ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

ЗАТВЕРДЖУЮ
Декан ФПКТС
_____ Савенко О.С.
«27» 01 2021 р.

СИЛАБУС

Навчальна дисципліна: "Моделювання систем захисту даних, оцінка ризиків і прийняття рішень"

Освітньо-професійна програма: «Кібербезпека»

Рівень вищої освіти: перший (бакалаврський)

Загальна інформація

Позиція	Інформація
Викладач(і)	Орленко Вікторія Сергіївна
Профайл викладач(ів)	http://ksm.khnu.km.ua/sklad-kafedry/
E-mail викладача(ів)	orlenkovs@khmnu.edu.ua
Контактний телефон	Наявний в ІСУ
Сторінка дисципліни в ІСУ	https://msn.khnu.km.ua/course/view.php?id=6455
Сторінки інтернет-ресурсів для онлайн занять	ZOOM: https://us04web.zoom.us/j/8577265687 * пароль у викладача, старости групи і на сторінці дисципліни в ІСУ
Навчальний рік, семестр	2022-2023, семестр VII (осінньо-зимовий)
Розклад	
Консультації	

Характеристика дисципліни

Форма навчання	Курс	Семестр	Обсяг дисципліни		Кількість годин						Курсовий проект	Курсова робота	Форма семестрового контролю	
					Аудиторні заняття				Індивідуальна робота студента	Самостійна робота, у т.ч. ІРС				
			Кредити ЄКТС	Години	Разом	Лекції	Лабораторні роботи	Практичні заняття					Залік	Іспит
Д	4	7	5	150	68	17	34	17	-	82	-	-	-	+

Анотація дисципліни

Дисципліна формує у студентів знання про основні поняття, положення, завдання, засади, кроки прийняття рішень за різних умов; сутність процесу вибору, визначення функцій вибору та здійснення операцій над ними; основні критерії прийняття рішень в різних інформаційних ситуаціях; положення прийняття групових рішень; основи теорії ризиків, поняття моделей та методів моделювання у задах захисту інформації та навчає їх виокремлювати складові процесу прийняття рішень; формалізувати задачі прийняття рішень; приймати рішення в умовах конфлікту, невизначеності та зумовленого ними ризику; приймати рішення за наявності багатьох критеріїв та цілей; здійснювати груповий вибір; приймати рішення в різних сферах інформаційних технологій; моделювати загрози та системи захисту інформації; визначати моделі порушника, проводити верифікацію отриманих результатів моделювання; застосовувати моделі для прогнозу та узгодженості з реальними статистичними даними.

Дисципліна викладається для студентів денної форми навчання спеціальності «Кібербезпека». При викладанні дисципліни використовуються наступні форми (методи) навчання: пояснювально-ілюстративні, практичні, продуктивні, проблемні, контекстні, моделювання, застосування інформаційно-комп'ютерних технологій (Matlab, Coras Tool та інших).

Пререквізити: теорія ймовірності та математична статистика.

Кореквізити: комплексні системи захисту інформації: проектування, впровадження, супровід; кваліфікаційна робота.

Мета і завдання дисципліни

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; *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.

Тематичний і календарний план вивчення дисципліни

№ тижня	Тема лекції*	Тема лаб. роботи **	Тема практ. роботи*	Самостійна роботи		
				Зміст	Год.	Література
1	**Сутність, функції і завдання теорії прийняття рішення в інформаційній та кібербезпеці** Загальний опис проблем прийняття рішень в інформаційній та кібербезпеці. Моделі прийняття рішень в задачах інформаційної та кібербезпеки. Характеристика однокритеріаль-них та багатокритері-альних задач прийняття рішень, методи розв'язку	-	**ПЗ1.** Розробка, аналіз та перевірка адекватності прогнозних моделей, як складових забезпечення безперервності бізнес-процесів	Опрацювання теоретичного матеріалу лекції №1. Виконання завдань ПЗ1.	4	[1] с. 10-80 [2] с. 8-12 [3] с. 84-95 [12] с. 4-12, с. 40-53, с. 63-69

