ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Нормативно-правове забезпечення кібербезпеки

Галузь знань – F Інформаційні технології
Спеціальність – F5 Кібербезпека та захист інформації
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека та захист інформації
Обсяг дисципліни – 6 кредитів ЄКТС
Шифр дисципліни – ОФП.08
Мова навчання – Українська
Статус дисципліни – Обов'язкова (фахової підготовки)
Факультет – Інформаційних технологій
Кафедра – Кібербезпеки

Форма здобуття освіти	Курс	Семестр	Загальний обсяг		Кількість годин						Курсовий проєкт	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття					Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	3	5	6	180	66	32			34	114				+
Разом ДФН			**6**	**180**	**66**	**32**			**34**	**114**				**1**

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека та захист інформації» за спеціальністю F5 «Кібербезпека та захист інформації»

Робоча програма складена _____ канд. техн. наук, доцент Віктор ЧЕШУН
Підпис автора(ів) Науковий ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 29.08.2025 № 1. Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2025

ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ініціали, прізвище
Завідувач кафедри, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. Пояснювальна записка

Дисципліна «Нормативно-правове забезпечення кібербезпеки» є однією із дисциплін фахової підготовки і займає провідне місце у підготовці здобувачів першого (бакалаврського) рівня вищої освіти, очної (денної) (далі – денної) форми здобуття вищої освіти, які навчаються за освітньо-професійною програмою «Кібербезпека та захист інформації» в межах спеціальності F5 «Кібербезпека та захист інформації».

***Пререквізити*:** ОЗП.05 Англійська мова за професійним спрямуванням; ОФП.01 Основи інформаційної безпеки.

***Кореквізити**:* ОФП.10 Адміністрування та захист баз і сховищ даних; ОФП.11 Адміністрування та захист баз і сховищ даних (курсовий проєкт); ОФП.12 Комплексні системи захисту інформації; ОФП.13 Технології виявлення вразливостей та вторгнень; ОФП.14 Управління інформаційною безпекою; ОФП.15 Виробнича практика 1; ОФП.16 Виробнича практика 2.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

***компетентностей*:** ІК Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації; ЗК01 Здатність застосовувати знання у практичних ситуаціях; ЗК02 Знання та розуміння предметної області і розуміння професійної діяльності; ЗК03 Здатність спілкуватися державною мовою як усно, так і письмово; ЗК04 Здатність спілкуватися іноземною мовою; ЗК06 Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні; ЗК08 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; ФК01 Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

***програмних результатів навчання*:** ПРН01 Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків; ПРН02 Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації; ПРН04 Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН05 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ПРН06 Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат; ПРН07 Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; ПРН09 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

Мета дисципліни. Поглиблення знання та розуміння предметної області та розуміння професії щодо вимог нормативно-правових актів в сфері кібербезпеки та захисту інформації на рівні Законів України і Постанов КМУ , державних і міжнародних стандартів та інших нормативних документів тощо.

Предмет дисципліни. Закони та інші регулюючі акти України в сфері кібербезпеки та захисту інформації, міжнародні та національні стандарти інформаційної та кібербезпеки, передові практики та фреймворки нормативно-правового регулювання кібербезпеки.

Завдання дисципліни. Формування у здобувачів освіти системи знань і практичних навичок застосування законодавчої та нормативно-правової бази, а також державних та міжнародних вимог, практик і стандартів з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

Результати навчання. Після вивчення дисципліни студент повинен: *знати* та *застосовувати* законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації; *адаптуватися* до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат; з*астосовувати* знання у практичних ситуаціях, *аналізувати, аргументувати, приймати рішення* при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; *застосовувати* нормативно визначені поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; *застосовувати* знання державної та іноземних мов для вивчення міжнародних та національних стандартів, а також *використовувати* термінологію (державною та аншлійською мовами) цих стандартів з метою забезпечення ефективності професійної комунікації.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:		
	лекції	**семінарські заняття**	**СРС**
Тема 1. Становлення системи стандартизації в сфері кібербезпеки	6	6	20
Тема 2. Нормативно-правове регулювання інформаційної безпеки в Україні	18	18	60
Тема 3. Міжнародні практики нормативно-правового регулювання кібербезпеки	8	10	34
Разом:	**32**	**34**	**114**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотації	Кількість годин
	Тема 1. Становлення системи стандартизації в сфері кібербезпеки	**6**
1	**Початок стандартизації, веселкова серія стандартів інформаційної безпеки.** 1. Початок стандартизації в інформаційній безпеці. 2. Введення до веселкової серії. 3. Помаранчева книга (Критерії безпеки довірених комп'ютерних систем) як фундамент веселкової серії 4. Критичний аналіз помаранчевої книги 5. Червона книга веселкової серії (Трактування довірених мереж) 6. Зелена книга веселкової серії (Керуючі принципи використання паролів) 7. Жовто-коричнева книга (Керівництво до розуміння аудиту у довірених системах) Літ.: [3] с.23-28; [6] с.130-166	2
2	**Перші міжнародні стандарти Європи в галузі безпеки – ITSEC. Федеральні та Канадські критерії безпеки (стандарти FCITS і CTCPEC)** 1. Історичні умови створення ITSEC. 2. Основні положення ITSEC 3. Специфікації функцій безпеки стандарту ITSEC 4. Федеральні критерії безпеки інформаційних технологій FCITS 5. Канадські критерії безпеки комп'ютерних систем CTCPEC 6. Аналітичний висновок Літ.: [3] с.29-42; [6] с.190-217	2
3	**Загальні критерії оцінки безпеки інформаційних технологій** (стандарт **ISO/IEC** 15408), **стандарти Германії (BSI) та Великобританії (BS 7799)** 1. Загальні критерії оцінки безпеки інформаційних технологій 2. Угода про взаємне визнання сертифікатів 3. Стандарт Германії BSI 4. Стандарти Великобританії BS 7799 5. Міжнародний стандарт ISO 17799 6. Передумови появи серій міжнародних стандартів інформаційної безпеки Літ.: [3] с.42-45; [6] с.167-176, 190-217	2
	Тема 2. Нормативно-правове регулювання інформаційної безпеки в Україні	**18**
4	**Регулятивні складові інформаційної безпеки. Стратегії кібербезпеки та інформаційної безпеки України** 1. Регулятивні складові інформаційної безпеки 2. Становлення правового регулювання інформаційної безпеки в Україні 3. Стратегія кібербезпеки України 4. План реалізації Стратегії кібербезпеки України 5. Стратегія інформаційної безпеки України 6. План заходів з реалізації Стратегії інформаційної безпеки (на період до 2025 року*) Літ.: [1] с.1-14; [2] с.114-127; [5] с.195-214; [6] с.250-267; [7]; [8]	2
5	**Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки України** 1. Закон України «Про національну безпеку України» 2. Закон України «Про основні засади забезпечення кібербезпеки України» 3. Положення про організаційно-технічну модель кіберзахисту Літ.: [1] с.80-96; [2] с.56-61, 128-139; [5] с.215-228; [9]; [10]; [11]	2
6	**Нормативно-правове забезпечення захисту інформації в Законах України** 1. Закон України «Про інформацію» 2. Закон України «Про науково-технічну інформацію» 3. Закон України «Про доступ до публічної інформації» Літ.: [1] с.17-18, 28-36; [12]; [13]; [14]	2
7	**Нормативно-правове забезпечення захисту інформації в інформаційно-комунікаційних системах** 1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» Літ.: [1] с.58-80; [4] с.165-256; [15]	2
8	**Нормативно-правове забезпечення захисту персональних даних** 1. Закон України «Про захист персональних даних» Літ.: [1] с.36-46; [16]	2
9	**Нормативно-правове забезпечення захисту державної таємниці** 1. Закон України «Про державну таємницю» Літ.: [1] с.18-28, 47-57; [4] с.129-150; [17]	2

