди з міста. *Завдання для студентів:* Визначте алгоритм дій: 1. Роль «Патрульного / Офіцера громади» 2. Роль аналітика з кібербезпеки 3. Роль «Керівника підрозділу».	2	0,25	*10 тиждень*

	Тема дискусії на основі цього кейсу: «Алгоритм "Цифрової першої допомоги": чи повинен поліцейський чекати на офіційну позицію міністерства, чи має право самостійно спростовувати локальні фейки в чатах для збереження публічного порядку?»			
Самостійна робота	**Тема 10. Протидія кібершахрайству та деструктивним впливам у мережі.** *Питання для розгляду:* 1. Складіть перелік установ та організацій, куди має звернутися людина в перші 30 хвилин після того, як зрозуміла, що стала жертвою інтернет-шахраїв. 2. Ознайомтеся з алгоритмом дій кіберполіції у разі отримання заяви про кібершахрайство. 3. Які психологічні «гачки» використовуються для залучення молоді до протиправної діяльності (наприклад, підпалів військових авто або передачі координат)? Чому цей процес класифікується як деструктивний вплив, а не як «свобода поглядів»? 4. Які цифрові інструменти (наприклад, чат-боти «Стоп-наркотик» або освітні платформи) є найбільш ефективними для запобігання кібербулінгу? 5. Опишіть алгоритм дій поліції, якщо вчителем виявлено групу у соцмережах, де схиляють дітей до самоушкодження або радикальних дій. 6. Які юридичні наслідки передбачені для батьків згідно зі ст. 184 КУпАП (Невиконання обов'язків щодо виховання дітей), якщо їхня дитина була втягнута у диверсійну діяльність через соцмережі? 7. Чи звільняє неповнолітнього від відповідальності факт «маніпуляції» з боку дорослого вербувальника? 8. Чи здатні Ви провести межу між свободою слова в інтернеті та розпалюванням ворожнечі або підготовкою до терористичної діяльності? 9. Назвіть найшвидші інструменти передачі інформації від цивільних до спецслужб в умовах прифоронтового Запоріжжя? 10. Куди можна повідомити про підозрілих осіб, які фотографують критичну інфраструктуру (ДніпроГЕС, вокзали, підстанції), намагаються встановити «маячки» або розпитують про рух техніки ЗСУ?	5	9	*10 тиждень*
Лекція 11	**Тема 11. Кібергігієна та захист персональних даних у правоохоронній діяльності**	2	0,25	*11 тиждень*

Практичне заняття 11 (*практичний форкшоп «Цифровий слід»*)	**Тема 11. Кібергігієна та захист персональних даних у правоохоронній діяльності** *Перелік питань:* 1.Персональна кібергігієна як елемент національної безпеки. 2. Технічні засоби самозахисту. 3.Цифрова безпека правоохоронця: ризики використання соціальних мереж, контроль метаданих у фотознімках, небезпека геолокації під час виконання службових завдань. 4.Захист конфіденційної інформації та персональних даних громадян. 5.Правові аспекти доступу правоохоронців до приватної інформації. *Завдання:* 1.Проаналізуйте власний цифровий слід в мережах за 10 хвилин (чи можна дізнатися з відкритих джерел адресу проживання, марку авто, коло спілкування та іншу інформацію?); 2. Налаштуйте двофакторну автентифікацію (2FA) в усіх месенджреах; 3.Проаналізуйте хто має доступ до мікрофона та геолокації 24/7; 4. налаштуйте автоматичне видалення повідомлень у робочих чатах.	2	0,25	*11 тиждень*
Самостійна робота	**Тема 11. Кібергігієна та захист персональних даних у правоохоронній діяльності** *Перелік питань:* 1. Яку відповідальність (адміністративну та кримінальну) несе працівник поліції за несанкціоновану перевірку осіб через бази даних (наприклад, АРМОР) в особистих цілях або на прохання третіх осіб? 2. Як регламентується «право на забуття» та захист персональних даних свідків у цифрових реєстрах? 3. У чому полягає різниця між «оглядом» відкритої сторінки особи у соцмережі та «доступом до приватного листування» в месенджері? 4. Які процесуальні документи (ухвала слідчого судді тощо) необхідні для легітимного отримання інформації з мобільного пристрою підозрюваного? 5. Що таке метадані (EXIF) і як вони можуть видати місце дислокації підрозділу або слідчої групи? 6. Які існують доступні канали та алгоритми дій для цивільної особи у разі виявлення в інформаційному просторі (зокрема в Telegram) деструктивного контенту або ворожого ІПСО?	6	9	*11 тиждень*

