МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____Ігор ЯКИМЕНКО
«___» _____ 2023 р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____Віктор ОСТРОВЕРХОВ
«___» _____ 2023 р.

РОБОЧА ПРОГРАМА

з дисципліни

«НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ»

Ступінь вищої освіти – **бакалавр**
Галузь знань – **12 Інформаційні технології**
Спеціальність – **125 Кібербезпека**
Освітньо-професійна програма – **Кібербезпека**

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. роботи (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	Самост. робота студ. (год.)	Разом (год.)	Екзамен (семестр)
Денна	3	5	28	28	3	8	83	150	5

Тернопіль – 2023

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», затвердженої Вченою радою ЗУНУ протокол № 9 від 26.05.2021 р.

Робочу програму склали: завідувач кафедри кібербезпеки, д.т.н., професор Василь ЯЦКІВ та викладач кафедри кібербезпеки Сергій КУЛИНА.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 28.08.2023 р.

Завідувач кафедри Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол №1 від 30.08.2023 р.

Голова групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОПП Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Нормативно-правове забезпечення”

Дисципліна – «Нормативно-правове забезпечення»	**Галузь знань, спеціальність, ОПП, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань – 12 «Інформаційні технології»	Статус дисципліни – обов’язкова Мова навчання – українська
Кількість залікових модулів – 3	Спеціальність – 125 «Кібербезпека»	Рік підготовки: 3 Семестр: 5
Кількість змістових модулів – 3	Освітньо-професійна програма – «Кібербезпека»	Лекції: 28 год. Лабораторні заняття: 28 год.
Загальна кількість годин – 150	Ступінь вищої освіти – бакалавр	Індивідуальна робота: 3 год. Тренінг, КПІЗ: 8 год. Самостійна робота: 83 год.
Тижневих годин – 11, з них аудиторних – 4		Вид підсумкового контролю – іспит

2. Мета і завдання дисципліни “Нормативно-правове забезпечення”

2.1. Мета вивчення дисципліни

Мета дисципліни “Нормативно-правове забезпечення” полягає у формуванні в майбутніх спеціалістів умінь та компетенцій для визначення місця і ролі кібербезпеки у загальній системі національної безпеки, стану та принципів забезпечення інформаційної безпеки особистості, суспільства та держави, необхідних для подальшої роботи та оволодіння навичками застосування методів та засобів ефективного та безпекового поводження з інформацією незалежно від її походження та виду в умовах широкого використання сучасних інформаційних технологій.

Вивчення курсу «Нормативно-правове забезпечення» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи інформаційних технологій», «Алгоритми та структури даних», «Архітектура комп’ютерів та систем»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.2. Завдання вивчення дисципліни

В результаті вивчення курсу «Нормативно-правове забезпечення» студенти повинні:

– засвоїти основні фундаментальні поняття і закони нормативно-правового забезпечення кібербезпеки для їх використання в сучасних системах;

– розуміти взаємозв’язок інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;

– знати основи державної та міжнародної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки;

– знати основні закони, принципи та правила поводження з інформацією;

– виявляти реальні та потенційні загрози у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;

– знати основні методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;

– знати основні положення юридичної відповідальності за правопорушення в інформаційній сфері та зміст основних міжнародних договорів з питань інформаційної безпеки;

– розуміти основні проблеми правового забезпечення інформаційної безпеки.

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із головними питаннями курсу «Нормативно-правове забезпечення». Завдання проведення лекцій полягає у: викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Нормативно-правове забезпечення» та формуванні у студентів цілісної системи теоретичних знань з курсу «Нормативно-правове забезпечення».

Мета проведення практичних занять полягає у тому, щоб виробити у студентів практичні навички використання теоретичного матеріалу. Завдання проведення практичних занять полягає у глибшому засвоєнні та закріпленні теоретичних знань, одержаних на лекціях.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни

Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Нормативно-правове забезпечення» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів («Основи інформаційних технологій», «Алгоритми та структури даних», «Архітектура комп'ютерів та систем»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

2.5. Результати навчання

Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

Діяти на основі законодавчої та нормативно правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.