10	**Нормативно-правове забезпечення кіберзахисту об'єктів критичної інфраструктури** 1. Постанова КМУ від 19 червня 2019 року № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» 2. Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом Літ.: [1] с.96-98; [18]; [19]	2
11	**Технічний захист інформації – Державні Стандарти України** 1. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення 2. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт 3. ДСТУ 3396.2-97 Захист інформації .Технічний захист інформації. Терміни та визначення Літ.: [20]; [21]; [22]	2
12	**Технічний захист інформації – нормативні документи** 1. Загальний огляд НД ТЗІ 2. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» 3. НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» Літ.: [3] с.45-55; [23]	2
	Тема 3. Міжнародні практики нормативно-правового регулювання кібербезпеки	**8**
13	**Міжнарожні конвенції про боротьбу з кіберзлочинністю** 1. Конвенція Ради Європи «Про кіберзлочинність» 2. Додатковий протокол до Конвенції про кіберзлочинність 3. Конвенція ООН про боротьбу з кіберзлочинністю Літ.: [24]; [25]	2
14	**Серія міжнародних стандартів ISO/IEC 15408** 1. Склад серії міжнародних стандартів ISO/IEC 15408 2. ISO/IEC 15408-1 - Інформаційні технології. Кібербезпека та захист конфіденційності. Критерії оцінювання безпеки ІТ. Частина 1. Вступ та загальна модель 3. ISO/IEC 15408-2 - Інформаційні технології. Методи захисту.Критерії оцінювання. Частина 2. Функціональні вимоги 4. ISO/IEC 15408-3 - Інформаційні технології. Методи захисту. Критерії оцінювання. Частина 3. Вимоги до гарантії безпеки Літ.: [6] с.268-288; [26]; [27]; [28]; [29]; [30]	2
15	**Серія міжнародних стандартів ISO/IEC 27xxx** 1. Склад серії міжнародних стандартів ISO/IEC 27xxx 2. ISO/IEC 27000 - Інформаційні технології. Методи захисту. Системи менеджменту інформаційної безпеки. Огляд і словник термінів 3. ISO/IEC 27001 - Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги 4. ISO/IEC 27002 – Інформаційна безпека, кібербезпека та захист конфіденційності. Заходи забезпечення інформаційної безпеки 5. ISO/IEC 27003 - Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова Літ.: [6] с.268-288; [31]; [32]; [33]; [34]	2
16	**Регламенти Європейського Парламенту і Ради (ЄС)** 1. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року «Про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій» 2. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) Літ.: [35]; [36]	2
	Разом:	**32**

5.2 Зміст семінарських занять

№ з/п	Теми семінарських занять	Кількість годин
	Тема 1. Становлення системи стандартизації в сфері кібербезпеки	**6**
1	**Веселкова серія стандартів інформаційної безпеки.** Літ.: [3] с.23-28; [6] с.130-166	2
2	**Критерії оцінки безпеки інформаційних технологій ITSEC, федеральні критерії безпеки інформаційних технологій FCITS, Канадські критерії безпеки комп'ютерних систем і CTCPEC** Літ.: [3] с.29-42; [6] с.190-217	2
3	**Загальні критерії оцінки безпеки інформаційних технологій ISO/IEC** 15408, **Посібник із захисту інформаційних технологій для базового рівня захищеності BSI, Стандарт Великобританії BS 7799** Літ.: [3] с.42-45; [6] с.167-176, 190-217	2
	Тема 2. Нормативно-правове регулювання інформаційної безпеки в Україні	**18**
4	**Стратегія кібербезпеки України та план заходів з реалізації Стратегії** Літ.: [1] с.1-14; [2] с.114-127; [5] с.195-214; [6] с.250-267; [7]; [8]	2
5	**Нормативно-правові акти, які закріплюють концептуальні положення кібербезпеки України** Літ.: [1] с.80-96; [2] с.56-61, 128-139; [5] с.215-228; [9]; [10]; [11]	2
6	**Нормативно-правове забезпечення захисту інформації в Законах України** Літ.: [1] с.17-18, 28-36; [12]; [13]; [14]	2
7	**Нормативно-правове забезпечення захисту інформації в інформаційно-комунікаційних системах** Літ.: [1] с.58-80; [4] с.165-256; [15]	2
8	**Нормативно-правове забезпечення захисту персональних даних** Літ.: [1] с.36-46; [16]	2
9	**Нормативно-правове забезпечення захисту державної таємниці** Літ.: [1] с.18-28, 47-57; [4] с.129-150; [17]	2
10	**Нормативно-правове забезпечення кіберзахисту об'єктів критичної інфраструктури** Літ.: [1] с.96-98; [18]; [19]	2
11	**ДСТУ 3396 - Захист інформації. Технічний захист інформації.** Літ.: [20]; [21]; [22]	2
12	**Технічний захист інформації – нормативні документи** Літ.: [3] с.45-55; [23]	2
	Тема 3. Міжнародні практики нормативно-правового регулювання кібербезпеки	**10**
13	**Конвенція Ради Європи «Про кіберзлочинність» та Додатковий протокол до Конвенції** Літ.: [24]; [25]	2
14	**Серія міжнародних стандартів ISO/IEC 15408** Літ.: [6] с.268-288; [26]; [27]; [28]; [29]; [30]	2
15	**Серія міжнародних стандартів ISO/IEC 27xxx** Літ.: [6] с.268-288; [31]; [32]; [33]; [34]	2
16	**Регламенти Європейського Парламенту і Ради (ЄС)** Літ.: [35]; [36]	2
17	Узагальнююче заняття	2
	Разом:	**34**

