ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ

Декан факультету інформаційних технологій

_____ Тетяна ГОВОРУЩЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

29 серпня 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Моделювання систем захисту даних, оцінка ризиків і прийняття рішень

Галузь знань – 12 Інформаційні технології
Спеціальність – 125 Кібербезпека
Рівень вищої освіти – Перший (бакалаврський)
Освітньо-професійна програма – Кібербезпека
Обсяг дисципліни – 5 кредитів ЄКТС
Шифр дисципліни – ОПП.15
Мова навчання – Українська
Статус дисципліни– Обов'язкова (професійної 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. ІРЗ				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття	Семінарські заняття				Залік	Іспит
Д	4	7	5	150	50	16	34			100				+
Разом ДФН			**5**	**150**	**50**	**16**	**34**			**100**				1

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ канд. техн. наук, доцент Віра ТІТОВА
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

2. ЛИСТ ПОГОДЖЕННЯ

Посада	Назва кафедри	Підпис	Ім'я, ПРІЗВИЩЕ
Завідувач кафедри кібербезпеки, канд. техн. наук, доц.	Кібербезпеки		Юрій КЛЬОЦ
Гарант освітньо-професійної програми, канд. техн. наук, доц.	Кібербезпеки		Віктор ЧЕШУН

3. Пояснювальна записка

Дисципліна «Моделювання систем захисту даних, оцінка ризиків і прийняття рішень» - складова професійної підготовки бакалаврів зі спеціальності «Кібербезпека».

Пререквізити: вища математика; теорія ймовірності та математична статистика.

Постреквізити: комплексні системи захисту інформації; кваліфікаційна робота.

Відповідно до освітньої програми дисципліна сприяє забезпеченню:

компетентностей: ІК Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризуються комплексністю та неповною визначеністю умов; ЗК 4 Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням; ФК 2 Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки; ФК 3 Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах; ФК 4 Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки; ФК 5 Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки; ФК 9 Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою; ФК 12 Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки

програмних результатів навчання: ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення; ПРН 12 Розробляти моделі загроз та порушника; ПРН 14 Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень; ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент; ПРН 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем; ПРН 28 Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та/або кібербезпеки; ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів; ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем; ПРН 33 Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків; ПРН 44 Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами; ПРН 45 Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів; ПРН 46 Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

Мета дисципліни. Надання глибоких та міцних знань з питань застосування методів та засобів оцінки ризиків і прийняття рішень у кібербезпеці в умовах широкого використання сучасних інформаційних технологій, вміння працювати з методами та засобами моделювання загроз, порушника та захисту інформації, використовувати отримані до прикладних задач кібербезпеки.

Предмет дисципліни. Фундаментальні поняття і закони теорії ризиків та прийняття рішень; методи прийняття та підтримки прийняття рішень, алгоритми оцінювання та управління ризиками у інформаційній та кібербезпеці; методи та засоби оцінювання та забезпечення необхідного рівня захищеності інформації за допомогою апарату управління ризиками та прийняття рішень; методи моделювання загроз, порушника та захисту інформації.

Завдання дисципліни. Формування у майбутніх спеціалістів знань про методи імітаційного моделювання, умінь та компетенцій для забезпечення ефективної оцінки ризиків інформаційної та кібербезпеки і прийняття рішень в умовах ризику, необхідних для подальшої роботи.

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *організовувати* за допомогою методів та засобів теорії прийняття рішень та ризиків власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; *забезпечувати* неперервність бізнесу за рахунок використання різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів, та шляхом розв'язку задач забезпечення безперервності бізнес-процесів організації на основі теорії ризиків, *організовувати* процес створення планів неперервності бізнесу на основі теорії ризиків; *аналізувати, аргументувати, приймати* рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, за допомогою методів та засобів теорії прийняття рішень; *виявляти*, *ставити* та *вирішувати* проблеми за професійним спрямуванням, пов'язані *з* аналізом та мінімізацією ризиків обробки інформації в інформаційно-телекомунікаційних системах; *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та *давати* оцінку результативності якості прийнятих рішень; *здійснювати* оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів з рахунок методів та засобів теорії ризиків та прийняття рішень; *здійснювати* професійну діяльність та *аналізувати*, *виявляти* і *оцінювати* можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам за допомогою методів та засобів теорії ризиків та прийняття рішень; *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент з метою реалізації встановленої політики інформаційної та кібербезпеки; *аналізувати, виявляти* та *оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки, *проводити* оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та кібербезпеки, *забезпечувати* захист інформації, з метою реалізації встановленої політики інформаційної та кібербезпеки; *розробляти* моделі загроз та порушника; *впроваджувати* заходи та *забезпечувати* реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