2	-	**ЛР1.** Розробка, аналіз та перевірка адекватності прогнозних моделей, як складових забезпечення безперервності бізнес-процесів, з використанням програмних засобів	-	Підготовка до виконання ЛР1.	3	[3] с. 84-95
3	**Прийняття управлінських рішень в задачах інформаційної та кібербезпеки** Основи управлінських рішень. Управлінські рішення, як складова безперервності бізнесу. Прийняття управлінських рішень в умовах невизначеності та ризику, дерева рішень	-	**ПЗ2.** Розв'язання транспортної задачі, як складової забезпечення безперервності бізнес-процесів	Опрацювання теоретичного матеріалу лекції №2. Виконання завдань ПЗ2.	4	[3] с. 9-43, с. 60-67 [4] с. 71-136 [12] с. 69-71
4	-	**ЛР2.** Розв'язання транспортної задачі, як складової забезпечення безперервності бізнес-процесів, з використанням програмних засобів	-	Підготовка до захисту ЛР1. Підготовка до виконання ЛР2.	6	[3] с. 60-67, с. 84-95

5	**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	-	**ПЗ3.** Вирішення завдань захисту програм та інформації за допомогою багатокритеріаль-ної оптимізації на прикладі методу аналізу ієрархій	Опрацювання теоретичного матеріалу лекції №3. Виконання завдань ПЗ3.	4	[1] с. 66-80, с. 185-200 [16] с. 10-60
6	-	**ЛР3.** Вирішення завдань захисту програм та інформації за допомогою багатокритеріаль ної оптимізації з використанням програмних засобів	-	Підготовка до захисту ЛР2. Підготовка до виконання ЛР3.	6	[1] с. 66-78 [3] с. 60-67 [12] с. 40-53

7	**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	-	**ПЗ4.** Оцінювання можливості реалізації потенційної загрози інформації та прийняття рішення в умовах ризику	Опрацювання теоретичного матеріалу лекції №4. Виконання завдань ПЗ4.	4	[1] с. 146-160 [5] с. 13-21 [6] с.7-22, с. 129-180 [10] с. 7-36 [12] с. 53-62
8	-	**ЛР4.** Оцінювання можливості реалізації потенційної загрози інформації та прийняття рішення в умовах ризику з використанням програмних засобів	-	Підготовка до захисту ЛР3. Підготовка до виконання ЛР4.	6	[1] с. 66-78, с. 146-160 [12] с. 40-62

9	**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	-	**ПЗ5.** Якісний та кількісний аналіз інформаційних ризиків	Опрацювання теоретичного матеріалу лекції №5. Виконання завдань ПЗ5.	4	[7] с.180-233 [10] с. 163-186, с. 198-221
10	-	**ЛР5.** Якісний та кількісний аналіз ризиків інформаційної безпеки з використанням програмних засобів	-	Підготовка до захисту ЛР4. Підготовка до виконання ЛР5.	6	[1] с. 146-160 [12] с. 53-62 [15] с. 36-55
11	**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	-	**ПЗ6.** Дослідження методик управління ризиками інформаційної безпеки.	Опрацювання теоретичного матеріалу лекції №6. Виконання завдань ПЗ6.	4	[8] с. 30-44 [10] с. 120-148 [11] с.7-42 [13] с. 16-22