5.4 Зміст самостійної (у т.ч. індивідуальної) роботи здобувача вищої освіти

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до семінарських занять, тестування, тощо. Крім цього до послуг студентів сторінка навчальної дисципліни у Модульному середовищі для навчання, де розміщені Робоча програма дисципліни та необхідні документи з її навчально-методичного забезпечення.

Номер тижня	Вид самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу Т1, підготовка до семінарського заняття №1.	6
2	Опрацювання теоретичного матеріалу Т1, підготовка до семінарського заняття №2.	6
3	Опрацювання теоретичного матеріалу Т1, підготовка до семінарського заняття №3. Тестування.	7
4	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №4.	7
5	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №5.	7
6	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №6.	7
7	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №7.	6
8	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №8.	6
9	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №9.	6
10	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №10.	7
11	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №11.	7
12	Опрацювання теоретичного матеріалу Т2, підготовка до семінарського заняття №12. Тестування.	7
13	Опрацювання теоретичного матеріалу Т3, підготовка до семінарського заняття №13.	7
14	Опрацювання теоретичного матеріалу Т3, підготовка до семінарського заняття №14.	7
15	Опрацювання теоретичного матеріалу Т3, підготовка до семінарського заняття №15.	7
16	Опрацювання теоретичного матеріалу Т3, підготовка до семінарського заняття №16.	7
17	Опрацювання теоретичного матеріалу. Тестування.	7
	Разом:	**114**

***Примітки*:** Т – тема навчальної дисципліни

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних технологій та методів. Зокрема, лекції проводяться з використанням словесних, наочних, інтерактивних та проблемних методів з супроводом мультимедійних технологій та презентаційних матеріалів; семінарські заняття – з використанням частково-пошукових методів, технологій ситуативного, позиційного та контекстного навчання; самостійна робота – з використанням пояснювально-ілюстративних та частково-пошукових методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час аудиторних семінарських занять, а також у дні проведення контрольних заходів, встановлених робочою програмою і графіком освітнього процесу, в т.ч. з використанням Модульного середовища для навчання. При цьому використовуються такі методи поточного контролю:

– оцінювання результатів роботи на семінарських заняттях (опитування теоретичного матеріалу, участь у обговоренні ситуацій);

– тестовий контроль засвоєння теоретичного та практичного матеріалу дисципліни.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контролю, який проводиться з усього матеріалу дисципліни за білетами, попередньо розробленими і затвердженими на засіданні кафедри. Здобувач вищої освіти, який набрав з будь-якого виду навчальної роботи, суму балів нижчу за 60 відсотків від максимального балу, не допускається до семестрового контролю, поки не виконає обсяг роботи, передбачений Робочою програмою. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу) з усіх видів поточного контролю і не склав іспит, вважається таким, який має академічну заборгованість. Ліквідація академічної заборгованості із семестрового контролю здійснюється у період екзаменаційної сесії або за графіком, встановленим деканатом відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ».

8. Політика дисципліни

Політика навчальної дисципліни загалом визначається системою вимог до здобувача вищої освіти, що передбачені чинними положеннями Університету про організацію і навчально-методичне забезпечення освітнього процесу. Зокрема, відвідування занять з дисципліни є обов'язковим. За об'єктивних причин (підтверджених документально) теоретичне навчання за погодженням із лектором може відбуватись в он-лайн режимі. Успішне опанування дисципліни і формування фахових компетентностей і програмних результатів навчання передбачає необхідність підготовки до семінарських занять (вивчення теоретичного матеріалу з теми заняття), активно працювати на занятті, брати участь у дискусіях тощо.

Здобувачі вищої освіти мають дотримуватися встановлених термінів виконання всіх видів навчальної роботи відповідно до робочої програми навчальної дисципліни. Пропущене семінарське заняття студент зобов'язаний відпрацювати у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння студентом теоретичного матеріалу з дисципліни оцінюється за результатами опитування під час семінарських занять й тестуванням.

Здобувач вищої освіти, виконуючи завдання семінарських занять і тестів з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення порушення політики академічної доброчесності в будь-яких видах навчальної роботи здобувач вищої освіти отримує незадовільну оцінку і має повторно виконати завдання з відповідної теми (виду роботи), що передбачені робочою програмою. Будь-які форми порушення академічної доброчесності ***не допускаються.***

У межах вивчення навчальної дисципліни здобувачам вищої освіти передбачено визнання і зарахування результатів навчання, набутих шляхом неформальної освіти, що розміщені на доступних платформах, які сприяють формування компетентностей і поглибленню результатів навчання, визначених робочою програмою дисципліни, або забезпечують вивчення відповідної теми та/або виду робіт з програми навчальної дисципліни (детальніше у Положенні про порядок визнання та зарахування результатів навчання здобувачів вищої освіти у ХНУ).

9. Оцінювання результатів навчання студентів у семестрі

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». При поточному оцінюванні виконаної здобувачем роботи з кожної структурної одиниці і отриманих ним результатів викладач виставляє йому певну кількість балів із встановлених Робочою програмою для цього виду роботи. При цьому кожна структурна одиниця навчальної роботи може бути зарахована, якщо здобувач набрав не менше 60 відсотків (мінімальний рівень для позитивної оцінки) від максимально можливої суми балів, призначеної структурній одиниці.