	7. Опишіть можливості анонімного інформування правоохоронних органів та спеціалізованих центрів через цифрові інструменти (чат-боти).			
Лекція 12	**Тема 12: Кібербезпека об'єктів критичної інфраструктури та превенція екстремізму**	2	0,25	*12 тиждень*
Практичне заняття 12	**Тема 12: Кібербезпека об'єктів критичної інфраструктури та превенція екстремізму** *Перелік питань*: 1.Захист критичної інформаційної інфраструктури (КІІ): класифікація об'єктів (енергетика, водопостачання, транспорт) та їх вразливості до кібердиверсій. 2.Алгоритми дій правоохоронців при техногенних та кіберінцидентах: охорона об'єктів та підтримання порядку при відключенні зв'язку чи атаках на держреєстри. 3.Моніторинг деструктивних субкультур у мережі: виявлення ознак радикалізації молоді та підготовки до терористичних актів/диверсій. 4. Профілактика екстремізму та онлайн-вербування: інструменти державної молодіжної політики у протидії поширенню радикальних ідеологій.	2	0,25	*12 тиждень*
Самостійна робота	**Тема 12: Кібербезпека об'єктів критичної інфраструктури та превенція екстремізму** *Перелік питань*: 1. Опишіть протокол дій правоохоронця при виконанні службових завдань в умовах техногенної аварії та критичного збою інформаційних систем (без доступу до Інтернету та мобільної мережі). 2. Опишіть порядок міжвідомчої взаємодії між підрозділами Кіберполіції НПУ та Департаментом контррозвідувального захисту інтересів держави у сфері інформаційної безпеки (ДКІБ) СБУ під час ліквідації наслідків кібератаки на об'єкт енергетики. 3. Чому при одночасному залученні Кіберполіції та СБУ до ліквідації кібератаки необхідна участь Національного координаційного центру кібербезпеки? 4. Які інструменти державної молодіжної політики (освітні хаби, кіберспортивні заходи, медіаграмотність) є найбільш ефективними у протидії ворожій пропаганді в Запорізькій області? 5. Чи можна вважати підлітка, який здійснив підпал військового авто за винагороду в криптовалюті, повноцінним суб'єктом диверсії, або він є виключно жертвою цифрової маніпуляції та	6	9	*12 тиждень*

	специфічних фінансових технологій?» 6. Оцініть гейміфікацію як інструмент схиляння неповнолітніх осіб до вчинення диверсій або підпалів автомобілів військовослужбовців ЗСУ			
Лекція 13	**Тема 13: Гібридні загрози та протидія інформаційно-психологічним операціям (ІПСО)**	2	0,25	*13 тиждень*
Практичне заняття 13 *дискусія*	**Тема 13. Гібридні загрози та протидія інформаційно-психологічним операціям (ІПСО).** Перелік питань: 1.Інструментарій гібридної війни: роль дезінформації, фейків та маніпуляцій у дестабілізації публічного порядку. 2.Методика розпізнавання ІПСО: аналіз ботоферм, пропагандистських наративів та технік емоційного маніпулювання. 3. Забезпечення інформаційного суверенітету держави: роль правоохоронних органів у протидії ворожим впливам та паніці серед населення. 4. Взаємодія з внутрішньо переміщеними особами (ВПО) та громадами: запобігання конфліктам, що провокуються через цифрові канали зв'язку. *Дискусія для семінару:* «Чи є ефективною діяльність правоохоронних органів України щодо іноземних ботоферм, якщо виконавців неможливо притягнути до кримінальної відповідальності через відсутність правової допомоги з боку країни-агресора?» **Кейс «ІПСО»** **Обставини справи:** У популярному запорізькому Telegram-каналі «Типове Запоріжжя» о 19:00 з'являється пост від «дружини бійця 110-ї бригади». Вона публікує фотографію зацвілого хліба та брудних наметів, стверджуючи, що її чоловік на Оріхівському напрямку «кинутий командирами без боєкомплекту, а гуманітарну допомогу, яку збирали запоріжці, бачили на прилавках магазинів Запоріжжя». Проаналізуйте зміст повідомлення та визначте: за допомогою яких психологічних «гачків» організатори операції намагаються вимкнути критичне мислення у мешканців Запоріжжя? Чому для дестабілізації обрано саме вечірній час та поєднання тем «голоду на фронті» та «корупції в тилу»? Як правоохоронні органи, використовуючи відкриті дані (OSINT), можуть швидко перевірити автентичність цього повідомлення? Опишіть ознаки, що вказуватимуть на роботу ботоферми у коментарях (часові інтервали, схожість синтаксису, профілі користувачів).	2	0,25	*13 тиждень*