3. Програма навчальної дисципліни: «Нормативно-правове забезпечення»

Змістовий модуль 1. Нормативно-правові акти України

Тема 1. Учасники кіберпростору, кібербезпека, загальні питання управління безпекою

Основні терміни кібербезпеки. Взаємозв'язки у кіберпросторі. Класифікація учасників кіберпростору. Взаємодія учасників кіберпростору. Концепції ведення кібероборотьби. Фактори впливу на кібербезпеку. Модель управління інформаційною та кібербезпекою.

Тема 2. Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки в Україні

Ієрархії нормативних актів. Конституція України. Закон України «Про національну безпеку». Визначення термінів. Стратегія національної безпеки України. Закони України «Про інформацію», «Про доступ до публічної інформації», «Про захист персональних даних», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про радіочастотний ресурс», «Про телекомунікації», «Про захист суспільної моралі», «Про оборону України», «Про Збройні Сили України», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації».

Тема 3. Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення кібербезпеки в Україні

Указ Президента «Про Стратегію кібербезпеки України». Закон України «Про Основні засади розвитку інформаційного суспільства в Україні». Стратегія розвитку інформаційного суспільства в Україні. Закон України «Про Національну програму інформатизації». Закон України «Про Концепцію Національної програми інформатизації». Концепція формування системи національних електронних інформаційних ресурсів. Положення про Національний реєстр електронних інформаційних ресурсів. Закон України «Про захист персональних даних».

Тема 4. Нормативно-правові акти, які визначають порядок охорони державної таємниці в Україні

Закон України «Про державну таємницю». Визначення термінів. Законодавство України про державну таємницю. Державна політика щодо державної таємниці. Компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці. Реалізація прав на секретну інформацію та її матеріальні носії. Інформація, що може бути віднесена до державної таємниці. Строк дії рішення про віднесення інформації до державної таємниці.

Тема 5. Нормативно-правові акти з інформаційної безпеки телекомунікаційних систем

Закони України щодо інформаційної безпеки в Україні. Постанови Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 р. №373 та «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736. Нормативні документи в галузі технічного захисту інформації.

Змістовий модуль 2. Закони та державні стандарти України у сфері забезпечення технічного захисту інформації

Тема 6. Закони України про електронний документообіг та електронний цифровий підпис

Визначення термінів. Законодавство про електронні документи та електронний документообіг. Державне регулювання електронного документообігу. Електронний документ. Електронний підпис. Правовий статус електронного документа та його копії. Електронний документообіг. Перевірка цілісності електронного документа.

Тема 7. Підзаконні нормативні акти щодо електронного документообігу та електронного цифрового підпису

Закон України «Про концепцію Національної програми інформатизації». Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні». Указ Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади». Постанова Кабінету Міністрів України «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади».

Тема 8. Нормативно-правові акти, які визначають порядок технічного захисту інформації в Україні

Концепція технічного захисту інформації в Україні. Положення про технічний захист інформації в Україні. Закон «Про стандартизацію». Положення про порядок розроблення, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації.

Тема 9. Нормативно-правові акти у сфері захисту державних електронних інформаційних ресурсів України

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України». Закон України «Про захист інформації в інформаційно-комунікаційних системах». Закон України «Про електронну комерцію». Типова інструкція з документування управлінської інформації в електронній формі та організації роботи з електронними документами в діловодстві, електронного міжвідомчого обміну.

Тема 10. Державні стандарти України в сфері забезпечення технічного захисту інформації

ДСТУ 3396.0-96 «Захист інформації Технічний захист інформації. Основні положення». ДСТУ 3396.1-96 «Захист інформації Технічний захист інформації. Порядок проведення робіт». ДСТУ 3396.2-97 «Захист інформації Технічний захист інформації. Терміни та визначення».

4. Структура залікового кредиту дисципліни «Нормативно-правове забезпечення»

	Кількість годин					
	Лекції	Лаб. заняття	Інд. робота	Тренінг, КПІЗ	Самост. робота	Контрольні заходи
Змістовий модуль 1. Нормативно-правові акти України						
Тема 1. Учасники кіберпростору, кібербезпека, загальні питання управління безпекою.	2	2	1	4	6	Поточне опитування
Тема 2. Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки в Україні	4	4			8	
Тема 3. Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення кібербезпеки в Україні	4	4			8	
Тема 4. Нормативно-правові акти, які визначають порядок охорони державної таємниці в Україні	2	2			8	

