ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ЗАТВЕРДЖУЮ
Декан факультету ІТ
_____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ
«__» 08 2023 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.13
Мова навчання	Українська
Статус дисципліни	Обов'язкова, дисципліна професійної підготовки
Факультет	Інформаційних технологій
Кафедра	Кібербезпеки

Форма навчання	Курс	Семестр	Обсяг дисципліни		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
Очна (денна)	4	7	5	150	68	17	34	17		82				+

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека»

Робоча програма складена _____ канд. техн. наук, доц. Віра ТІТОВА
Підпис(и) автора(ів) Ступінь, вчене звання, Ім'я, ПРІЗВИЩЕ автора(ів)

Схвалена на засіданні кафедри Кібербезпеки

Протокол від 31.08.2023 № 1 Зав. кафедри _____ Юрій КЛЬОЦ
Підпис Ім'я, ПРІЗВИЩЕ

Робоча програма розглянута та схвалена вченою радою факультету інформаційних технологій

Голова вченої ради факультету _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Хмельницький 2023

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

Студент, 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.

Кореквізити: комплексні системи захисту інформації, кваліфікаційна робота.

Запланована навчальна діяльність: лекцій 17, лабораторних робіт 34 год., самостійної роботи 99 год., разом 150 год.

Методи навчання: словесні та наочні (лекції); практичні та частково-пошукові (лабораторні роботи); пояснювально-ілюстративні та дослідницькі (самостійна робота).

Форми оцінювання результатів навчання: захист лабораторних робіт, письмова контрольна робота, підсумковий контрольний захід.

Вид семестрового контролю: іспит.

Навчальні ресурси:

1. Теорія прийняття рішень/ Л.С. Файнзільберг, О.А. Жуковська, В.С. Якимчук. Київ: Освіта України, 2018. 246 с.
2. Моделювання систем захисту інформації/ А.О. Антонюк. Ірпінь: Національний університет ДПС України, 2015. 273 с.
3. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник./ В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко. К.:ДУТ, 2015. 345 с.
4. Модульне середовище для навчання MOODLE. Доступ до ресурсу: https://msn.khmnu.edu.ua
5. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php

Викладач: к.т.н., доц. Тітова В.Ю.

ВСТУП

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

Метою викладання навчальної дисципліни «Моделювання систем захисту даних, оцінка ризиків і прийняття рішень» є 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; розвиток у студентів фахового стилю мислення; 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.

Предметом дисципліни є фундаментальні поняття і закони теорії ризиків та прийняття рішень; методи прийняття рішень та підтримки прийняття, 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.

Завданням дисципліни є забезпечити набуття компетентностей та досягнення програмних результатів навчання відповідно до Стандарту вищої освіти та освітньо-професійної програми підготовки бакалаврів зі спеціальності «Кібербезпека»:

***компетентності*:**

КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та кібербезпеки;

КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах;

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки;

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки;

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою;

КФ 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.

результати навчання:

РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;

РН 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;

РН 12. Розробляти моделі загроз та порушника;

РН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами, та давати оцінку результативності якості прийнятих рішень;

РН 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;
РН 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;
РН 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 кібербезпеки;
РН 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;
РН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем;
РН 33. Організовувати процес створення планів неперервності бізнесу організації на основі теорії ризиків;
РН 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;
РН 45. Застосовувати різні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;
РН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.

Студент, 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; *розроблятиі* 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.

СТРУКТУРА ЗАЛІКОВИХ КРЕДИТІВ ДИСЦИПЛІНИ

Назва теми	Кількість годин відведених на:		
	лекції	**лабораторні роботи**	**самостійну роботу**
Тема 1. Теорія прийняття рішень в інформаційній та кібербезпеці	6	16	46
Тема 2. Теорія ризиків в інформаційній та кібербезпеці	6	8	26
Тема 3. Моделювання систем захисту даних, загроз та порушника	5 (6/4)*	10	27 (26/28)*
Разом:	**17 (18/16)***	**34**	**99 (98/100)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст лекційного курсу