Самостійна робота	**Тема 13: Гібридні загрози та протидія інформаційно-психологічним операціям (ІПСО).** *Перелік питань:* 1. У чому небезпека технології діпфейків (відео з підробленими обличчями та голосами керівництва держави чи ЗСУ) для стабільності фронту та тилу? 2. Які техніки самодопомоги та інформаційної гігієни мають застосовувати правоохоронці, щоб ворожі наративи (наприклад, про «неминучу поразку» або «корумпованість командування») не впливали на їхню здатність виконувати службові обов'язки? 3. Які специфічні заходи реагування можуть застосовувати правоохоронні органи України (Кіберполіція, СБУ) у разі виявлення ботоферм та центрів ІПСО, що фізично розташовані поза межами української юрисдикції (наприклад, у рф чи Китаї)?	6	9	*13 тиждень*

4. Види і зміст контрольних заходів

5.

Вид заняття/роботи	Вид поточного контрольного заходу	Зміст контрольного заходу*	Критерії оцінювання та термін виконання*	Усього балів
Поточний контроль				
Практичне заняття №1 кейс робота в малих групах	Групова практична вправа	Перевірка вміння студентів диференціювати види кіберзлочинів за міжнародними стандартами (Будапештська конвенція).	Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що	**4**
кейс	перевірка результатів аналітичного завдання (письмово або у формі виступу);	Перевірка розуміння студентами особливостей матеріального кримінального права в Будепашській конвенції		

			порушують закон, або не може пояснити логіку міркувань	
Практичне заняття №2 Кейс	перевірка результатів аналітичного завдання (письмово або у формі виступу);	Спроможність студента знайти в нормативному акті (Стратегії) алгоритми захисту банківської системи від DDoS-атак.	Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що порушують закон, або не може пояснити логіку міркувань	**2**
рефлексія	професійна дискусія	Здатність аргументувати управлінське рішення щодо розподілу сил і засобів у критичних умовах (технічний захист vs ІПСО)	**2 бали: аналітичний рівень.** Студент не лише описує досвід, а й аналізує причини успіху/помилок. **1 бал: Описовий**. Студент констатує факти, але не пояснює їх важливість. Аналіз поверхневий, висновки загального характеру. **0 балів: формальний.** Рефлексія відсутня, беззмістовна або не проведена.	**2**

Практичне заняття №3 Робота в малих групах, інтерактивний кейс, рефлексія	Моніторинг групової динаміки та оцінювання результатів командної роботи. Експертне оцінювання вирішення ситуаційної задачі (Case-study). Професійна дискусія	Здатність студентів до розподілу ролей, ефективної комунікації та досягнення спільного результату в обмежений час. Оцінюється повнота виконання поставленого завдання та здатність групи презентувати консолідовану позицію. Перевірка вміння студентів переносити теоретичні норми на практичні обставини. Викладач контролює правильність правової кваліфікації події, обґрунтованість обраного алгоритму дій та дотримання процедурних вимог (законності). Перевірка рівня усвідомлення вивченого матеріалу, здатності студента критично оцінювати власні рішення, виявляти прогалини у знаннях та проектувати отриманий досвід на майбутню професійну діяльність.	Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що порушують закон, або не може пояснити логіку міркувань	**2** **2** **2**
Практичне заняття №4 Опитування	Опитування фронтальне Індивідуально-комбіноване	Рівень володіння термінологією правильність, впевненність здатність до синтезу	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі	**2**