4. Структура залікових кредитів дисципліни

Назва розділу (теми)	Кількість годин, відведених на:		
	лекції	лабораторні роботи	СРС
Тема 1. Теорія прийняття рішень в інформаційній та кібербезпеці	6	12	36
Тема 2. Теорія ризиків в інформаційній та кібербезпеці	6	12	36
Тема 3. Системи виявлення та запобігання вторгненням	4	10	28
Разом :	**16**	**34**	**100**

5. Програма навчальної дисципліни

5.1 Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
	Тема 1. Теорія прийняття рішень в інформаційній та кібербезпеці	**6**
1	**Сутність, функції і завдання теорії прийняття рішення інформаційній та кібербезпеці** Загальний опис проблем прийняття рішень в інформаційній та кібербезпеці. Моделі прийняття рішень в задачах інформаційної та кібербезпеки. Характеристика однокритеріальних та багатокритеріальних задач прийняття рішень, методи розв'язку Літ.: [1] с. 10-80; [2] с. 8-12; [12] с. 4-12, с. 40-53, с. 63-69	2
2	**Прийняття управлінських рішень в задачах інформаційної кібербезпеки** Основи управлінських рішень. Управлінські рішення, як складова безперервності бізнесу. Прийняття управлінських рішень в умовах невизначеності та ризику, дерева рішень. Літ.: [3] с. 9-43; [4] с. 71-136; [9] с. 40-87; [12] с. 69-71	2
3	**Оцінювання ефективності та рівня захищеності інформаційних ресурсів** Моніторинг. Безпосереднє використання статистичних даних при оцінюванні рівня захищеності програм та інформації. Виявлення і використання формалізованих закономірностей при оцінюванні рівня захищеності програм та інформації. Оцінювання ефективності прийнятих рішень при вирішенні завдань захисту програм та інформації. Критерії та фактори, що впливають на ефективність прийнятих рішень. Літ.: [1] с. 185-200; [16] с. 10-60	2
	Тема 2. Теорія ризиків в інформаційній та кібербезпеці	**6**
4	**Сутність, функції і завдання теорії ризиків в інформаційній та кібербезпеці** Поняття, компоненти та види інформаційного ризику. Мінімізація інформаційних ризиків. Відмінності ризиків інформаційної безпеки та кібербезпеки. Стандарти та методики, орієнтовані на управління ризиками інформаційної безпеки. Порівняння методів управління ризиками інформаційної безпеки. Літ.: [5] с. 13-21; [6] с.7-22, с. 129-180; [12] с. 53-62	2
5	**Процедура оцінювання ризиків інформаційної безпеки** Початкові умови задачі оцінювання ризиків інформаційної безпеки. Інвентаризація інформаційних активів та місць їх зберігання, оцінювання можливості реалізації потенційних загроз інформації. Оцінювання ризиків інформаційної безпеки. Ризик-орієнтовані політики безпеки та контрольні заходи щодо поліпшення безпеки. Літ.: [7] с.180-233	2
6	**Методи оцінювання ризиків кібербезпеки** Порівняльний аналіз методів оцінювання ризиків кібербезпеки. Аналіз нормативно-правової бази, що регулює сфери кібербезпеки та управління ризиками. Рекомендації щодо вибору методу оцінювання ризиків кібербезпеки. Літ.: [8] с. 30-44; [11] с.7-42	2
	Тема 3. Моделювання систем захисту даних, загроз та порушника	**4**