Номер лекції	Перелік тем лекцій, їх анотація	Години
Тема 1. Теорія прийняття рішень в інформаційній та кібербезпеці		
1	**Сутність, функції і завдання теорії прийняття рішення в інформаційній та кібербезпеці** 1. Загальний опис проблем прийняття рішень в інформаційній та кібербезпеці 2. Моделі прийняття рішень в задачах інформаційної та кібербезпеки 3. 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 та кібербезпеки** 1. Основи управлінських рішень. Управлінські рішення, як складова безперервності бізнесу 2. 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** 1. Моніторинг. Безпосереднє використання статистичних даних при оцінюванні рівня захищеності програм та інформації 2. Виявлення і використання формалізованих закономірностей при оцінюванні рівня захищеності програм та інформації 3. 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		
4	**Сутність, функції і завдання теорії ризиків в інформаційній та кібербезпеці** 1. Поняття, компоненти та види інформаційного ризику 2. Мінімізація інформаційних ризиків 3. Відмінності ризиків інформаційної безпеки та кібербезпеки 4. Стандарти та методики, орієнтовані на управління ризиками інформаційної безпеки 5. 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** 1. Початкові умови задачі оцінювання ризиків інформаційної безпеки 2. Інвентаризація інформаційних активів та місць їх зберігання, оцінювання можливості реалізації потенційних загроз інформації 3. Оцінювання ризиків інформаційної безпеки 4. Ризик-орієнтовані політики безпеки та контрольні заходи щодо поліпшення безпеки Літ.: [7] с.180-233	2
6	**Методи оцінювання ризиків кібербезпеки** 1. Порівняльний аналіз методів оцінювання ризиків кібербезпеки 2. Аналіз нормативно-правової бази, що регулює сфери кібербезпеки та	2

	управління ризиками 3. Рекомендації щодо вибору методу оцінювання ризиків кібербезпеки Літ.: [8] с. 30-44; [11] с.7-42	
Тема 3. Моделювання систем захисту даних, загроз та порушника		
7	**Загальні моделі у задачах захисту даних та інформації** 1. Мова, об'єкти, суб'єкти у моделях захисту даних та інформації, об'єктно-суб'єктна модель 2. Модель процесу, системи та функцій захисту 3. Модель взаємодії відкритих систем у захисті від несанкціонованого доступу 4. Модель з повним перекриттям загроз 5. Інформаційно-аналітична модель оцінки захисту інформації від загроз несанкціонованого доступу 6. Вартісна модель 7. Логіко-ймовірнісна модель захисту інформаційних систем, функція імовірності захищеності Літ.: [17] с. 5-12, с. 19-36; [18] с. 49-81, с. 280-309, с. 465-473; [19] с. 41-54	2
8	**Моделювання загроз та порушника** 1. Загрози та їх класифікація, як об'єкт моделювання 2. Дестабілізуючі чинники 3. Узагальнений підхід щодо побудови моделі загроз 4. Побудова моделі порушника 5. Технологія побудови дерева атак Літ.: [14]; [18] с. 116-142, с. 168-177; [20], с. 67-75; [21]	2 (2/1)*
9	**Моделі безпеки систем** 1. Модель ADEPT-50 2. Модель HRU 3. Модель Take-Grant 4. Модель Белла-Лападула 5. Модель цілісності Літ.: [18] с. 240-280; [19] с. 54-69, с. 105-109	2 (2/1)*
	Разом за семестр:	**17 (18/16)***

* За чисельником / за знаменником (розрахунок здійснюється відповідно до розкладу занять)

Зміст лабораторних робіт

№ п/п	Теми лабораторних робіт	Кількість годин
1	Розробка, аналіз та перевірка адекватності прогнозних моделей, як складовихзабезпеченнябезперервностібізнес-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. Контрольна робота	2
	Разом за семестр:	**34**

Зміст самостійної (у т.ч. індивідуальної) роботи

Об'єм самостійної роботи з дисципліни "Моделювання систем захисту даних, оцінка ризиків і прийняття рішень" становить 99 годин. Він включає опрацювання лекційного матеріалу та літературних джерел, підготовку до контрольної роботи, підготовку до виконання та захисту лабораторних робіт. Керівництво самостійною роботою здійснює викладач згідно з розкладом консультацій в позаурочний час.