При оцінюванні результатів навчання здобувачів вищої освіти з будь-якого виду навчальної роботи (структурної одиниці) рекомендується використовувати наведені нижче узагальнені критерії:

Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти

Оцінка та рівень досягнення здобувачем запланованих ПРН та сформованих компетентностей	**Узагальнений зміст критерія оцінювання**
Відмінно (високий)	Здобувач вищої освіти глибоко і у повному обсязі опанував зміст навчального матеріалу, легко в ньому орієнтується і вміло використовує понятійний апарат; уміє пов'язувати теорію з практикою, вирішувати практичні завдання, впевнено висловлювати і обґрунтовувати свої судження. Відмінна оцінка передбачає логічний виклад відповіді мовою викладання (в усній або у письмовій формі). Здобувач не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки, демонструє практичні навички з вирішення фахових завдань. При відповіді допустив дві–три несуттєві ***похибки***.
Добре (середній)	Здобувач вищої освіти виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом, орієнтується у вивченому матеріалі; свідомо використовує теоретичні знання для вирішення практичних задач; виклад відповіді грамотний, але у змісті і формі відповіді можуть мати місце окремі неточності, нечіткі формулювання правил, закономірностей тощо. Відповідь здобувача вищої освіти будується на основі самостійного мислення. Здобувач вищої освіти у відповіді допустив дві–три ***несуттєві помилки***.
Задовільно (достатній)	Здобувач вищої освіти виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та практичної діяльності за професією, справляється з виконанням практичних завдань, передбачених програмою. Як правило, відповідь здобувача вищої освіти будується на рівні репродуктивного мислення, здобувач вищої освіти має слабкі знання структури навчальної дисципліни, допускає неточності і ***суттєві помилки*** у відповіді, вагається при відповіді на видозмінене запитання. Разом з тим, набув навичок, необхідних для виконання нескладних практичних завдань, які відповідають мінімальним критеріям оцінювання і володіє знаннями, що дозволяють йому під керівництвом викладача усунути неточності у відповіді.
Незадовільно (недостатній)	Здобувач вищої освіти виявив розрізнені, безсистемні знання, не вміє виділяти головне і другорядне, допускається помилок у визначенні понять, перекручує їх зміст, хаотично і невпевнено викладає матеріал, не може використовувати знання при вирішенні практичних завдань. Як правило, оцінка «незадовільно» виставляється здобувачеві вищої освіти, який не може продовжити навчання без додаткової роботи з вивчення навчальної дисципліни.

Структурування дисципліни за видами навчальної роботи і оцінювання результатів навчання студентів

Аудиторна робота						**Контрольні заходи**			**Семестровий контроль**	
Семінарські заняття №						Тестовий контроль			Іспит	Разом балів
1-3	4-6	7-9	10-12	13-14	15-16	Т 1	Т 2	Т 3		
Кількість балів за кожний вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	6-10	6-10	6-10	24-40	**60-100***
18-30						**18-30**			**24-40***	

Примітки: *За набрану з будь-якого виду навчальної роботи з дисципліни кількість балів, нижче встановленого мінімуму, здобувач отримує незадовільну оцінку і має її перездати у встановлений викладачем (деканом) термін. Інституційна оцінка встановлюється відповідно до таблиці «**Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС**».

Оцінювання на семінарських заняттях

Оцінка, яка виставляється за семінарське заняття, складається з таких елементів: усне опитування студентів на знання теоретичного матеріалу з теми, вільне володіння студентом термінологією дисципліни, уміння обґрунтувати прийняті рішення при розв'язуванні типових ситуацій.

При оцінюванні семінарського заняття викладач керується узагальненими критеріями, наведеними у таблиці «**Критерії оцінювання навчальних досягнень здобувача вищої освіти**» (мінімальний позитивний бал – 3 бали, максимальний – 5 балів).

Оцінювання результатів тестового контролю

Кожний з тестів, передбачених Робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним.

Відповідно до таблиці структурування видів робіт за тестовий контроль здобувач залежно від кількості правильних відповідей може отримати від 6 до 10 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	**0-55**	**60**	**65**	**70**	**75**	**80**	**85**	**90**	**95**	**100**
Кількість отриманих балів	0	6	7		8		9		10	

На тестування відводиться 30 хвилин. Студент проходить тестування в он-лайн режимі у Модульному середовищі для навчання. Також, студент може проходити тестування письмово, записуючи правильні відповіді у талоні відповідей. При отриманні негативної оцінки тест слід перездати до терміну ***наступного*** контролю.

Оцінювання результатів підсумкового семестрового контролю (іспит)

Освітня програма передбачає підсумковий семестровий контроль з дисципліни у формі іспиту, завданням якого є системне й об'єктивне оцінювання як теоретичної, так і практичної підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами. Відповідно до цього в екзаменаційному білеті пропонується поєднання питань як теоретичного , так і практичного характеру (в т.ч. у тестовій формі).

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів денної форми навчання (40 балів для підсумкового контролю)

Види завдань	**Для кожного окремого виду завдань**		
	Мінімальний (достатній) бал (задовільно)	**Потенційні позитивні бали* (середній бал) (добре)**	**Максимальний (високий) бал (відмінно)**
Теоретичне питання № 1	6	8	10
Теоретичне питання № 2	6	8	10
Тестові завдання	12	16	20
Разом:	**24**		**40**

Примітка. *Позитивний бал за іспит, відмінний від мінімального (24 бали) та максимального (40 балів), знаходиться в межах 25-39 балів та розраховується як сума балів за усі структурні елементи (завдання) іспиту.

Відповідно до таблиці **оцінювання результатів підсумкового семестрового контролю** за тестові завдання здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 балів.

Розподіл балів в залежності від наданих правильних відповідей на тестові завдання підсумкового контролю

Кількість правильних відповідей	0-11	12	13	14	15	16	17	18	19	20
Відсоток правильних відповідей	**0-55**	**60**	**65**	**70**	**75**	**80**	**85**	**90**	**95**	**100**
Кількість отриманих балів	0	12	13	14	15	16	17	18	19	20

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання у балах з усіх видів навчальної роботи до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС наведені нижче у таблиці «Співвідношення».

