

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра _____ кібербезпеки _____
(назва кафедри, яка забезпечує викладання дисципліни)

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
РИЗИК-МЕНЕДЖМЕНТ

_____ (назва навчальної дисципліни)

рівень вищої освіти _____ перший (бакалаврський) _____
перший (бакалаврський) / другий (магістерський)

галузь знань _____ 12 Інформаційні технології _____
(шифр і назва)

спеціальність _____ 125 Кібербезпека _____
(шифр і назва)

освітня програма _____ Кібербезпека _____
(назви освітньої програми)

вид дисципліни _____ спеціальна (фахова) підготовка; вибіркова _____
(загальна підготовка / спеціальна (фахова) підготовка; обов'язкова/вибіркова)

форма навчання _____ денна _____
(денна / заочна/дистанційна)

Харків – 2022 рік

ЛИСТ ЗАТВЕРДЖЕННЯ

Робоча програма з навчальної дисципліни РИЗИК-МЕНЕДЖМЕНТ
(назва дисципліни)

Розробники:

доц, к.е.н., доц.
(посада, науковий ступінь та вчене звання)



(підпис)

Станіслав МІЛЕВСЬКИЙ
(ім'я та прізвище)

Робоча програма розглянута та затверджена на засіданні кафедри

кібербезпеки
(назва кафедри, яка забезпечує викладання дисципліни)

Протокол від “22” серпня 2022 року № 1

Завідувач кафедри



(підпис)


Сергій ЄВСЕЄВ
(ім'я та прізвище)

ЛИСТ ПОГОДЖЕННЯ

Шифр та назва освітньої програми 125 “Кібербезпека”


Кафедра кібербезпеки
(назва кафедри на якій викладається дисципліна)

Гарант ОП

 22.08.2022р
(Підпис, дата)

Сергій ЄВСЕЄВ
(ім'я та прізвище)

Завідувач кафедрою

 22.08.2022р
(Підпис, дата)

Сергій ЄВСЕЄВ
(ім'я та прізвище)

ЛИСТ ПЕРЕЗАТВЕРДЖЕННЯ РОБОЧОЇ НАВЧАЛЬНОЇ ПРОГРАМИ

№ зп	Дата засідання кафедри-розробника РПНД	Номер протоколу	Підпис завідувача кафедри (яка викладає)	Підпис завідувача кафедри (на якій викладається)	Підпис гаранта освітньої програми
1					
2					
3					
4					
5					

МЕТА, КОМПЕТЕНТНОСТІ, РЕЗУЛЬТАТИ НАВЧАННЯ ТА СТРУКТУРНО-ЛОГІЧНА СХЕМА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни “Ризик-менеджмент” – оволодіння майбутніми фахівцями компетентностями, що забезпечують ефективне управління ризиками в сучасних кіберсистемах, уможливають кваліфіковану оцінку ризиків в умовах широкого використання сучасних методів кібербезпеки.

Компетентності та результати навчання

Компетентності	Результати навчання
<p>КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.</p>	<p>РН–9. впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p> <p>РН–13. аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;</p> <p>РН–14. вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;</p> <p>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;</p> <p>РН–18. використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів;</p> <p>РН–19. застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–20. забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;</p> <p>РН–21. вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>РН–22. вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і</p>

Компетентності	Результати навчання
	<p>користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки;</p> <p>РН–23. реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>РН–24. вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових);</p> <p>РН–25. забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;</p> <p>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;</p> <p>РН–27. вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>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\або кібербезпеки;</p> <p>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;</p> <p>РН–32. вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>РН–34. приймати участь у розробці та впровадженні стратегії інформаційної безпеки та\або кібербезпеки відповідно до цілей і завдань організації;</p> <p>РН–35. вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки;</p> <p>РН–42. впроваджувати процеси виявлення,</p>

Компетентності	Результати навчання
	<p>ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p> <p>РН–43. застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів;</p> <p>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;</p> <p>РН–45. застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>РН–46. здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–47. вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>РН–48. виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>РН–49. забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>РН–50. забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>РН–51. підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p>РН–52. використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>РН–53. вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.</p>	<p>РН–9 впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки;</p> <p>РН–13 аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних;</p> <p>РН–14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості</p>

Компетентності	Результати навчання
	<p>прийнятих рішень;</p> <p>RH-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;</p> <p>RH-19 застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах;</p> <p>RH-23 реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах;</p> <p>RH-25 забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту;</p> <p>RH-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;</p> <p>RH-32 вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки;</p> <p>RH-33 вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків;</p> <p>RH-34 приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації;</p> <p>RH-35 вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і/або кібербезпеки;</p> <p>RH-41 забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур;</p> <p>RH-42 впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки;</p> <p>RH-43 застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів;</p>