7	**Загальні моделі у задачах захисту даних та інформації. Моделювання загроз та порушника** Мова, об'єкти, суб'єкти у моделях захисту даних та інформації, об'єктно-суб'єктна модель. Модель процесу, системи та функцій захисту. Загрози та їх класифікація, як об'єкт моделювання. Дестабілізуючі чинники. Узагальнений підхід щодо побудови моделі загроз. Побудова моделі порушника. Технологія побудови дерева атак. Літ.: [14]; [17] с. 5-12, с. 19-36; [18] с. 49-81, с. 116-142, с. 168-177, с. 280-309, с. 465-473; [19] с. 41-54; [20], с. 67-75; [21]	2
8	**Моделі безпеки систем** Модель ADEPT-50. Модель HRU. Модель Take-Grant. Модель Белла-Лападула. Модель цілісності Літ.: [18] с. 240-280; [19] с. 54-69, с. 105-109	2
	Разом:	**16**

5.2 Зміст лабораторних занять

№ п/п	Тема лабораторного заняття	Кількість годин
1	Розробка, аналіз та перевірка адекватності прогнозних моделей, як складових забезпечення безперервності бізнес-процесів, з використанням програмних засобів Літ.: [3] с. 84-95	4
2	Розв'язання транспортної задачі, як складової забезпечення безперервності бізнес-процесів, з використанням програмних засобів Літ.: [3] с. 60-67	4
3	Вирішення завдань захисту програм та інформації за допомогою багатокритеріальної оптимізації з використанням програмних засобів Літ.: [1] с. 66-78; [12] с. 40-53	4
4	Оцінювання можливості реалізації потенційної загрози інформації та прийняття рішення в умовах ризику з використанням програмних засобів Літ.: [1] с. 146-160; [12] с. 53-62	4
5	Якісний та кількісний аналіз ризиків інформаційної безпеки з використанням програмних засобів Літ.: [15] с. 36-55	4
6	Управління ризиками інформаційної безпеки з використанням програмних засобів Літ.: [7] с.180-233	4
7	Моделювання захисту даних та інформації з використанням компонентів нечіткої логіки Літ.: [10]; [23] с. 32-73	4
8	Оцінювання рівня захищеності інформаційної системи підприємства з використанням програмних засобів Літ.: [7] с.180-233	4
9	Підсумкове заняття. Тестування	2
	Разом за семестр:	**34**

5.3 Зміст самостійної (у т.ч. індивідуальної) роботи

Самостійна робота студентів полягає у систематичному опрацюванні програмного матеріалу з відповідних джерел інформації, підготовці до виконання і захисту лабораторних робіт, підготовці до тестування тощо. Керівництво самостійною роботою здійснюється викладачем згідно з розкладом консультацій у позаурочний час. 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.

№ тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №1. Підготовка до виконання лабораторної роботи №1.	6
2	Опрацювання теоретичного матеріалу лекції №1. Оформлення звіту та підготовка до захисту лабораторної роботи №1.	6
3	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №2. Підготовка до виконання лабораторної роботи №2.	6
4	Опрацювання теоретичного матеріалу лекції №2. Оформлення звіту та підготовка до захисту лабораторної роботи №2.	6

5	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №3. Підготовка до виконання лабораторної роботи №3.	6
6	Опрацювання теоретичного матеріалу лекції №3. Оформлення звіту та підготовка до захисту лабораторної роботи №3.	6
7	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №4. Підготовка до виконання лабораторної роботи №4.	6
8	Опрацювання теоретичного матеріалу лекції №4. Оформлення звіту та підготовка до захисту лабораторної роботи №4.	6
9	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №5. Підготовка до виконання лабораторної роботи №5.	6
10	Опрацювання теоретичного матеріалу лекції №5. Оформлення звіту та підготовка до захисту лабораторної роботи №5.	6
11	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №6. Підготовка до виконання лабораторної роботи №6.	6
12	Опрацювання теоретичного матеріалу лекції №6. Оформлення звіту та підготовка до захисту лабораторної роботи №6.	6
13	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №7. Підготовка до виконання лабораторної роботи №7.	6
14	Опрацювання теоретичного матеріалу лекції №7. Оформлення звіту та підготовка до захисту лабораторної роботи №7.	6
15	Опрацювання конспекту лекцій та теоретичного матеріалу лекції №8. Підготовка до виконання лабораторної роботи №8.	6
16	Опрацювання теоретичного матеріалу лекції №8. Оформлення звіту та підготовка до захисту лабораторної роботи №8.	6
17	Підготовка до тестування за пройденим теоретичним матеріалом.	4
	Разом за семестр:	**100**

6. Технології та методи навчання

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції проводяться з використанням словесних, наочних та проблемних методів з супроводом презентаційних матеріалів; лабораторні роботи – з використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій та технологій моделювання тощо; самостійна робота (опрацювання теоретичного матеріалу, підготовка до виконання та захисту лабораторних робіт, тестування) – з використанням пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання.