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав студент з дисципліни за результатами поточного контролю, знаходиться у межах від 60 до 100 балів. При цьому за інституційною шкалою ставиться оцінка

«відмінно/добре/задовільно», а за шкалою ЄКТС – буквене позначення оцінки, що відповідає набраній студентом сумі балів відповідно до таблиці Співвідношення.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	**Рейтингова шкала балів**	**Інституційна оцінка** (рівень досягнення здобувачем вищої освіти запланованих результатів навчання з навчальної дисципліни)	
		Залік	**Іспит/диференційований залік**
A	90-100	Зараховано	***Відмінно*/*Excellent*** – високий рівень досягнення запланованих результатів навчання з навчальної дисципліни, що свідчить про безумовну готовність здобувача до подальшого навчання та/або професійної діяльності за фахом
B	83-89		***Добре*/*Good*** – середній (максимально достатній) рівень досягнення запланованих результатів навчання з навчальної дисципліни та готовності до подальшого навчання та/або професійної діяльності за фахом ***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
C	73-82		
D	66-72		
E	60-65		
FX	40-59	Незараховано	***Незадовільно*/*Fail*** – Низка запланованих результатів навчання з навчальної дисципліни відсутня. Рівень набутих результатів навчання є недостатнім для подальшого навчання та/або професійної діяльності за фахом
F	0-39		***Незадовільно*/*Fail*** – Результати навчання відсутні

10. Питання для самоконтролю результатів навчання

1. Правове, нормативне і регулятивне забезпечення інформаційної безпеки.
2. Початок стандартизації в інформаційній безпеці. Веселкова серія (Веселкові книги) – короткий огляд серії стандартів.
3. Помаранчева книга TCSEC (Trusted Computer System Evaluation Criteria) як фундамент веселкової серії. Категорії вимог щодо безпеки.
4. Класи захисту і рівні захищеності стандарту TCSEC (Trusted Computer System Evaluation Criteria - помаранчева книга).
5. Критичний аналіз помаранчевої книги
6. Трактування довірених мереж TNI (Trusted Network Interpretation – червона книга) як розвиток TCSEC.
7. Зелена та біла книга веселкової серії як основа стандарів Європи.
8. ITSEC як перші міжнародні стандарти Європи в галузі ІБ. Передумови і цілі створення. Основні положення ITSEC.
9. Специфікації функцій безпеки стандарту ITSEC.
10. Класи функцій безпеки стандарту ITSEC.
11. Федеральні критерії безпеки інформаційних технологій FCITS
12. Канадські критерії безпеки комп'ютерних систем CTCPEC
13. Загальні критерії безпеки інформаційних технологій (Common Criteria for Information Technology Security Evaluation) – передумови і основні цілі створення, етапи розвитку, основні іноваційні досягнення.
14. Аналітичний огляд основних розділів загальних критеріїв безпеки інформаційних технологій.
15. Задачі захисту (Security Objectives), Профіль захисту (Protection Profile) і Завдання з безпеки (Security Target) в концепції загальних критеріїв безпеки інформаційних технологій.
16. Функціональні вимоги, вимоги і рівні адекватності в концепції загальних критеріїв безпеки інформаційних технологій.
17. Угода про взаємне визнання сертифікатів.
18. Стандарт Германії BSI – основні нововведення, загальна методологія і компоненти управління інформаційною безпекою.
19. Стандарт Германії BSI – план здійснення аналізу, класифікація видів загроз і контрзаходів.
20. Стандарти Великобританії BS 7799
21. Міжнародний стандарт ISO 17799 (розвиток BS 7799)
22. Серії міжнародних стандартів інформаційної безпеки – передумови появи та загальні тенденції.
23. Міжнародні стандарти безпеки інформаційних технологій серія ISO/IEC 13335.
24. Серія ISO/IEC 15408 - Інформаційні технології: методи захисту - критерії оцінки.
25. Міжнародні стандарти для системи управління інформаційною безпекою ISO 27xxx
26. Закон України «Про основні засади забезпечення кібербезпеки України» – положення щодо принципів застосування.
27. Закон України «Про основні засади забезпечення кібербезпеки України» – об’єкти кібербезпеки та кіберзахисту
28. Закон України «Про основні засади забезпечення кібербезпеки України» – суб’єкти забезпечення кібербезпеки.
29. Об’єкти критичної інфраструктури в Законі України «Про основні засади забезпечення кібербезпеки України».
30. Закон України «Про основні засади забезпечення кібербезпеки України» – принципи забезпечення кібербезпеки.
31. Закон України «Про основні засади забезпечення кібербезпеки України» – національна система

кібербезпеки: визначення, суб’єкти, функціонування.

32. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA в Законі України «Про основні засади забезпечення кібербезпеки України».
33. Закон України «Про захист інформації в інформаційно-комунікаційних системах» – об'єкти захисту в системі та суб'єкти відносин, пов'язаних із захистом інформації в ІКС.
34. Закон України «Про захист інформації в інформаційно-комунікаційних системах» – відносини між суб'єктами відносин, пов'язаних із захистом інформації в ІКС.
35. Закон України «Про захист інформації в інформаційно-комунікаційних системах» – доступ до інформації та забезпечення захисту інформації в системі.
36. Закон України «Про захист інформації в інформаційно-комунікаційних системах» – умови обробки інформації в системі.
37. Закон України «Про захист інформації в інформаційно-комунікаційних системах» – повноваження державних органів у сфері захисту інформації в системах.
38. Закон України «Про інформацію» – основні принципи інформаційних відносин та державна інформаційна політика
39. Закон України «Про інформацію» – суб'єкти і об'єкт інформаційних відносин.
40. Закон України «Про інформацію» – доступ до інформації, інформація з обмеженим доступом та інформація із забороною обмеження доступу. Суспільно необхідна інформація.
41. Закон України «Про інформацію» – право на інформацію, гарантії і охорона права на інформацію.
42. Закон України «Про інформацію» – види інформації.
43. Закон України «Про інформацію» – відповідальність за порушення законодавства про інформацію, звільнення від відповідальності.
44. Закон України «Про науково-технічну інформацію» – об’єкт та суб’єкти відносин у сфері науково-технічної інформації.
45. Закон України «Про науково-технічну інформацію» – правовий режим науково-технічної інформації.
46. Закон України «Про науково-технічну інформацію» – національна система науковотехнічної інформації.
47. Закон України «Про науково-технічну інформацію» – ринок науково-технічної інформації.
48. Закон України «Про науково-технічну інформацію» – державна політика у сфері науково-технічної інформації.
49. Закон України «Про науково-технічну інформацію» –міжнародне співробітництво у сфері науково-технічної інформації.
50. Закон України «Про державну таємницю» – сфера дії Закону, компетенція державних органів, органів місцевого самоврядування та їх посадових осіб у сфері охорони державної таємниці
51. Закон України «Про державну таємницю» – поняття доступу і допуску до державної таємниці, режим секретності і категорія режиму секретності, ступінь секретності і гриф секретності.
52. Закон України «Про державну таємницю» – інформація, що може бути віднесена до державної таємниці; інформація, що не може бути віднесена до державної таємниці.
53. Закон України «Про державну таємницю» – порядок віднесення інформації до державної таємниці.
54. Закон України «Про державну таємницю» – державні експерти з питань таємниць: роль, права та обов’язки.
55. Закон України «Про державну таємницю» – вимоги до рішення державного експерта з питань таємниць.
56. Закон України «Про державну таємницю» – звід відомостей, що становлять державну таємницю.
57. Закон України «Про державну таємницю» – строки дії рішень про віднесення інформації до державної таємниці.
58. Закон України «Про державну таємницю» – засекречування та розсекречування матеріальних носіїв інформації.
59. Закон України «Про державну таємницю» – основні організаційно-правові заходи щодо охорони державної таємниці.
60. Закон України «Про державну таємницю» – дозвільний порядок провадження діяльності, пов'язаної з державною таємницею, та режим секретності.
61. Закон України «Про державну таємницю» – режимно-секретні органи.
62. Закон України «Про державну таємницю» – допуск громадян до державної таємниці та відмова у наданні допуску.
63. Закон України «Про державну таємницю» – перевірка громадян у зв'язку з допуском їх до державної таємниці, переоформлення допуску до державної таємниці, підвищення або зниження його форми та скасування.
64. Закон України «Про державну таємницю» – доступ громадян до державної таємниці.
65. Закон України «Про державну таємницю» – контроль за забезпеченням охорони державної таємниці та нагляд за додержанням законодавства про державну таємницю.
66. Закон України «Про державну таємницю» – відповідальність за порушення законодавства про державну таємницю.
67. Закон України «Про захист персональних даних» – об'єкти захисту і суб'єкти відносин, пов'язаних із персональними даними.
68. Закон України «Про захист персональних даних» – загальні та особливі вимоги до обробки персональних даних.
69. Закон України «Про захист персональних даних» – права суб'єкта персональних даних.
70. Закон України «Про захист персональних даних» – порядок доступу до персональних даних.
71. Закон України «Про захист персональних даних» – збирання, накопичення та зберігання, використання та поширення персональних даних. Відстрочення або відмова у доступі до персональних даних.
72. Закон України «Про захист персональних даних» – обробка персональних даних: підстави, повідомлення.
73. Закон України «Про захист персональних даних» – забезпечення захисту персональних даних.

11. Навчально-методичне забезпечення

Освітній процес з дисципліни «Нормативно-правове забезпечення кібербезпеки» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання:

1. Курс «Нормативно-правове забезпечення кібербезпеки»: https://msn.khmnu.edu.ua/course/view.php?id=6583

12. Матеріально-технічне та програмне забезпечення дисципліни (за потреби)

Інформаційна та комп'ютерна підтримка: ПК, планшет, смартфон або інший мобільний пристрій, мультимедійний проєктор. Програмне забезпечення: програми Microsoft Office або аналогічні, доступ до мережі Інтернет.

Вивчення навчальної дисципліни не потребує використання спеціального програмного прикладного забезпечення, крім загальновживаних програм і операційних систем.

13. Рекомендована література

Основна

1. Кушнір М. Я., Цеханський В. Д. Законодавчі питання інформаційної безпеки: Електронний навчальний посібник. Чернівці : Чернівецький національний університет, 2024. 102 с. URL: https://drive.google.com/file/d/1r7JUzLpdq-RM2Oq-iDM_Uzk3nG4V2wAC/view
2. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук та ін. Ірпінь: Державний податковий університет, 2024. 202 с. URL: https://dpu.edu.ua/images/Documents/NAUKA/Naukova%20biblioteka/Navcalno-metodicna%20literatura/N/Pravove%20reguluvanna%20nacionalnoi%20bezpeki.pdf
3. Потенко О.С. Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз : дис. … канд. техн. наук : 05.13.21, Київ, 2024. 172 с. URL: https://ipme.kiev.ua/docs/Potenko/Dis_Potenko.pdf
4. Кримінально-правова охорона інформаційної безпеки в Україні: монографія / В. І. Борисов та ін.; за заг. ред. В. І. Борисова, О. О. Пащенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 328 с. DOI: https://doi.org/10.31359/9786178518899.
5. Основи кіберпростору, кібербезпеки та кіберзахисту. навч. посіб. / В. М. Богуш та ін.. К.: Видавництво Ліра-К, 2022. 554 с.
6. Організаційно-правові основи забезпечення кібербезпеки / А. І. Марущак та ін. К.: Видавництво Ліра-К, 2023. 309 с.
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28 грудня 2021 року № 685/2021. URL: https://izmail.maup.com.ua/biblioteka/akademichna-dobrochesnist2/dstu-8302-2015/prikladi-oformlennya-bibliografichnih-posilan-dstu-8302-2015 (дата звернення: 28.08.2025).
8. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text (дата звернення: 28.08.2025).
9. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : редакція від 09.08.2024. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 28.08.2025).
10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 28.08.2025).
11. Про затвердження Положення про організаційно-технічну модель кіберзахисту : Постанова Кабінету Міністрів України; Положення від 29.12.2021 № 1426 : редакція від 26.12.2024. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text (дата звернення: 28.08.2025).
12. Про інформацію : Закон України від 02.10.1992 № 2657-XII : редакція від 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 28.08.2025).
13. Про науково-технічну інформацію : Закон України від 25.06.1993 № 3322-XII : редакція від 19.04.2014. URL: https://zakon.rada.gov.ua/laws/show/3322-12#Text (дата звернення: 28.08.2025).
14. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : редакція від 08.08.2025. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 28.08.2025).
15. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : редакція від 20.04.2025. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 28.08.2025).
16. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : редакція від 14.06.2025. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 28.08.2025).
17. Про державну таємницю : Закон України від 21.01.1994 № 3855-XII : редакція від 30.10.2024. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 28.08.2025).
18. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України; Вимоги, Перелік від 19.06.2019 № 518 : редакція від 07.09.2022. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 28.08.2025).
19. Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом : Постанова Кабінету Міністрів України; Порядок від 11.11.2020 № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#Text (дата звернення: 28.08.2025).
20. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. Чинний від 01.01.1997р. Київ : ДП «УкрНДНЦ», 1996. 6 с. URL: https://tzi.com.ua/downloads/DSTU%203396.0-96.pdf (дата звернення: 28.08.2025).
21. ДСТУ 3396.1-96/ Захист інформації. Технічний захист інформації. Порядок проведення робіт. Чинний від