№ тижня	Теми самостійної роботи	Кількість годин
1	Опрацювання теоретичного матеріалу лекції №1.	5/6*
2	Підготовка до виконання лабораторної роботи №1	6/5*
3	Опрацювання теоретичного матеріалу лекції №2.	5/6*
4	Підготовка до захисту лабораторної роботи №1. Підготовка до виконання лабораторної роботи №2.	6/5*
5	Опрацювання теоретичного матеріалу лекції №3.	6/8*
6	Підготовка до захисту лабораторної роботи №2. Підготовка до виконання лабораторної роботи №3.	6/5*
7	Опрацювання теоретичного матеріалу лекції №4.	5/6*
8	Підготовка до захисту лабораторної роботи №3. Підготовка до виконання лабораторної роботи №4.	6/5*
9	Опрацювання теоретичного матеріалу лекції №5.	5/6*
10	Підготовка до захисту лабораторної роботи №4. Підготовка до виконання лабораторної роботи №5.	6/5*
11	Опрацювання теоретичного матеріалу лекції №6.	5/6*
12	Підготовка до захисту лабораторної роботи №5. Підготовка до виконання лабораторної роботи №6.	6/5*
13	Опрацювання теоретичного матеріалу лекції №7.	5/6*
14	Підготовка до захисту лабораторної роботи №6. Підготовка до виконання лабораторної роботи №7.	6/6*
15	Опрацювання теоретичного матеріалу лекції №8.	6/6*
16	Підготовка до захисту лабораторної роботи №7. Підготовка до виконання лабораторної роботи №8.	6/6*
17	Опрацювання теоретичного матеріалу лекції №9. Підготовка до захисту лабораторної роботи №8. Підготовка до контрольної роботи за пройденим матеріалом.	8/8*
	Разом за семестр:	99 (98/100)*

* При плануванні лекцій та практичних за чисельником/за знаменником (розрахунок здійснюється відповідно до розкладу занять)

ТЕХНОЛОГІЇ ТА МЕТОДИ НАВЧАННЯ

Процес навчання з дисципліни ґрунтується на використанні традиційних та сучасних методів. Зокрема, лекції пояснювально-ілюстративними та проблемними методами з супроводом презентаційних матеріалів, лабораторні та практичні заняття проводяться з використанням практичних, продуктивних, проблемних та контекстних методів, методами моделювання та з застосуванням сучасних інформаційно-комп'ютерних технологій (Matlab, Coras Tool та інших) і мають за мету – набуття студентами практичних навичок оцінки ризиків, прийняття рішень та моделювання систем захисту даних у кібербезпеці, використання сучасних програмних та апаратних систем оцінки ризиків та прийняття рішень, використання сучасних інформаційних технологій моделювання рішень, пов'язаних з захистом інформації.

Застосовувані при викладанні дисципліни методи навчання сприяють розвитку у студентів навичок soft skills: обговорення проблемних питань під час лекцій, прилюдні захисти лабораторних робіт і презентація результатів виконання практичних занять з обґрунтуванням прийнятих рішень щодо вибору методів рішення завдань в діалозі з викладачем і групою сприяють формуванню і удосконаленню вмінь публічних виступів, емпатичного слухання, відстоювання власної точки зору, самоаналізу і самокритики; адаптованість, вміння користуватися інтернет-ресурсами та іншими джерелами інформації, синтезувати та критично осмислювати інформацію з різних джерел передбачені специфікою дисципліни; обмежений час на виконання лабораторних робіт, практичних і контрольних завдань, чітко визначені і надані в силабусі терміни проходження контрольних точок і відпрацювання заборгованостей сприяють розвитку пунктуальності, здатності до самоорганізації та управління часом (тайм-менеджменту).

При вивченні дисципліни можуть бути зараховані результати навчання, здобуті у неформальній освіті. Визнання результатів навчання, здобутих у неформальній освіті, реалізується згідно з чинним законодавством і регулюється Положенням про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

МЕТОДИ КОНТРОЛЮ

Поточний контроль здійснюється під час практичних та лабораторних занять, а також у дні проведення контрольних заходів, встановлених робочим планом дисципліни.

При цьому використовуються такі методи поточного контролю:

- захист лабораторних робіт;
- письмова контрольна робота.

Семестровий контроль проводиться у формі іспиту. При виведенні підсумкової семестрової оцінки враховуються результати як поточного контролю, так і підсумкового контрольного заходу.