7. Методи контролю

Поточний контроль здійснюється під час лабораторних, 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 захисту лабораторних робіт;
- тестовий контроль теоретичного матеріалу.

При виведенні підсумкової семестрової оцінки враховуються результати як поточного, так і підсумкового контролів, 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 весь обсяг, передбачений Робочою програмою для цього виду роботи. Здобувач вищої освіти, який набрав позитивний середньозважений бал (60 відсотків і більше від максимального балу, встановленого для кожної структурної одиниці) 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, проходження інструктажу з техніки безпеки; 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 лабораторних занять (вивчення теоретичного матеріалу з теми, попередню підготовку протоколу роботи, активно працювати на занятті, якісно підготувати звіт (відповідно до теми роботи), захистити результати виконаної роботи, брати участь у дискусіях щодо прийнятих конструктивних рішень при виконанні здобувачами лабораторних робіт тощо).

Здобувачі вищої освіти зобов'язані дотримуватися термінів виконання усіх видів робіт у встановлені терміни, передбачених робочою програмою навчальної дисципліни. Термін захисту лабораторної роботи вважається своєчасним, якщо здобувач захистив її на наступному після виконання роботи занятті. Пропущене

лабораторне заняття здобувач зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Засвоєння здобувачем теоретичного матеріалу з дисципліни оцінюється за результатами тестування.

Здобувач вищої освіти, виконуючи самостійну роботу з дисципліни, має дотримуватися політики доброчесності (заборонені списування, плагіат (в т.ч. із використанням мобільних девайсів)). У разі виявлення плагіату 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 (за наявності такого переліку, доцільно вказати рекомендовані курси), 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 здобувачів освіти

Оцінювання академічних досягнень здобувача вищої освіти здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Залежно від важливості окремих видів навчальної роботи, і їх ролі у формуванні компетентностей і результатів навчання, визначених освітньою програмою, розробники Робочої програми присвоюють кожному виду навчальної роботи (структурній одиниці) з дисципліни певну кількість балів. 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.

Будь-які форми порушення академічної доброчесності ***не допускаються***.

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), демонструє якісне оформлення роботи і володіння спеціальними та прикладними програмами. 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 здобувачів

Аудиторна робота								Контрольні заходи	Семестровий контроль	
Лабораторні роботи №:								Тестовий контроль:	Іспит	Разом балів
1	2	3	4	5	6	7	8	Т 1-2		
Кількість балів за вид навчальної роботи (мінімум-максимум)										
3-5	3-5	3-5	3-5	3-5	3-5	3-5	3-5	12-20	24-40	**60-100**
24-40								**12-20**	**24-40**	

Примітки: Т – тема навчальної дисципліни;

Оцінювання результатів захисту лабораторної роботи

Виконана й оформлена відповідно до встановлених Методичними рекомендаціями вимог лабораторна робота комплексно оцінюється викладачем при її захисті з урахуванням таких критеріїв: самостійність та правильність виконання; якість оформлення звіту; вільне володіння здобувачем спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення.

Результат виконання і захисту здобувачем вищої освіти кожної лабораторної роботи оцінюється відповідно до таблиці Критеріїв оцінювання навчальних досягнень здобувача вищої освіти та рівня досягнення здобувачем запланованих ПРН та сформованих компетентностей з присвоєнням йому відповідної суми балів.

У випадку виявлення здобувачем рівня знань, нижчого ніж 60 відсотків від максимального балу, встановленого Робочою програмою для кожної структурної одиниці, лабораторна робота йому ***не зараховується*** і для її захисту він має детальніше опрацювати матеріал з теми роботи, методику її виконання, виправити грубі помилки та повторно вийти на її захист у призначений для цього викладачем час.