01.07.1997р. Київ : ДП «УкрНДНЦ», 1996. 6 с. URL: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf
22. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. Чинний від 01.01.1998р. Київ : ДП «УкрНДНЦ», 1997. URL: https://learn.ztu.edu.ua/pluginfile.php/270982/mod_resource/content/1/dstu_3396.2-97.pdf (дата звернення: 28.08.2025).
23. Нормативні документи системи ТЗІ. Державна служба спеціального зв'язку та захисту інформації України. URL:https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi2024 (дата звернення: 28.08.2025).
24. Конвенція про кіберзлочинність : Рада Європи; Конвенція, Міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 28.08.2025).
25. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Рада Європи; Протокол, Міжнародний документ від 28.01.2003. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 28.08.2025).
26. ISO/IEC 15408-1:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 1: Introduction and general model. URL: https://www.iso.org/standard/72891.html (дата звернення: 28.08.2025).
27. ISO/IEC 15408-2:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 2: Security functional components. URL: https://www.iso.org/standard/72892.html (дата звернення: 28.08.2025).
28. ISO/IEC 15408-3:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 3: Security assurance components. URL: https://www.iso.org/standard/72906.html?browse=tc (дата звернення: 28.08.2025).
29. ISO/IEC 15408-4:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security Part 4: Framework for the specification of evaluation methods and activities. URL:https://www.iso.org/standard/72913.html (дата звернення: 28.08.2025).
30. ISO/IEC 15408-5:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security. Part 5: Pre-defined packages of security requirements. URL: https://www.iso.org/standard/72917.html (дата звернення: 28.08.2025).
31. ISO/IEC 27000:2018. Information technology – Security techniques - Information security management systems – Overview and vocabulary. URL: https://www.iso.org/standard/73906.html (дата звернення: 28.08.2025).
32. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 28.08.2025).
33. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection – Information security controls. URL: https://www.iso.org/standard/75652.html (дата звернення: 28.08.2025).
34. ISO/IEC 27003:2017. Information technology – Security techniques – Information security management systems – Guidance. URL: https://www.iso.org/standard/63417.html (дата звернення: 28.08.2025).
35. Регламент Європейського Парламенту і Ради (ЄС) 2019/881 від 17 квітня 2019 року про Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) та про сертифікацію кібербезпеки інформаційно-комунікаційних технологій, а також про скасування Регламенту (ЄС) № 526/2013 (Акт про кібербезпеку) : Європарламент, Рада ЄС; Регламент, Міжнародний документ, Вимоги від 17.04.2019 № 2019/881. URL: https://zakon.rada.gov.ua/laws/show/984_024-19#Text (дата звернення: 28.08.2025).
36. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) : Європарламент, Рада ЄС; Регламент, Міжнародний документ від 27.04.2016 № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 28.08.2025).
37. Загальний регламент про захист даних. GDPR Українською. URL: https://www.gdpr.org.ua/м (дата звернення: 28.08.2025).

Додаткова

38. Беспалов І. О. Правові засади інформаційної безпеки під час дії правового режиму воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2024. №11. DOI: https://doi.org/10.54929/2786-5746-2024-11-01-05
39. Шевчук М. О. Особливості правового забезпечення інформаційної безпеки з урахуванням сучасних загроз національній безпеці / М. О. Шевчук // Правовий часопис Донбасу. – 2024. – №1. – С.45–50. – DOI: https://doi.org/10.32782/2523-4269-2024-86-45-50
40. Босак І. Інформаційна безпека україни: загрози та методи протидії / І. Босак // Київський економічний науковий журнал. – 2025. – №9. – С.33-38. – DOI: https://doi.org/10.32782/2786-765X/2025-9-4
41. Терзі О.О. Принципи забезпечення інформаційної безпеки держави: досвід України та зарубіжних країн / О. О. Терзі // Право та державне управління. – 2024. – №3. – С.51-57. – DOI: https://doi.org/10.32782/pdu.2024.3.7
42. Шевчук М.О. Аналіз національного законодавства про інформаційну безпеку / М.О. Шевчук // Юридичний науковий електронний журнал. – 2025. – №1. – С.383-386. – DOI: https://doi.org/10.32782/2524-0374/2025-1/87
43. Котляров В. Аналіз сучасного стану інформаційної безпеки в Україні / В. Котляров // Mechanism of an Economic Regulation. – 2024. – №2(104). – С.101-104. – DOI: https://doi.org/10.32782/mer.2024.104.16
44. Скочиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні / О. Скочиляс-Павлів // Вісник Національного університету «Львівська політехніка». Серія: "Юридичні науки". – 2024. – Том 11, № 2 (42). – С. 151-158. – DOI: https://doi.org/10.23939/law2024.42.151
45. Кавин С. Правове регулювання забезпечення інформаційної безпеки в праві Європейського Союзу / С. Кавин // Європейські перспективи. – 2022. – № 2. – С.131-138.
46. Омельченко А. В.Організаційно-правові засади забезпечення кібербезпеки України / А. В. Омельченко // Київський часопис права. – 2021. – № 3. – С.140-145. – DOI: https://doi.org/10.32782/klj/2021.3.22
47. Yassine Maleh. Understanding Cybersecurity Standards / Yassine Maleh, Maleh Youness. // Cybersecurity in Morocco. – 2022. – P.13-27. – DOI:10.1007/978-3-031-18475-8_2
48. Taherdoost H. Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview. / H. Taherdoost // *Electronics*.– 2022. – №11(14):2181. – DOI: https://doi.org/10.3390/electronics11142181