Тема 5. Нормативно-правові акти з інформаційної безпеки телекомунікаційних систем	2	2			10	
Змістовий модуль 2. Закони та державні стандарти України у сфері забезпечення технічного захисту інформації						
Тема 6. Закони України про електронний документообіг та електронний цифровий підпис	4	4	1	4	8	Поточне опитування
Тема 7. Підзаконні нормативні акти щодо електронного документообігу та електронного цифрового підпису	2	2			8	
Тема 8. Нормативно-правові акти, які визначають порядок технічного захисту інформації в Україні	2	2			8	
Тема 9. Нормативно-правові акти у сфері захисту державних електронних інформаційних ресурсів України	2	2			8	
Тема 10. Державні стандарти України в сфері забезпечення технічного захисту інформації	4	4	1		11	
Разом	28	28	3	8	83	

5. Тематика лабораторних занять

Лабораторна робота №1

Тема: Реалізація політики менеджменту інформаційної безпеки між різними організаціями.

Мета: розглянути запропонований кейс та розробити конкретні пропозиції по реалізації політики менеджменту інформаційної безпеки стосовно запропонованих у кейсі аспектів.

Лабораторна робота №2

Тема: Реалізація політики менеджменту внутрішньої інформаційної безпеки.

Мета: розглянути запропонований кейс та розробити конкретні пропозиції по реалізації політики менеджменту інформаційної безпеки стосовно запропонованих у кейсі аспектів.

Лабораторна робота №3

Тема: Забезпечення фізичної безпеки в рамках менеджменту інформаційної безпеки.

Мета: розглянути запропонований кейс та запропонувати конкретні механізми реалізації цієї політики на підприємстві, наприклад: визначення контрольованої зони, засоби контролю, розміщення обладнання, кабельної мережі, небезпечних речовин, технічне обслуговування обладнання тощо.

Лабораторна робота №4

Тема: Забезпечення апаратно-програмних комплексів безпеки менеджменту інформаційної безпеки.

Мета: розглянути запропонований кейс та надати рекомендації щодо організації апаратно-програмних комплексів безпеки менеджменту інформаційної безпеки та

запропонувати конкретні механізми реалізації цієї політики на підприємстві, наприклад: захист від шкідливих програм, резервування інформації, мережева безпека, поводження з носіями інформації, моніторинг тощо.

Лабораторна робота №5

Тема: Зберігання відкритих даних.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту з отримання зберігання та використання відкритих даних.

Лабораторна робота №6

Тема: Захист персональних даних.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту з отримання зберігання та використання персональних даних клієнтів.

Лабораторна робота №7

Тема: Захист даних з обмеженим доступом.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту факультету з автентифікацією та зберіганням даних студентів.

Лабораторна робота №8

Тема: Захист персональних даних пацієнтів.

Мета: розглянути запропонований кейс та розробити пропозиції с точки зору виконання законодавства про персональні дані до технічного завдання (ТЗ) на розробку модуля сайту з отримання зберігання та використання персональних даних пацієнтів приватного кабінету.

6. Комплексне практичне індивідуальне завдання (КПІЗ).

Індивідуальне завдання з курсу «Нормативно-правове забезпечення» виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Метою виконання КПІЗ є дослідження та оволодіння навиками застосування відповідних нормативно-правових актів для конкретних задач кібербезпеки. Студенти повинні виконати один із варіантів:

1. Визначення сутності інформації.
2. Основні показники класифікації носіїв інформації.
3. Засоби передачі та сприйняття інформації.
4. Основні властивості інформації, які визначають її небезпечість.
5. Розкриття сутності інформаційної небезпеки.
6. Особисте бачення ролі та місця інформційної безпеки у життєдіяльнсті суспільства у сучасних умовах.
7. Визначення поняття «інформаційна безпека».
8. Розкриття сутності безпечності інформації.
9. Основні чинники, які впливають на небезпечність інформації.
10. Розкриття визначення поняття «безпека інформації».
11. Основні суб`єкти створення небезпечної інформації.
12. Основні чинники визначення об’єктів інформаційної небезпеки.
13. Основні чинники визначення ієрархії об’єктів інформаційної небезпеки.
14. Головний принцип, якій забезпечує необхідний рівень інформаційної безпеки
15. Об’єкти інформаційної небезпеки та їх обґрунтування.
16. Коротка характеристика прав суспільства в інформаційній сфері.