Оцінювання результатів тестового контролю

Тест, передбачений робочою програмою, складається із 20 тестових завдань, кожне з яких є рівнозначним. Максимальна сума балів, яку може набрати здобувач, складає 20.

Відповідно до таблиці структурування видів робіт за тематичний контроль здобувач залежно від кількості правильних відповідей може отримати від 12 до 20 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	0-59	60	65	70	75	80	85	90	95	100
Кількість отриманих балів	0	12	13	14	15	16	17	18	19	20

На тестування відводиться 20 хвилин. Правильні відповіді записуються у талоні відповідей. Здобувач може також пройти тестування і в он-лайн режимі у Модульному середовищі для навчання.

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 підготовки здобувача з навчальної дисципліни. Складання іспиту відбувається за попередньо розробленими і затвердженими на засіданні кафедри білетами.

Таблиця – Оцінювання результатів підсумкового семестрового контролю здобувачів вищої освіти (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
Практичне 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.

Для кожного окремого виду завдань підсумкового семестрового контролю застосовуються критерії оцінювання навчальних досягнень здобувача вищої освіти, наведені вище (**Таблиця – Критерії оцінювання навчальних досягнень здобувача вищої освіти)**.

Таблиця – Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС

Оцінка ЄКТС	Рейтингова шкала балів	Інституційна шкала (Опис рівня 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
C	73-82		
D	66-72		***Задовільно*/*Satisfactory*** – Наявні мінімально достатні для подальшого навчання та/або професійної діяльності за фахом результати навчання з навчальної дисципліни
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

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС визначається в автоматизованому режимі після внесення викладачем результатів оцінювання з усіх видів робіт до електронного журналу. Співвідношення інституційної шкали оцінювання і шкали оцінювання ЄКТС у наведеній нижче таблиці.

Семестровий іспит виставляється, якщо загальна сума балів, яку набрав здобувач з дисципліни за результатами поточного та підсумкового 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 здобувачем сумі балів відповідно до таблиці Співвідношення.

10. Питання для самоконтролю результатів навчання

1. Базові поняття теорії прийняття рішень.
2. Загальний опис проблем прийняття рішень.
3. Критерії та альтернативи.
4. Класифікація задач прийняття рішень.
5. Загальна характеристика однокритеріальних задач.
6. Загальна характеристика багатокритеріальних задач
7. Методи розв’язання багатокритеріальних задач прийняття рішень.
8. Основні поняття та визначення процесу підтримки прийняття рішень.
9. Основи управлінських рішень.
10. Комп’ютерні системи підтримки прийняття рішень та їх особливості.
11. Моделі підтримки прийняття рішень.
12. Класифікація технологічних методів інтелектуального аналізу даних.
13. Моніторинг. Безпосереднє використання статистичних даних.
14. Виявлення і використання формалізованих закономірностей.
15. Основні поняття теорії асоціативних правил.
16. Дерева рішень – загальні принципи технології.
17. Процес побудови дерева рішень.
18. Прийняття рішень. Основні поняття.
19. Аналіз процесу прийняття рішення.
20. Опис ситуації з прийняття рішення.
21. Категорії опису ситуації з прийняття рішення.
22. Критерії вибору рішення.
23. Аналіз ситуації з прийняття рішення.
24. Визначення обмежень (труднощів) процесу прийняття рішень.
25. Парето-оптимальні рішення.
26. Загальний адитивний критерій оцінки ризиків у кібербезпеці.
27. Метод послідовних поступок.
28. Диверсифікація як спосіб зниження ризику у кібербезпеці.
29. Недиверсифікований ризик у кібербезпеці.
30. Способи зниження ризику у кібербезпеці.
31. Вартість, час, ризик та інформація.
32. Показники якості прогнозування у кібербезпеці.
33. Прогнозування методом усереднення.
34. Прогнозування методом ковзаючого усереднення.
35. Прогнозування методом експоненціального згладжування.
36. Циклічність та сезонність у прогнозуванні в задачах кібербезпеки.
37. Сутність поняття "ризик". Основні компоненти ризику.
38. Поняття інформаційного ризику.
39. Мінімізація IT-ризиків.