рефлексія	Професійна дискусія	Перевірка рівня усвідомлення вивченого матеріалу, здатності студента критично оцінювати власні рішення, виявляти прогалини у знаннях та проектувати отриманий досвід на майбутню професійну діяльність.	фактичні помилки або повне нерозуміння предмета обговорення. **2 бали: аналітичний рівень.** Студент не лише описує досвід, а й аналізує причини успіху/помилок. **1 бал: Описовий**. Студент констатує факти, але не пояснює їх важливість. Аналіз поверхневий, висновки загального характеру. **0 балів: формальний.** Рефлексія відсутня, беззмістовна або не проведена.	**2**
Практичне заняття №5 *Брейнстормінг*	Моніторинг творчої активності.	Контроль здатності до швидкої розробки тактичних варіантів вирішення кризової ситуації	Самостійність, правильність, повнота від **1** до **2** балів Неправильна – 0 балів	**2**
Інтерактивний кейс	Експертне оцінювання вирішення ситуаційної задачі (Case-study).	Контроль відповідності висунутих ідей нормам чинного законодавства та відомчим інструкціям МВС	Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що порушують закон, або	**2**

			не може пояснити логіку міркувань	
Практичне заняття №6 Ситуаційний кейс	Опитування фронтальне, індивідуально-комбіноване Експертне оцінювання вирішення ситуаційної задачі (Case-study).	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу Контроль відповідності висунутих ідей нормам чинного законодавства та відомчим інструкціям МВС	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі фактичні помилки або повне нерозуміння предмета обговорення.	**2** **2**
Практичне заняття №7 опитування рефлексія	Опитування фронтальне, індивідуально-комбіноване Професійна дискусія	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу Перевірка рівня усвідомлення вивченого матеріалу, здатності студента критично оцінювати власні	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі фактичні помилки або повне нерозуміння предмета обговорення. **2 бали: аналітичний рівень.** Студент не лише описує досвід, а й аналізує причини успіху/помилок.	**2** **2**

		рішення, виявляти прогалини у знаннях та проектувати отриманий досвід на майбутню професійну діяльність.	**1 бал: Описовий**. Студент констатує факти, але не пояснює їх важливість. Аналіз поверхневий, висновки загального характеру. **0 балів: формальний.** Рефлексія відсутня, беззмістовна або не проведена.	
Практичне заняття №8 Ситуаційні кейси (3 кейси)	Експертне оцінювання вирішення ситуаційної задачі (Case-study).	Контроль відповідності висунутих ідей нормам чинного законодавства та відомчим інструкціям МВС	Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що порушують закон, або не може пояснити логіку міркувань	**2** **2** **2**
Практичне заняття № 9	Опитування фронтальне, індивідуально-комбіноване	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах	**2**

			або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі фактичні помилки або повне нерозуміння предмета обговорення.	
Практичне заняття №10	Опитування фронтальне, індивідуально-комбі новане	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі фактичні помилки або повне нерозуміння предмета обговорення	**2**
кейс	Експертне оцінювання вирішення ситуаційної задачі (Case-study).	Контроль відповідності висунутих ідей нормам чинного законодавства та відомчим інструкціям МВС.	Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що порушують закон, або	**2**

			не може пояснити логіку міркувань	
Практичне заняття №11	аудит персональної цифрової безпеки (Self-Audit) з демонстрацією результатів.	Якість самоаналізу Технічна грамотність Критичний аудит дозволів: Дотримання протоколів конфіденційності	**7- 10 балів:** Студент виконав усі 4 пункти; виявив критичні вразливості у своєму «цифровому сліді» та обґрунтував, як налаштування 2FA та видалення повідомлень захищають оперативну інформацію. **5-6 бал:** Завдання виконано частково (наприклад, налаштовано 2FA, але не проведено аналіз дозволів застосунків); студент не може пояснити зв'язок між «цифровим слідом» та інформаційною безпекою. **2-4 балів:** Завдання не виконано; студент не обізнаний щодо налаштувань безпеки відсутні; студент ігнорує вимоги цифрової гігієни.	**10**
Практичне заняття № 12	Опитування фронтальне, індивідуально-комбі новане	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом.	**2**