12	-	**ЛР6.** Управління ризиками інформаційної безпеки з використанням програмних засобів	-	Підготовка до захисту ЛР5. Підготовка до виконання ЛР6.	6	[14] с. 14-30 [15] с. 36-55
13	**Загальні моделі у задачах захисту даних та інформації** Мова, об'єкти, суб'єкти у моделях захисту даних та інформації, об'єктно-суб'єктна модель. Модель процесу, системи та функцій захисту. Модель взаємодії відкритих систем у захисті від несанкціонова-ного доступу. Модель з повним перекриттям загроз. Інформаційно-аналітична модель оцінки захисту інформації від загроз несанкціонова-ного доступу. Вартісна модель. Логіко-ймовірнісна модель захисту інформаційних систем, функція імовірності захищеності	-	**ПЗ7.** Моделювання захисту інформації з використанням моделі з повним перекриттям множини загроз	Опрацювання теоретичного матеріалу лекції №7. Виконання завдань ПЗ7.	4	[14] с. 5-13 [17] с. 5-12, с. 19-36 [18] с. 49-81
14	-	**ЛР7.** Моделювання захисту інформації з використанням компонентів нечіткої логіки	-	Підготовка до захисту ЛР6. Підготовка до виконання ЛР7.	6	[9] [14] с. 14-30 [19] с. 32-73

15	**Моделювання загроз та порушника.** Загрози та їх класифікація, як об'єкт моделювання. Дестабілізуючі чинники. Узагальнений підхід щодо побудови моделі загроз. Побудова моделі порушника. Технологія побудови дерева атак	-	**ПЗ8.** Визначення показників захищеності інформації при несанкціонованому доступі	Опрацювання теоретичного матеріалу лекції №8. Виконання завдань ПЗ8.	4	[14] с. 83-88 [18] с. 116-142, с. 168-177 [20], с. 67-75 [21] [22]
16	-	**ЛР8.** Оцінювання рівня захищеності інформаційної системи підприємства	**-**	Підготовка до захисту ЛР7. Підготовка до виконання ЛР8.	6	[9] [14] с. 32-63 [19] с. 32-73
17	**Моделі безпеки систем** Модель ADEPT-50. Модель HRU. Модель Take-Grant. Модель Белла-Лападула. Модель цілісності	Підсумкове заняття **Контрольна робота**	Підсумкове заняття	Опрацювання теоретичного матеріалу лекції №9. Підготовка до захисту ЛР8. Підготовка до контрольної роботи.	3	[14] с. 32-63 [18] с. 240-308, с. 465-473

*** лекції та практичні проводяться по 2 години раз на два тижні;**
**** лабораторні проводяться по 4 години раз в два тижні.**

ПОЛІТИКА ДИСЦИПЛІНИ

Організація освітнього процесу з дисципліни відповідає вимогам положень про організаційне і навчально-методичне забезпечення освітнього процесу, освітній програмі та навчальному плану. Студент зобов'язаний відвідувати лекції, практичні і лабораторні заняття згідно з розкладом, не запізнюватися на заняття, вчасно виконувати та здавати лабораторні та практичні роботи. Термін виконання лабораторної роботи вважається своєчасним, якщо студент здав/захистив її на поточному або наступному за ним занятті. За несвоєчасний захист лабораторної роботи з набраної студентом суми балів вираховується один бал. Підготовкою до виконання лабораторної роботи є виконання завдання відповідного (за темою) практичного заняття. Здача практичних робіт проводиться на початку відповідного (за темою) лабораторного заняття та є допуском студента до виконання лабораторної роботи. Пропущене з поважної причини лабораторне заняття студент повинен відпрацювати у встановлений викладачем термін.

Набуті особою знання з дисципліни або її окремих розділів у неформальній освіті зараховуються відповідно до Положення про порядок перезарахування результатів навчання та визначення академічної різниці у ХНУ https://www.khnu.km.ua/root/files/01/10/03/006.pdf.

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	Практичні заняття (мінімальна кількість оцінок - 8)	Лабораторні роботи	Контрольна робота	Семестровий контроль (іспит)
Тема	1-3		1-3	1-3
Ваговий коефіцієнт	0,15	0,25	0,2	0,4

Оцінювання практичних занять. Оцінка, яка виставляється за практичне заняття, складається з таких елементів: знання теоретичного матеріалу з теми; якість оформлення презентації виконаного завдання; вільне володіння студентом спеціальною термінологією і уміння застосовувати знання на практиці; своєчасна здача завдання з практики.