40. Відмінності ризиків інформаційної безпеки та кібербезпеки.
41. Стандарти, орієнтовані на управління ризиками інформаційної безпеки.
42. Порівняння методів оцінки ризиків.
43. Підхід до оцінки ризиків.
44. Оцінка ризиків інформаційної безпеки.
45. Контрольні заходи щодо поліпшення безпеки.
46. Функціональні методи оцінки ризиків кібербезпеки.
47. Нормативно-правова база, що регулює сфери кібербезпеки та управління ризиками.
48. Вибір функціональних методів для оцінки ризиків.
49. Поняття нечіткої логіки. Нечіткі логічні моделі.
50. Властивості даних та інформації, як об'єктів моделювання.
51. Основні поняття, що використовуються при моделюванні захисту даних та інформації.
52. Мова, об'єкти, суб'єкти у моделях захисту даних та інформації.
53. Ієрархічний метод моделювання.
54. Об'єктно-суб'єктна модель.
55. Загрози та їх класифікація, як об'єкт моделювання.
56. Дестабілізуючі фактори.
57. Узагальнений підхід щодо побудови моделі загроз.
58. Моделі порушень інформаційних ресурсів.
59. Побудова моделі порушника.
60. Модель ADEPT-50.
61. Модель HRU.
62. Модель Take-Grant.
63. Модель Белла-Лападула.
64. Моделі цілісності.
65. Модель процесу захисту.
66. Модель системи захисту.
67. Модель функцій захисту.
68. Інформаційно-аналітична модель оцінки захисту даних та інформації.
69. Вартісна модель.
70. Модель взаємодії відкритих систем у захисті від несанкціонованого доступу.
71. Логіко-ймовірнісна модель захисту інформаційних систем.
72. Функція імовірності захищеності.
73. Побудова дерева атак.

11. Методичне забезпечення

Освітній процес з дисципліни «Моделювання систем захисту даних, оцінка ризиків і прийняття рішень» забезпечений необхідними навчально-методичними матеріалами, що розміщені в Модульному середовищі для навчання MOODLE:

1. Курс «Моделювання систем захисту даних, оцінка ризиків і прийняття рішень»: https://msn.khmnu.edu.ua/course/view.php?id=8068

12. Матеріально-технічне та програмне забезпечення

Інформаційна та комп'ютерна підтримка: ПК, ноутбук, планшет, смартфон або інший мобільний пристрій, проєктор, доступ до мережі Інтернет, робота з презентаціями.

Спеціальне та прикладне програмне забезпечення: OS MS Windows 10 або вище, Matlab 2019 або вище.

13. Рекомендована література

Основна

1. Козачок В.А., Гайдур Г.І., Гахов С.О., Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів Київ: ДУТ ННІЗІ, 2020. 167 с.
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега, видання друге, перероблене, доповнене – Одеса: ОНАЗ ім. О.С. Попова, 2020. 327 с.
3. Калініченко З.Д. Ризик-менеджмент: навчальний посібник / Дніпро: ДДУВС, 2021. 224 с.
4. Коломійцев О. В. Теорія ризиків [Електронний ресурс] : навч. посібник / О. В. Коломійцев, В. І. Панченко, Д. О. Лисиця ; Нац. техн. ун-т "Харків. політехн. ін-т". Харків : НТУ "ХПІ", 2025. 408 с.

Додаткова

5. Теорія прийняття рішень/ Л.С. Файнзільберг, О.А. Жуковська, В.С. Якимчук. Київ: Освіта України, 2018. – 246 с.
6. Теорії прийняття рішень: курс лекцій/ укладач О.С. Юрков. - Мукачево: МДУ, 2016. 135 с.
7. Управління фінансовими ризиками: навчальний посібник/ С.Г. Шклярук. Київ: ДП «Вид. дім «Персонал», 2019. 494 с.
8. Менеджмент інформаційної безпеки: навчальний посібник/ О.Г. Корченко, М.Є. Шелест, С.В. Казмірчук, Ю.М. Ткач, Є.В. Іванченко. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с.