17. Коротка характеристика обов’язків держави в інформаційній сфері.
18. Основна об’єктивна причина складності правового забезпечення інформаційної безпеки.
19. Основні суб’єктивні причини складності правового забезпечення інформаційної безпеки.
20. Коротке обґрунтування визначення кібернетики як об`єкту небезпеки.
21. Сутність поняття «кібернетична безпека» (кібербезпека).
22. Чинники, які визначають взаємозв`язок понять «інформаційна безпека» та «кібербезпека».
23. Чинники, які визначають застосування термінів «інформаційна безпека» та «кібербезпека».
24. Сутність, поняття та правове визначення інформаційної діяльності.
25. Складові інформаційної діяльності.
26. Особисте розуміння співвідношення понять «національна безпека», «інформаційна безпека» та «кібернетична безпека».
27. Основні відмінності у сутності понять «інформаційна безпека» та «кібербезпека».
28. Чинники, які визначають взаємозв`язок інформаційної діяльності та інформаційної безпеки.
29. Сутність інформаційного насильства.
30. Суб’єкти інформаційної діяльності та їх вплив на процеси забезпечення інформаційної безпеки.
31. Основні чинники, які визначають особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.
32. Сутність маніпуляції.
33. Найбільше розповсюджені види маніпуляції.
34. Суб’єкти інформаційної діяльності та їх вплив на процеси забезпечення кібербезпеки.
35. Особливості маніпулювання свідомістю у сучасних умовах.
36. Наведіть приклади проявів інформаційного насильства.
37. Коротка оцінка ролі маніпулювання в системі державного управління.
38. Коротка оцінка місця маніпулювання в політичної системі.
39. Коротка оцінка ролі та місце маніпулювання в системі міжнародних відносин.
40. Трансформація ролі та значення інформації на різних етапах розвитку людства.
41. Перспективи розвитку та механізми здійснення інформаційного насильства.
42. Механізми впливу інформації на поведінку людини.
43. Тотожності та відмінності об’єктів інформаційної небезпеки та інформаційної безпеки.
44. Аргументуйте, чому інформаційна діяльність є апріорі небезпечною з точки національної безпеки.
45. Спрямованість розвитку інформаційної діяльності.
46. Роль та значення інформаційних ресурсів у розвитку людства.
47. Тенденції змін у системі доступу до інформаційних ресурсів.
48. Оцінка стану національного інформаційного суверенітету у сучасних умовах.
49. Чинники, які впливають на інформаційний суверенітет.
50. Витоки глобалізації інформаційного простору.
51. Механізми та засоби глобалізації інформаційного простору.
52. Основні принципові наслідки глобалізації інформаційного простору.
53. Структура нормативно-правової бази забезпечення захисту інформації.
54. Розкриття поняття «інформаційно-комунікаційна технологія» (ІКТ).
55. Розкриття понять «глобальна інформаційна система» та «глобальна мережа».
56. Природа тероризму.
57. Розкриття поняття «соціалізація»

58. Поняття об’єктності та суб`єктності в системі правовідносин.
59. Розкриття поняття «інформаційна технологія».
60. Розкриття поняття «інформаційна інфраструктура».

Виконання КПІЗ є одним із обов’язкових складових модулів залікового кредиту.

7. Тематика самостійної роботи

№ з/п	Тематика
1.	Тотожності та відмінності об`єктів інформаційної небезпеки та інформаційної безпеки.
2.	Об’єкти інформаційної діяльності.
3.	Суб’єкти інформаційної діяльності.
4.	Небезпечність інформаційної діяльності з точки зору національної безпеки.
5.	Спрямованість розвитку інформаційної діяльності.
6.	Загальне розуміння поняття «суверенітет».
7.	Чинники які впливають на інформаційний суверенітет.
8.	Оцінка стану національного інформаційного суверенітету в сучасних умовах
9.	Розуміння поняття «національна безпека» у сучасних умовах.
10.	Розуміння ролі та місця інформаційної безпеки в системі національної безпеки.
11.	Основні положення Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25.02.2017 р. № 47/2017.
12.	Основні положення Стратегії кібербезпеки України, затвердженої Указом Президента України від 15.03.2016 р. № 96/2016.
13.	Основні положення Стратегії національної безпеки України, затвердженої Указом Президента України від 06.05.2015 р. № 287/2015
14.	Основні положення Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537- V.
15.	Структура нормативно-правової бази забезпечення захисту інформації.
16.	Основні положення Закону України «Про телекомунікації» від 18.11.2003 р. № 1280- IV.
17.	Основні положення Закону України «Про інформацію» від 02.10.92 р. № 2657-XII.
18.	Розкриття поняття «інформаційно-комунікаційна технологія».
19.	Розкриття понять «глобальна інформаційна система» та «глобальна мережа».
20.	Природа тероризму.
21.	Розкриття поняття «соціалізація»
22.	Основні положення Конвенції Ради Європи « Про кіберзлочинність від 23.11.2001 р. № 994-575.
23.	Основні положення розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» Кримінального кодексу України.