			1 бал: Відповідь правильна по суті, але неповна, містить неточності в термінах або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі фактичні помилки або повне нерозуміння предмета обговорення	
Практичне заняття №13	Опитування фронтальне, індивідуально-комбіноване	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах або потребує навідних запитань викладача. **0 балів:** Відсутність відповіді, грубі фактичні помилки або повне нерозуміння предмета обговорення	**2**
Практичне заняття №14 Опитування	Опитування фронтальне, індивідуально-комбіноване	Оцінка рівня володіння термінологією правильність, впевненість здатність до синтезу	**2 бали:** Відповідь повна, вичерпна, з використанням професійної термінології та посиланнями на нормативну базу. Студент демонструє впевнене володіння матеріалом. **1 бал:** Відповідь правильна по суті, але неповна, містить неточності в термінах. **0 балів:** Відсутність відповіді, грубі фактичні помилки/ повне нерозуміння	**2**

кейс	Експертне оцінювання вирішення ситуаційної задачі (Case-study).	Оцінка розуміння студентами методики деконструкції маніпулятивних технік та розпізнавання штучної дестабілізації	предмета обговорення. Рівень: **Професійний – 2 бали** рішення цілісне, аргументоване нормами законод-ва та професійною логікою; **Адаптивний – 1 бал** Рішення прийнято, але обґрунтування є неповним або базується на загальних уявленнях без посилання на спеціальну нормативну базу та професійні стандарти **Низький – 0 балів** Студент не здатний прийняти рішення, пропонує дії, що порушують закон, або не може пояснити логіку міркувань	**2**
Усього за поточний контроль				**60**
Підсумков. семестр. контроль	Тестування	Підсумковий тест https://moodle.znu.edu.ua/course/view.php?id=18045	Правильна відповідь – 1 бал (усього 40 питань)	**40**
Усього				**100**

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 Стратегію кібербезпеки України: URL : рішення Ради національної безпеки і оборони України від 14 травня 2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text
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 Стратегію кібербезпеки України»: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text
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. 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. Положення про організаційно-технічну модель кіберзахисту. Затверджено постановою КМ України від 29 грудня 2021 р. № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-п#Text
15.Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури. Затверджені постановою КМ України від 19 червня 2019 року. № 518. URL:
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

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. Батраченко Т.С. , Розгон О.Г., Єфімова І.В. Застосування безпілотних літальних апаратів для фото-та відеозапису в діяльності Національної поліції України. *Юридичний науковий електронний журнал.* 2024. № 1. С. 486-488.
4. Підготовка поліцейських підрозділів превентивної діяльності, слідства, та дізнання, кіберполіцейських з питань убезпечення дітей у кіберпросторі : навч.-метод. посіб. / А. М. Апетик, А. Д. Дьякова, О. В. Ковальова [та ін.] ; за заг. ред. Т. В. Журавель, О. В. Ковальової. Київ : ГО «Волонтер», 2023. 232 с.
5. 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.
6. Боженко В. В., Кушнерьов О. С., Кільдей А. Д. Детермінанти поширення кіберзлочинності у сфері фінансових послуг. *Економічний форум*. 2021. № 4. С. 116– 121.
7. Вейц А.М. Особливості розслідування кіберзлочинів, вчинених у військовому середовищі. *Інформація і право*. 2024. № 4 (51). С. 233-242.
8. 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.
9. Воронов І.О. Криміналістичний аналіз кримінальних правопорушень у сфері використання комп'ютерів. *Юридичний бюлетень*. 2022. № 4. С. 180-186.
10. Гуржій С.В. Засади інституціонально-функціонального забезпечення кібербезпеки в сучасних умовах. Інформація і право. 2021. № 2 (37). С. 103-104.
11. Гуцалюк М.В. Особливості протидії кіберзлочинності під час воєнного стану. *Інформація і право.* 2023. № 3 (46). С. 108-117.
12. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі «Даркнет». *Інформація і право*. 2018. № 3 (26). С. 102-108.
13. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. № 1(28). С. 118-128.
14. 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.
15. 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
16. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : методичні матеріали для працівників підрозділів поліції / [уклад. В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов,В. В. Чумак, В. А. Світличний] ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 44 с.
17. 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