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ СТУДЕНТІВ

Оцінювання академічних досягнень студента здійснюється відповідно до «Положення про контроль і оцінювання результатів навчання здобувачів вищої освіти у ХНУ». Кожний вид роботи з дисципліни оцінюється за інституційною чотирибальною шкалою. Семестрова підсумкова оцінка визначається як середньозважена з усіх видів навчальної роботи, виконаних і зданих позитивно з урахуванням коефіцієнта вагомості. Вагові коефіцієнти змінюються залежно від структури дисципліни і важливості окремих видів її робіт.

Структурування дисципліни за видами робіт і оцінювання результатів навчання студентів за ваговими коефіцієнтами

	Аудиторна робота	**Контрольні заходи**	**Підсумковий контрольний захід**
Вид заняття	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-3	1-3	1-3
Ваговий коефіцієнт	0,4	0,2	0,4

Оцінювання лабораторних робіт. Оцінка, яка виставляється за лабораторну роботу, складається з таких елементів: оцінка, отримана за здачу відповідної за номером та темою практики; знання теоретичного матеріалу з теми; якість оформлення звіту; вільне володіння студентом спеціальною термінологією і уміння професійно обґрунтувати прийняті конструктивні рішення; своєчасний захист лабораторної роботи.

Термін захисту звіту з лабораторної роботи вважається своєчасним, якщо студент захистив її в день виконання або на наступному після виконання роботи занятті. Пропущене заняття студент зобов'язаний відпрацювати в лабораторіях кафедри у встановлений викладачем термін з реєстрацією у відповідному журналі кафедри, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за лабораторну роботу викладач оголошує одразу після захисту звіту і проставляє в електронний журнал дисципліни.

Оцінювання контрольних робіт. Контрольна робота складається з теоретичного питання та практичного завдання за темою одного з практичних занять. Оцінювання здійснюється за чотирибальною шкалою.

Оцінку «відмінно» отримує студент який дав повну письмову відповідь на теоретичне питання та правильно вирішив завдання, з обґрунтуванням вибору методів для його розв'язування.

Оцінку «добре» отримує студент, який дав правильну відповідь на теоретичне питання та правильно вирішив завдання, але у відповіді присутні дві-три несуттєві помилки, або є вагання з обґрунтуванням вибору методів вирішення.

Оцінку «задовільно» отримує студент, який дав часткову відповідь на теоретичне питання та допустив суттєві помилки при вирішення завдання.

Оцінку «незадовільно» отримує студент, який не зміг обрати правильні методи для вирішення завдання або не дав відповіді на теоретичне питання.

Оцінку за контрольну роботу викладач проставляє в електронний журнал дисципліни не пізніше ніж через десять днів після проведення контрольного заходу.

Семестровий контроль (іспит). Підсумковий контрольний захід з дисципліни проводиться в формі іспиту. Екзаменаційний білет складається з теоретичного питання і задачі. Під час іспиту за наданими відповідями і рішеннями (розв'язками) виконується оцінювання рівня засвоєння студентом матеріалу дисципліни.

Оцінка за підсумковий контрольний захід проставляється викладачем в електронний журнал дисципліни в день здачі іспиту і враховується в автоматизованому режимі при визначенні підсумкової семестрової оцінки студента з дисципліни за інституційною шкалою і шкалою ЄКТС

Засвоєння студентом матеріалу з дисципліни оцінюється за наведеними в таблиці критеріями.

Критерії оцінювання знань студентів

Оцінка за інституційною шкалою	Узагальнений критерій
Відмінно	Студент 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 державною мовою (в усній або у письмовій формі), демонструє якісне оформлення роботи і володіння спеціальними інструментами. Студент не вагається при видозміні запитання, вміє робити детальні та узагальнюючі висновки. При відповіді допустив дві-три несуттєві похибки.
Добре	Студент виявив повне засвоєння навчального матеріалу, володіє понятійним апаратом і фаховою термінологією, 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 закономірностей тощо. Відповідь студента будується на основі самостійного мислення. Студент у відповіді допустив дві–три несуттєві помилки.
Задовільно	Студент 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 студента будується на рівні репродуктивного мислення, студент має слабкі знання структури курсу, 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	Студент 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 студенту, який не може продовжити навчання без додаткової роботи з вивчення дисципліни.

Якщо студент отримав негативну оцінку за певним видом робіт, то він має перездати її в установленому порядку, але обов'язково до терміну наступного контролю.