9. Інтелектуальні системи підтримки прийняття рішень/ Навч. посібник за ред. П.І. Бідюка. Київ: Національна академія управління, 2016. 188 с.
10. Сучасні інформаційні системи і технології: управління знаннями: навчальний посібник/ В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. – Ірпінь: Національний університет ДПС України, 2016. – 212 с.
11. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. – 288 с.
12. Основи теорії прийняття рішень/ О.І. Кушлик-Дивульська, Б.Р. Кушлик. К., 2014. 94 с.
13. Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни "Менеджмент інформаційної безпеки" / уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018. URL: http://dspace.kntu.kr.ua/jspui/bitstream/ 123456789/8659/1/Menedzh_inf_bezp_lab.pdf
14. Математична модель порушника інформаційної безпеки/ Ю.М. Щебланін, Д.І. Рабчун. – Кібербезпека: освіта, наука, техніка. 2018. №1(1). С. 63-72.
15. Методичні вказівки до виконання практичних робіт з навчальної дисципліни "Менеджмент інформаційної безпеки" [Електронний ресурс]/ уклад. І. А. Лисенко Кропивницький: ЦНТУ, 2018. – режим доступу: http://dspace.kntu.kr.ua/jspui/bitstream/ 123456789/8431/1/Osn_ypr_kiber.pdf
16. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник/ Д.В. Ланде, І.Ю. Субач, Ю.Є. Бояринова. К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. 297 с.
17. Технології захисту інформації: конспект лекцій / А.Ф.Карачка. Тернопіль: ТНЕУ, 2017. URL: http://dspace.tneu.edu.ua/retrieve/52646/lekzii.pdf.
18. Моделювання систем захисту інформації/ А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. 273 с.
19. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту: монографія/ А. В. Дудатьєв. Вінниця: ВНТУ, 2017. 128 с.
20. Інформаційна безпека держави: навч. посіб./ В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
21. Кіреєнко О. Модель порушника в інформаційно-комунікаційних системах. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2017. С. 69-77.
22. Сучасні інформаційні системи і технології: управління знаннями: навчальний посібник/ В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. Ірпінь: Національний університет ДПС України, 2016. 212 с.
23. Evaluation of a Formalized Model for Classification of Emergency Situations/ V. Titova, Ie. Gnatchuk "Computational linguistics and intelligent systems"/ Ukraine, Kharkiv. 2017 P. 110-120.
24. Підтримка прийняття рішень для диспетчера служб швидкого реагування за допомогою формалізованої моделі задачі класифікації надзвичайних ситуацій/ В.Ю. Тітова // Штучний інтелект. 2015. №3-4. С. 167-178.
25. Концептуальна модель системи захисту інформації в сучасних комп'ютерних системах/ В.Ю. Тітова, С.О Савчук, В.Ю. Черниш// Вісник Хмельницького національного університету. Технічні науки. 2019. №3. С. 164-167.
26. Класифікація моделей загроз в комп'ютерних системах / В. Ю. Тітова, Ю. П. Кльоц, С. О. Савчук // Вісник Хмельницького національного університету. Технічні науки. 2020. № 2. С.201-203.

14. Інформаційні ресурси

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8068
2. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/
3. Інституційний репозитарій ХНУ. URL : https://library.khmnu.edu.ua/

МОДЕЛЮВАННЯ СИСТЕМ ЗАХИСТУ ДАНИХ, ОЦІНКА РИЗИКІВ І ПРИЙНЯТТЯ РІШЕНЬ

Тип дисципліни	Обов'язкова
Освітній рівень	Перший (бакалаврський)
Мова викладання	Українська
Семестр	Сьомий
Кількість встановлених кредитів ЄКТС	5
Форми навчання, для яких викладається дисципліна	Очна (денна)

Результати навчання. Здобувач, який успішно завершив вивчення дисципліни, повинен: *організовувати* за допомогою методів та засобів теорії прийняття рішень та ризиків власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність; *забезпечувати* неперервність бізнесу за рахунок використання різних класів політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів, та шляхом розв'язку задач забезпечення безперервності бізнес-процесів організації на основі теорії ризиків, *організовувати* процес створення планів неперервності бізнесу на основі теорії ризиків; *аналізувати, аргументувати, приймати* рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, за допомогою методів та засобів теорії прийняття рішень; *виявляти*, *ставити* та *вирішувати* проблеми за професійним спрямуванням, пов'язані *з* аналізом та мінімізацією ризиків обробки інформації в інформаційно-телекомунікаційних системах; *вирішувати* завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та *давати* оцінку результативності якості прийнятих рішень; *здійснювати* оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах, можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів з рахунок методів та засобів теорії ризиків та прийняття рішень; *здійснювати* професійну діяльність та *аналізувати*, *виявляти* і *оцінювати* можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам за допомогою методів та засобів теорії ризиків та прийняття рішень; *забезпечувати* захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах, процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент з метою реалізації встановленої політики інформаційної та кібербезпеки; *аналізувати, виявляти* та *оцінювати* можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та кібербезпеки, *проводити* оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та кібербезпеки, *забезпечувати* захист інформації, з метою реалізації встановленої політики інформаційної та кібербезпеки; *розробляти* моделі загроз та порушника; *впроваджувати* заходи та *забезпечувати* реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