18. 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.
19. Колосовський В.Ю. Сучасний стан кібербезпеки України в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402-405.
20. 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.
21. Красніков С.А. Кібергігієна як чинник запобігання кіберзагрозам. *Нове українське право*. 2024. Вип. 6. С. 57-62.
22. 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.
23. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. № 5. С. 304-307.
24. 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.
25. 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.
26. Ньюман М. Історія кіберзлочинності: Від комп'ютерних вайрусів до кібервійн. К.: Видавництво «Наукова думка». 2019. 368 с.
27. 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.
28. Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери: науково-методичні рекомендації / О. В. Манжай. Х. : ХНУВС, 2019. 24 с.
29. 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.
30. 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.
31. 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.
32. Розвиток навичок кібергігієни. URL: https://ua.issp.com/_files/ugd/2d3fc0_8dc46933eb064737aea6b2bda0b01821.pdf
33. 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.
34. Рябчинська О.П. Протидія кіберзагрозам національній безпеці України: інституційно-превентивна спроможність. *Науковий вісник Ужгородського національного університету. Серія Право*. 2025. Випуск № 92. Ч.4. С. 206-214.

35. Рябчинська О.П. Темпоральні межі зберігання персональних даних правоохоронними та антикорупційними органами: загальний та спеціальний європейські стандарти. Право і суспільтство. 2025. № 4. С. 308-316.
36. Саєнко М.І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського Національного Університету. Серія ПРАВО*. 2021. Випуск 64. С. 386-391.
37. 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.
38. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса. 2020. 112 с.
39. Самойленко О. А. Діяльність правоохоронних органів у протидії кіберзлочинності [Текст] : навчально-методичний посібник / О. А. Самойленко. Одеса. 2020. 133 с.
40. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса: ТЕС, 2020. 372 с.
41. Самойленко О.А. Виявлення та розслідування кіберзлочинів. Одеса, 2020.112 с.
42. Сироїд Т. Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Актуальна юриспруденція. зб. матеріалів інтернет-конференції. Київ. 2018. С.77-80.
43. 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/
44. Федушко С. Сучасні підходи до дослідження кібербезпеки та кібергігієни в умовах цифрової трансформації суспільства. *Вісник Хмельницького національного університету*. 2023. № 3 (321). С. 210–213.
45. Хілько В. І. Кіберзахист: Теорія і практика. К.: Видавництво "Логос", 2020. 288 с.
46. Холлінс Т. Ж. Кіберзлочинність і кібербезпека: Основи, виклики та рішення. Дніпро: Видавництво «Ліга-Прес», 2021. 416 с.

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://reyestr.court.gov.ua – Офіційний сайт єдиного державного реєстру судових рішень України";
5. URL: http://www.rada.kiev.ua/laws/pravo/all/sites.htm – перелік серверів державних органів на сайті Верховної Ради України;
6. URL: https://supreme.court.gov.ua/supreme/ – Офіційний сайт Верховного Суду;
7. URL: http://www.minjust.gov.ua/ – Офіційний сайт Міністерства юстиції України;
8. URL: http://anticyber.com.ua – Кіберзлочинність: проблеми боротьби і прогнози. Антикібер Національне антикорупційне бюро.

7. Регуляції і політики курсу

Відвідування занять. Регуляція пропусків.

✓ **Обов'язковість відвідування занять**

Відвідування всіх лекційних та практичних занять є **обов'язковим** для здобувачів вищої освіти.

Систематичне відвідування занять розглядається як базова передумова успішного засвоєння навчального матеріалу та є складовою академічної дисципліни.

✓ **Активність здобувача під час заняття**

Якість участі здобувача у заняттях оцінюється за такими критеріями: виявлення зацікавленості, участь у дискусіях, аналіз правових ситуацій, виконання усних або письмових завдань у межах заняття. **Пасивна присутність на занятті не враховується як повноцінна участь** і може негативно вплинути на підсумкову оцінку за семестр.