Оскільки виконане завдання з практики є допуском до виконання відповідної за темою та номером лабораторної роботи, то термін здачі практики вважається своєчасним, якщо студент здав її в день виконання відповідної лабораторної роботи або до цього моменту. У випадку невиконання практики студент не допускається до виконання відповідної за темою та номером лабораторної роботи та зобов'язаний здати виконане практичне завдання у встановлений викладачем термін, але не пізніше, ніж за два тижні до кінця теоретичних занять у семестрі.

Оцінку за практичне заняття викладач оголошує одразу після здачі і проставляє в електронний журнал дисципліни.

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

Оцінка ЄКТС	**Інституційна інтервальна шкала балів**	**Інституційна оцінка, критерії оцінювання**	
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
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 повністю і в достатній кількості забезпечений необхідною навчально-методичною літературою, яка розміщена в модульному середовищі MOODLE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

№	Назва	Режим доступу
1.	Теорія прийняття рішень/ Л.С. Файнзільберг, О.А. Жуковська, В.С. Якимчук. - Київ: Освіта України, 2018. – 246 с.	https://mses.kpi.ua/knigi/zmist/TPR.pdf
2.	Теорії прийняття рішень: курс лекцій/ О.С. Юрков. - Мукачево: МДУ, 2016. - 135 с.	http://www.dut.edu.ua/uploads/l_78_33056835.pdf
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.	http://www.dut.edu.ua/uploads/l_104_95052646.pdf
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.	http://www.dut.edu.ua/uploads/l_1242_54311567.pdf
5.	Управління фінансовими ризиками: навчальний посібник/ С.Г. Шклярук. – Київ: ДП «Вид. дім «Персонал», 2019. – 494 с.	http://maup.com.ua/assets/files/lib/book/upr_fin_ryzik.pdf
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.	https://essuir.sumdu.edu.ua/bitstream-download/123456789/50229/5/Ekonomichnyi_ryzyk%20.pdf
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.	http://ir.stu.cn.ua/bitstream/handle/123456789/19244/Менеджмент%20інформ.%20безп.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
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.	http://apeps.kpi.ua/downloads/Караєва_еколог_економ_ризик.pdf
9.	Методика анализа рисков информационной безопасности с использованием нечёткой логики на базе инструментария Matlab/ Е.К. Баранова, А.М. Гусев. - Образовательные ресурсы и технологии. – 2016. – 1 (13). – С. 88-96.	https://www.muiv.ru/vestnik/pdf/pp/ot_2016_1_088-096.pdf
10.	Оценка и анализ рисков: учебник/ Т.Г. Гурнович, Е.А. Остапенко, С.А. Молчаненко; под общ. ред. Т.Г. Гурнович. – Москва: КНОРУС, 2019. – 252 с.	https://ozon-st.cdn.ngenix.net/multimedia/1024408136.pdf
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.	http://www.dut.edu.ua/uploads/p_303_79299367.pdf
12.	Основи теорії прийняття рішень/ О.І. Кушлик-Дивульська, Б.Р. Кушлик. – К., 2014. – 94 с.	https://ela.kpi.ua/bitstream/123456789/6917/1/13-14-055.pdf
13.	Методичні вказівки до виконання лабораторних робіт з навчальної дисципліни "Менеджмент інформаційної безпеки" [Електронний ресурс]/ уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018.	http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8659/1/Menedzh_inf_bezp_lab.pdf
14.	Моделирование системы защиты информации. Практикум: Учеб. пособие./ Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2015. - 120 с.	https://publications.hse.ru/mirror/pubs/share/folder/w8p5lbfvz1/direct/203455445.pdf
15.	Методичні вказівки до виконання практичних робіт з навчальної дисципліни "Менеджмент інформаційної безпеки" [Електронний ресурс]/ уклад. І. А. Лисенко – Кропивницький: ЦНТУ, 2018.	http://dspace.kntu.kr.ua/jspui/bitstream/123456789/8431/1/Osn_ypr_kiber.pdf
16.	Основи теорії і практики інтелектуального аналізу даних у	http://dwl.kiev.ua/art/oiad/oiad.