Зміст навчальної дисципліни: Базові поняття теорії прийняття рішень. Критерії та альтернативи. Класифікація задач прийняття рішень. Прийняття рішень в умовах ризику та невизначеності. Методи розв'язання багатокритеріальних задач прийняття рішень. Основи управлінських рішень. Моделі підтримки прийняття рішень. Класифікація технологічних методів інтелектуального аналізу даних. Безпосереднє використання статистичних даних та виявлення формалізованих закономірностей. Основні поняття теорії асоціативних правил. Дерева рішень. Сутність поняття "ризик". Основні компоненти ризику. Види ризиків. Якісний та кількісний аналіз ризиків. Методики та програмні засоби, орієнтовані на управління ризиками інформаційної та кібербезпеки. Оцінювання ризиків інформаційної безпеки. Функціональні методи оцінювання ризиків кібербезпеки. Властивості інформації, як об'єкту моделювання. Мова, об'єкти, суб'єкти у моделях захисту інформації. Ієрархічний метод моделювання. Об'єктно-суб'єктна модель. Загрози та їх класифікація. Дестабілізуючі фактори. Моделі порушень інформаційних ресурсів. Побудова моделі порушника. Моделі безпеки систем (модель ADEPT-50, модель HRU, модель Take-Grant, модель Белла-Лападула, модель цілісності). Модель з повним перекриттям загроз. Інформаційно-аналітична модель оцінки захисту інформації від загроз несанкціонованого доступу. Вартісна модель. Модель взаємодії відкритих систем у захисті від несанкціонованого доступу. Логіко-ймовірнісна модель захисту інформаційних систем, функція імовірності захищеності. Побудова дерева атак.

Пререквізити: вища математика; теорія ймовірності та математична статистика.

Постреквізити: комплексні системи захисту інформації; кваліфікаційна робота.

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 та проблемних методів з супроводом презентаційних матеріалів); лабораторні роботи (з використанням практичних, частково-пошукових та ігрових методівз використанням практичних, частково-пошукових та ігрових методів, із застосуванням сучасних інформаційно-комп'ютерних технологій та технологій моделювання тощо); самостійна робота (з використанням

пояснювально-ілюстративних та дослідницьких методів, інформаційно-комп'ютерних технологій та технологій дистанційного навчання).

Форми оцінювання результатів навчання: оцінювання результатів захисту лабораторних робіт; тестовий контроль теоретичного матеріалу.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Козачок В.А., Гайдур Г.І., Гахов С.О., Власенко В.О., Чумак Н.С. Політики безпеки. Навчальний посібник для студентів вищих навчальних закладів Київ: ДУТ ННІЗІ, 2020. 167 с.
2. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега, видання друге, перероблене, доповнене. Одеса: ОНАЗ ім. О.С. Попова, 2020. 327 с.
3. Калініченко З.Д. Ризик-менеджмент: навчальний посібник / Дніпро: ДДУВС, 2021. 224 с.
4. Коломійцев О. В. Теорія ризиків [Електронний ресурс] : навч. посібник / О. В. Коломійцев, В. І. Панченко, Д. О. Лисиця ; Нац. техн. ун-т "Харків. політехн. ін-т". Харків : НТУ "ХПІ", 2025. 408 с.
5. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/course/view.php?id=8068
6. Електронна бібліотека ХНУ. URL: http://lib.khmnu.edu.ua/

Викладач: канд. техн. наук, доцент Тітова В.Ю.