8. Організація і проведення тренінгу

Тематика: Нормативно-правові інструменти та механізми протидії інформаційному насильству.

Порядок проведення:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.

3. Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

9. Методи навчання

У навчальному процесі використовуються: лекції, практичні та індивідуальні заняття, групова робота, реферування, а також методи опитування, тестування, ділові ігри тощо.

10. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Нормативно-правове забезпечення» використовуються наступні методи оцінювання навчальної роботи студентів:

- поточне тестування та поточне опитування;
- залікове модульне тестування та опитування;
- оцінювання виконання КПІЗ;
- ректорська контрольна робота;
- екзамен.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Нормативно-правове забезпечення» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4 (екзамен)
20 %	20 %	20 %	40 %
1. Поточне опитування на заняттях: 5 тем по 4 балів – max 20 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання: 4 завдань по 6 бали – max 24 балів	1. Поточне опитування на заняттях: 5 тем по 4 балів – max 20 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання: 4 завдань по 6 бали – max 24 балів	1. Підготовка КПІЗ – max 40 балів. 2. Захист КПІЗ – max 40 балів. 3. Виконання завдань на тренінгах – max 20 балів	1. Теоретичні питання: 3 питання по 20 балів – max 60 балів. 2. Практичне завдання – max 40 балів

Шкала оцінювання:

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	**За національною шкалою**	**За шкалою ECTS**
90-100	відмінно	A (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)

1-34		**F** (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№ з/п	Найменування	Номер теми
1.	Електронний варіант лекцій	1-10
2.	Методичні вказівки до виконання практичних робіт (електронний варіант)	1-10
3.	ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570.	1-10
4.	Microsoft Windows, Microsoft Office 2013, Mozilla Firefox, FoxitReader, AdobeReader, WinRAR, WinZip, DjVu Viewer, Total Commander	1-10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
3. Закон України «Про науково-технічну інформацію». URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text
4. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
5. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Закон України «Про державну таємницю». URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text
7. Закон України «Про захист персональних даних». URL: https://zakononline.com.ua/documents/show/306885___702634
8. Закон України «Про національну безпеку України». URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
9. Конвенція про кіберзлочинність, ратифікована Верховною Радою України 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
10. Постанова від 19 червня 2019 р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
11. ДСТУ 3396.0-96 Захист інформації Технічний захист інформації. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf
12. ДСТУ 3396.2-97 Захист інформації Технічний захист інформації. Терміни та визначення. URL: https://tzi.com.ua/downloads/%D0%94%D0%A1%D0%A2%D0%A3%203396.2-97.docx
13. Мельник М.І. «Правоохоронні органи та правоохоронна діяльність». -К.: «Атіка», 2019. – 576 с.
14. Правознавство: Підручник /За відп. ред. О.В. Дзери. – 10-е вид., перероб. і допов. - К.: Юрінком Інтер, 2019. – 848 с.
15. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І. В. Арістова, О. А. Баранов, О. П. Дзьобань

та ін.; за заг. ред. проф. К. І. Бєлякова. Київ:КВІЦ, 2019. 344 с..URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf

16. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315

17. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.2017 р. № 47 / Офіційний вісник Президента України. - 2017. - № 5. - С. 15.

18. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021 року. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

19. Стратегія національної безпеки України : Указ Президента України від 14 вересня 2020 року. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

20. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069

21. Стратегія воєнної безпеки України: Указ Президента України від 25 березня 2021 року № 121/2021 року. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n8.

22. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. URL: https://tzi.com.ua/downloads/2.5-004-99.pdf