	сфері кібербезпеки: навчальний посібник/ Д.В. Ланде, І.Ю. Субач, Ю.Є. Бояринова. – К.: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2018. – 297 с.	pdf
17.	Технології захисту інформації: конспект лекцій [Електронний ресурс]/ А.Ф.Карачка. – Тернопіль: ТНЕУ, 2017.	https://drive.google.com/file/d/1zkTJji64rLODwwbEIp49zIDijXA_5gAM/view?usp=sharing
18.	Моделювання систем захисту інформації/ А.О. Антонюк. - Ірпінь: Національний університет ДПС України, 2015. - 511 с.	https://drive.google.com/file/d/1lIUqEsB2lmpDPTBybiupi8MXS4p-SBys/view?usp=sharing
19.	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.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj3rMLyqojuAhVCtIsKHa_tDlcQFjABegQIAxAC&url=http%3A%2F%2Fir.nusta.edu.ua%2Fjspui%2Fbitstream%2Fdoc%2F857%2F1%2F849_IR%2520.pdf&usg=AOvVaw2zKjASuE2wmT0CCiA4pntw
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.	http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ.%20безпека%20держ.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
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.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwia2_SRqIjuAhXSmIsKHUdKDWcQFjAAegQIAxAC&url=http%3A%2F%2Fjrnl.nau.edu.ua%2Findex.php%2FInfosecurity%2Farticle%2Fdownload%2F13198%2F19118&usg=AOvVaw2AKby6Ib-tNwGpD-OzS0Ns
22.	Математична модель порушника інформаційної безпеки/ Ю.М. Щебланін, Д.І. Рабчун. – Кібербезпека: освіта, наука, техніка. – 2018. – №1(1). – С. 63-72.	https://www.csecurity.kubg.edu.ua/index.php/journal/article/view/21/62

Додаткова

23.	Simulation Modeling and Arena/ Manuel D. Rossetti. – 2nd ed. – Hoboken: John Wiley & Sons, Inc., 2016. – 744 p.	https://fac.ksu.edu.sa/sites/default/files/manuel_d._rossetti-simulation_modeling_and_arena-wiley_2015.pdf
24.	Optimization Models/ G. C. Calafiore, L. El Ghaoui. – Cambridge University Press, 2014. – 627 p.	https://vel.life/凸优化/Optimization.Models.pdf
25.	A Gentle Introduction to Optimization/ B. Guenin, J. Könemann, L. Tunçel. – Cambridge University Press, 2014. – 267 p.	https://industri.fatek.unpatti.ac.id/wp-content/uploads/2019/03/116-A-Gentle-Introduction-to-Optimization-B.-Guenin-J.-Könemann-L.-Tunçel-Edisi-1-2014.pdf
26.	Optimization in Practice with MATLAB: For Engineering Students and Professionals/ A. Messac. – Cambridge University Press, 2015. – 494 p.	http://1.droppdf.com/files/0CRVw/optimization-in-practice-with-matlab-for-engineering-students-and-professionals-achille-messac.pdf
27.	A game theoretic approach to cyber security risk management./ S. Musman, A. Turner// Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. – 2018. - vol. 15(2). – p.127–146.	https://www.researchgate.net/publication/315700133_A_game_theoretic_approach_to_cyber_security_risk_management
28.	Decision Making Under Uncertainty and Reinforcement Learning/Ch. Dimitrakakis, R. Ortner. – CA, USA, 2020. – 267 p.	http://www.cse.chalmers.se/~chrdimi/downloads/book.pdf
29.	Data Mining/ C.C. Aggarwal. – Cham: Springer, Int. Publ. – Switzerland, 2015. - 746 p.	https://doc.lagout.org/Others/Data%20Mining/Data%20Mining_%20The%20Textbook%20%5B