49. Kalogeraki E. M., Polemi, N. A taxonomy for cybersecurity standards / // Journal of Surveillance, Security and Safety. – 2024. – №5. – P.95-115. – DOI: http://dx.doi.org/10.20517/jsss.2023.50
50. Paz Santiago. Cybersecurity Standards and Frameworks / Paz Santiago// IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK). – 2023. – P.397-416. – DOI:10.1002/9781119987635.ch23
51. Wasyihun S. Cyber security: State of the art, challenges and future directions / Wasyihun Sema Admass, Yirga Yayeh Munaye, Abebe Abeshu Diro // Cyber Security and Applications – 2024. – Volume 2. – DOI: https://doi.org/10.1016/j.csa.2023.100031.
52. The Impact of Cybersecurity Laws on Legal Procedures and Case Law / Ok Emmanuel, Aria Javiera, Jose Dylan, Diego Catalina // Cybersecurity. – 2025.
53. Josh Aditya. Study of Cybersecurity Laws and Regulations / Josh Aditya// Indian Journal of Law. – 2024. – №2. – P.7-14. – DOI:10.36676/ijl.v2.i3.27
54. Pier Giorgio Chiara. Towards a right to cybersecurity in EU law? The challenges ahead / Pier Giorgio Chiara // Computer Law & Security Review, – 2024. – Volume 53. – DOI: https://doi.org/10.1016/j.clsr.2024.105961.
55. Lee A. Bygrave, The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes / Lee A. Bygrave// Computer Law & Security Review. – 2025. – Volume 56. – DOI: https://doi.org/10.1016/j.clsr.2024.106071.
56. Fahey E. The evolution of EU–US cybersecurity law and policy: on drivers of convergence / E. Fahey // Journal of European Integration, – 2024. – №46(7). – P,1073–1088. – DOI: https://doi.org/10.1080/07036337.2024.2411240

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=6583
2. Електронна бібліотека ХНУ. URL: http://library.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://elar.khmnu.edu.ua/home
4. Законодавство України. Офіційний портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws
5. ISO Standards. Офіційний портал ISO – International Organization for Standardization. URL: https://www.iso.org/standards.html

НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Тип дисципліни	Обов'язкова
Рівень вищої освіти	Перший (*бакалаврський*)
Мова викладання	Українська
Семестр	П'ятий
Кількість призначених кредитів ЄКТС	5,0
Форми здобуття освіти, для яких викладається дисципліна	Очна (денна)

Результати навчання. Після вивчення дисципліни студент повинен: *знати* та *застосовувати* законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації; *адаптуватися* до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат; з*астосовувати* знання у практичних ситуаціях, *аналізувати, аргументувати, приймати рішення* при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; *застосовувати* нормативно визначені поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності; *застосовувати* знання державної та іноземних мов для вивчення міжнародних та національних стандартів, а також *використовувати* термінологію (державною та аншлійською мовами) цих стандартів з метою забезпечення ефективності професійної комунікації.

Зміст навчальної дисципліни. Становлення системи стандартизації в сфері кібербезпеки, нормативно-правове регулювання інформаційної безпеки в Україні, міжнародні практики нормативно-правового регулювання кібербезпеки.

Пререквізити: англійська мова за професійним спрямуванням; основи інформаційної безпеки.

Кореквізити: адміністрування та захист баз і сховищ даних; адміністрування та захист баз і сховищ даних (курсовий проєкт); комплексні системи захисту інформації; технології виявлення вразливостей та вторгнень; управління інформаційною безпекою; виробнича практика 1; виробнича практика 2.

Запланована навчальна діяльність: Мінімальний обсяг навчальних занять в одному кредиті ЄКТС навчальної дисципліни для ***першого*** (бакалаврського) рівня вищої освіти за денною формою здобуття освіти становить 10 годин на 1 кредит ЄКТС.

Форми (методи) навчання: лекції (з використанням словесних, наочних, інтерактивних та проблемних методів); семінарські заняття (з використанням частково-пошукових методів, технологій ситуативного, позиційного та контекстного навчання); самостійна робота (з використанням пояснювально-ілюстративних та частково-пошукових методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання).

Форми оцінювання результатів навчання: оцінювання результатів роботи на семінарських заняттях; тестовий контроль; оцінювання результатів підсумкового семестрового контролю (іспит).

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Кушнір М. Я., Цеханський В. Д. Законодавчі питання інформаційної безпеки: Електронний навчальний посібник. Чернівці : Чернівецький національний університет, 2024. 102 с.
2. Правове регулювання національної безпеки : навчальний посібник / О. Г. Боднарчук та ін. Ірпінь: Державний податковий університет, 2024. 202 с.
3. Потенко О.С. Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз : дис. … канд. техн. наук : 05.13.21, Київ, 2024. 172 с.
4. Кримінально-правова охорона інформаційної безпеки в Україні: монографія / В. І. Борисов та ін.; за заг. ред. В. І. Борисова, О. О. Пащенка ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України. Харків : Право, 2024. 328 с. DOI: https://doi.org/10.31359/9786178518899.
5. Законодавство України. Офіційний портал Верховної Ради України. Доступ до ресурсу: https://zakon.rada.gov.ua/laws
6. ISO Standards. Офіційний портал ISO – International Organization for Standardization. Доступ до ресурсу: https://www.iso.org/standards.html
7. Модульне середовище для навчання. Доступ до ресурсу: https://msn.khmnu.edu.ua/course/view.php?id=6583
8. Електронна бібліотека ХНУ. Доступ до ресурсу: http://library.khmnu.edu.ua/

Викладач: канд. техн. наук, доцент Віктор Чешун