✓ **Своєчасність виконання самостійної роботи**

Здобувачі зобов'язані виконувати завдання самостійної роботи **у встановлені строки**. Несвоєчасне подання завдань без поважних причин тягне за собою зниження оцінки. У разі об'єктивних обставин (хвороба, форс-мажор), здобувач має завчасно повідомити викладача та погодити нові строки.

✓ **Відпрацювання пропущених занять**

Пропущені заняття підлягають **обов'язковому відпрацюванню** у встановлений викладачем термін. Відпрацювання може здійснюватися у формі індивідуального усного опитування, письмової роботи, участі в додатковому практичному занятті або іншій формі, визначеній викладачем. Без відпрацювання пропущених занять здобувач не допускається до підсумкового контролю.

✓ **Обов'язковість особистої присутності на заліку/екзамені**

Особиста присутність здобувача вищої освіти на заліку або екзамені є **обов'язковою**. У разі неможливості з поважних причин (підтверджених належними документами) з'явитися на залік або екзамен у встановлений день, здобувач зобов'язаний повідомити про це не пізніше ніж за добу до проведення форми контролю. За умови належного підтвердження причини відсутності, йому буде призначено індивідуальний день складання.

Не допускається:

- ✓ пропуск занять без поважних причин;
- ✓ запізнення на заняття;
- ✓ користування телефонами для спілкування під час лекційних та практичних занять;
- ✓ списування та академічна недоброчесність**.**

Політика академічної доброчесності

Відповідно до Закону України «Про освіту» академічна доброчесність — це сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, складання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Академічна доброчесність здобувача вищої освіти полягає у:

1. **Самостійному виконанні навчальних завдань**, контрольних, тестових, індивідуальних, а також екзаменаційних і залікових випробувань без використання заборонених джерел, сторонньої допомоги або обману;
2. **Недопущенні плагіату** — умисного чи ненавмисного привласнення чужих ідей, текстів, досліджень, результатів без належного посилання на автора/джерело;
3. **Сумлінному дотриманні вимог навчальної дисципліни**, своєчасному та якісному виконанні завдань, виявленні поваги до праці викладача та до колективної роботи під час групових занять;
4. **Використанні лише достовірної інформації та перевірених джерел**, посиланні на наукові й нормативні матеріали коректним способом згідно з академічними стандартами;
5. **Недопущенні фальсифікації результатів навчання чи досліджень**, маніпулюванні з даними або створенні неправдивих результатів у письмових роботах;
6. **Утриманні від отримання неправомірної вигоди, списування, змови під час оцінювання**, замовлення робіт у третіх осіб (академічного шахрайства) або надання допомоги іншим у таких діях;

7. **Повагою до інтелектуальної власності**, дотриманням авторських прав і академічних етичних норм у всіх формах навчальної діяльності;
8. **Готовністю відповідати за свої дії та визнавати допущені помилки**, сприяючи формуванню культури доброчесності в академічному середовищі.

Використання комп'ютерів/телефонів на занятті
Використання електронних пристроїв під час занять дозволяється виключно у навчальних цілях та з дозволу викладача.
Під час виконання заходів контролю використання електронних пристроїв заборонено. У разі порушення цієї заборони роботу буде анульовано без права перескладання.

Комунікація
Основною платформою для комунікації викладача зі здобувачами є Moodle.
Важливі повідомлення регулярно розміщуються викладачем на форумі курсу.
Для персональних запитів використовується сервіс приватних повідомлень.

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, затвердженому Вченою радою ЗНУ від 25.02.2025 р. (протокол №8). (URL: https://sites.znu.edu.ua/navchalnyj_viddil/normatyvna_basa/polozhennya_zapor__z__kogo_nats__onal__nogo_un__versitetu_pro_poryadok_viznannya_rezul__tat__v_navchannya__zdobutikh_shlyakhom_neformal__noyi_ta_abo___nformal__noyi_osv__ti.pdf).

ДОДАТКОВА ІНФОРМАЦІЯ

ГРАФІК ОСВІТНЬОГО ПРОЦЕСУ НА 2025-2026 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://sites.znu.edu.ua/navchalnyj_viddil/normatyvna_basa/polozhennya_pro_organ__zats__yu_ta_metodiku_provedennya_potochnogo_ta_p__dsumkovogo_semestrovogo_kontrolyu_navchannya_student__v_znu_.pdf

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/