		Aggarwal%202015-04-14%5D.pdf
30.	Качественно-количественный метод оценивания рисков информационной безопасности/ А.Г. Корченко, С.В. Казмирчук // Защита информации - 2016. - т. 18, №2, квітень-червень. - С. 157-170.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Zi_2016_18_2_11
31.	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.	https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjFop27pa7rAhWNxosKHcOBC40QFjAAegQIAhAB&url=http%3A%2F%2Fjrnl.nau.edu.ua%2Findex.php%2FInfosecurity%2Farticle%2Fdownload%2F11824%2F15779&usg=AOvVaw2c4htwI8kpSKRiZpEb40tH
32.	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.	http://dspace.nbuv.gov.ua/bitstream/handle/123456789/117216/17-Titova.pdf?sequence=1
33.	Системи підтримки прийняття рішень: навч. посіб. / М.А. Демиденко; Нац. гірн. ун-т. – Електрон. текст. дані. – Д. : 2016. – 104 с.	http://kist.ntu.edu.ua/textPhD/sppr2.pdf
34.	Методология синтеза адаптивных систем оценивания рисков безопасности ресурсов информационных систем/ А. Г. Корченко, С. В. Казмирчук, Е. В. Иванченко. – Захист інформації. – 2017. – Т. 19, № 3. – С. 198-204.	http://nbuv.gov.ua/UJRN/Zi_2017_19_3_3
35.	Методы и модели адаптивных систем оценки рисков. Диссертация на соискание научной степени кандидата технических наук/ А.Ю. Гололобов. – Киев, 2017. – 182 с.	https://er.nau.edu.ua/bitstream/NAU/25287/1/Дисс_Гололобов.pdf
36.	Аналіз основних складових небезпеки при побудові системи інформаційної безпеки підприємства/ Л.А. Асєєва// Сучасний захист інформації. - 2019. - №2 (38). – с. 42-46.	https://core.ac.uk/download/pdf/325943065.pdf
37.	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.	http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Vchnu_tekh_2019_3_28
38.	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.	http://elar.khnu.km.ua/jspui/handle/123456789/9167
39.	Моделі і методи захисту від загрозливих програм інформаційних систем/ В. М. Джулій, В. О. Бойчук, В. Ю. Тітова, О. В. Сєлюков, О. В. Мірошніченко // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – Київ : ВІКНУ, 2020. – Вип. 67. – С. 72–84.	http://elar.khnu.km.ua/jspui/handle/123456789/9619
40.	Оцінювання ефективності рішень в системах захисту інформації/ В.Ю. Тітова, О.С. Андрощук, В.С. Орленко, І.М. Шевчук, В.С. Даценко// Вісник Хмельницького національного університету. Технічні науки. – 2020. – № 5. – С. 307-309.	http://journals.khnu.km.ua/vestnik/wp-content/uploads/2021/03/VKNU-TS-2020-N5-289.pdf

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Модульне середовище для навчання (розміщені усі необхідні матеріали з дисципліни, в тому числі завдання для поточного та семестрового контролю знань). Доступ до ресурсу: https://msn.khnu.km.ua.

2. Електронна бібліотека університету. Доступ до ресурсу: http://lib.khnu.km.ua/asp/php_f/p1age_lib.php.

Розробник	_____ Підпис	к.т.н., доцент Вчений ступінь, звання	В.С. Орленко Ініціали, прізвище викладача(ів)
Погоджено			
Гарант освітньої програми	_____ Підпис	к.т.н., доцент Вчений ступінь, звання	В.М. Чешун Ініціали, прізвище
Зав. кафедри кібербезпеки та комп'ютерних систем і мереж	_____ Підпис	к.т.н., доцент Вчений ступінь, звання	Ю.П. Кльоц Ініціали, прізвище