У випадку, коли студент не виконав індивідуальний план з дисципліни у заплановані терміни без поважних причин, то під час відпрацювання заборгованості при позитивній відповіді йому виставляється оцінка «задовільно».

Студент, який у встановлені терміни не виконав індивідуальний план поточної роботи з дисципліни повністю або частково, до здачі підсумкового контрольного заходу не допускається.

Студент, який набрав позитивний середньозважений бал за поточну роботу і не здав підсумковий контрольний захід (іспит), вважається невстигаючим.

Підсумкова семестрова оцінка за інституційною шкалою і шкалою ЄКТС встановлюється в автоматизованому режимі після внесення викладачем усіх оцінок до електронного журналу.

Співвідношення вітчизняної шкали оцінювання і шкали оцінювання ЄКТС

	Інституційна інтервальна балів	**Інституційна оцінка, критерії оцінювання шкала**	
A	4,75–5,00	5	***Відмінно*** – глибоке і повне опанування навчального матеріалу і виявлення відповідних умінь та навиків
B	4,25–4,74	4	***Добре*** – повне знання навчального матеріалу з кількома незначними помилками
C	3,75–4,24	4	***Добре*** – в загальному правильна відповідь з двома-трьома суттєвими помилками
D	3,25–3,74	3	***Задовільно*** – неповне опанування програмного матеріалу, але достатнє для практичної діяльності за професією
Оцінка ЄКТС E	3,00–3,24	3	***Задовільно*** – неповне опанування програмного матеріалу, що задовольняє мінімальні критерії оцінювання
FX	2,00–2,99	2	***Незадовільно*** – безсистемність одержаних знань і неможливість продовжити навчання без додаткових знань з дисципліни
F	0,00–1,99	2	***Незадовільно*** – необхідна серйозна подальша робота і повторне вивчення дисципліни

ПИТАННЯ ДЛЯ САМОКОНТРОЛЮ ЗДОБУТИХ СТУДЕНТАМИ 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.

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Навчальний процес з дисципліни «Моделювання систем захисту даних, оцінка ризиків і прийняття рішень» повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Теорія прийняття рішень/ Л.С. Файнзільберг, О.А. Жуковська, В.С. Якимчук. - Київ: Освіта України, 2018. – 246 с.
2. Теорії прийняття рішень: курс лекцій/ укладач О.С. Юрков. - Мукачево: МДУ, 2016. - 135 с.
3. Прийняття управлінських рішень: навчальний посібник/ Ю. Є. Петруня, Б. В. Літовченко, Т. О. Пасічник та ін.; за ред. Ю. Є. Петруні. - Дніпропетровськ: Університет митної справи та фінансів, 2015. - 209 с.
4. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.
5. Управління фінансовими ризиками: навчальний посібник/ С.Г. Шклярук. – Київ: ДП «Вид. дім «Персонал», 2019. – 494 с.
6. Економічний ризик: методи оцінки та управління: навч. посібник/ Т. А. Васильєва, С. В. Лєонов, Я. М. Кривич та ін. ; під заг. ред. д-ра екон. наук, проф. Т. А. Васильєвої, канд. екон. наук Я. М. Кривич. - Суми : ДВНЗ "УАБС НБУ", 2015. – 208 с.
7. 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.
8. Еколого-економічний ризик-менеджмент: методи оцінювання ризиків: [Електронний ресурс]: навч. посіб./ Н. В. Караєва; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2019. – режим доступу: http://apeps.kpi.ua/downloads/Караєва_еколог_економ_ризик.pdf
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" [Електронний ресурс]/ уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018. – режим доступу: 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 [Електронний ресурс]/ А.Ф.Карачка. – Тернопіль: ТНЕУ, 2017. – режим доступу: 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. Модель порушника в інформаційно-комунікаційних системах / О. Кіреєнко. – Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2017. – Вип. 2. – 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.

Додаткова

25. 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.
26. Information security risk assessment system – «RISK-CALCULATOR»/ O. Korchenko, B. Akhmetov, S.Kazmirchuk, Ye. Chasnovskiy. // Ukrainian Scientific Journal of Information Security. – 2017, vol. 23, issue 2. – P. 145-152.
27. 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.
38. 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.
39. 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.

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання. URL : https://msn.khmnu.edu.ua/
2. Електронна бібліотека університету. URL: http://lib.khmnu.edu.ua/asp/php_f/p1age_lib.php