Компетентності	Результати навчання
	<p>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;</p> <p>РН-45 застосовувати рінні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів;</p> <p>РН-46 здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах;</p> <p>РН-48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p> <p>РН-49 забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах;</p> <p>РН-50 забезпечувати) функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних);</p> <p>РН-51 підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах;</p> <p>РН-52 використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах;</p> <p>РН-53 вирішувати задачі аналізу програмного коду на наявність можливих загроз.</p>
<p>КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.</p>	<p>РН-14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень;</p> <p>РН-20 забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах;</p> <p>РН-31 застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем;</p> <p>РН-36 виявляти небезпечні сигнали технічних засобів;</p> <p>РН-37 вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоків технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації;</p> <p>РН-38 інтерпретувати результати проведення</p>

Компетентності	Результати навчання
	<p>спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації;</p> <p>РН-39 проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах;</p> <p>РН-40 інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації;</p> <p>РН-47 вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації;</p> <p>РН-48 виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах;</p>

Структурно-логічна схема вивчення навчальної дисципліни

Вивчення цієї дисципліни безпосередньо спирається на:	На результати вивчення цієї дисципліни безпосередньо спираються:
Вища математика	Організаційне забезпечення захисту інформації
Менеджмент інформаційної безпеки	Датамайнінг в системах безпеки
Основи математичного моделювання систем безпеки	

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

(розподіл навчального часу за семестрами та видами навчальних занять)

Семестр	Всього (годин) / кредитів ECTS	З них		За видами аудиторних занять (годин)			Індивідуальні завдання студентів (КП, КР, РГ, Р, РЕ)	Поточний контроль (кількість робіт)	Семестровий контроль	
		Аудиторні заняття (годин)	Самостійна робота (годин)	Лекції	Лабораторні заняття	Практичні заняття, семінари			Залік	Екзамен
1	2	3	4	5	6	7	8	9	10	11
6	90/3	36	54	24	12	-	-	2	-	+

Співвідношення кількості годин аудиторних занять до загального обсягу складає 40 (%).

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п.	Види навчальних занять (Л, ЛЗ, ПЗ, СР)	Кількість годин	Номер семестру (якщо дисципліна викладається у декількох семестрах). Найменування тем та питань кожного заняття. Завдання на самостійну роботу.	Рекомендована література (базова, допоміжна)
1	Л	2	Тема 1. Сутність та характеристика ризиків.	1-3
	СР	4		
2	Л	2	Тема 1. Сутність та характеристика ризиків	1-3
	ЛЗ СР	2 4	Лабораторне заняття № 1 "Критерії прийняття рішень у конфліктних ситуаціях".	
3	Л	2	Тема 2. Показники ризику та методи його оцінювання.	1-3
	СР	4		
4	Л	2	Тема 2. Показники ризику та методи його оцінювання.	1-3
	ЛЗ СР	2 4	Лабораторне заняття № 2 "Оцінка ризику за допомогою статистичного методу".	
5	Л	2	Тема 3. Система управління ризиками.	1-3
	СР	4		
6	Л	2	Тема 3. Система управління ризиками.	1-3
	ЛЗ СР	2 7	Лабораторне заняття № 3. "Визначення та аналіз ризику на підставі методу аналізу доцільності витрат".	
7	Л	2	Тема 4. Програма управління ризиками.	1-3
	СР	4		
8	Л	2	Тема 4. Програма управління ризиками.	1-3
	ЛЗ СР	2 4	Лабораторне заняття № 4. "Прийняття інвестиційних рішень в умовах проектного ризику".	
9	Л	2	Тема 5. Кількісна оцінка ризиків кібербезпеки.	1-3
	СР	4		
10	Л	2	Тема 5. Кількісна оцінка ризиків кібербезпеки.	1-3
	ЛЗ СР	2 4	Лабораторне заняття № 5. "Оцінка фінансового ризику при прийнятті рішень".	
11	Л	2	Тема 6. Управління ризиками інформаційної безпеки.	1-3
	СР	4		
12	Л	2	Тема 6. Управління ризиками інформаційної безпеки.	1-3
	ЛЗ СР	2 7	Лабораторне заняття № 6. "Проектування та аналіз системи управління ризиками кібербезпеки".	
Разом (годин)		90		

САМОСТІЙНА РОБОТА

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час.

№ з/п	Назва видів самостійної роботи	Кількість годин
1	Опрацювання лекційного матеріалу	24
2	Підготовка до лабораторних занять	30
	Разом	54

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальне завдання не передбачено.

МЕТОДИ НАВЧАННЯ

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди.

МЕТОДИ КОНТРОЛЮ

Поточний контроль при вивченні дисципліни реалізується у формі опитувань на лекційних заняттях, захисту лабораторних робіт, проведення контрольних робіт.

Контроль складової робочої програми, яка освоюється під час самостійної роботи студента, проводиться:

- з лекційного матеріалу – шляхом проведення тестування, презентацій докладів за темами лекційних занять;
- з лабораторних завдань – за допомогою перевірки виконаних завдань.

Семестровий контроль проводиться у формі екзамену відповідно до навчального плану в обсязі навчального матеріалу, визначеного навчальною програмою та у терміни, встановлені навчальним планом.

Семестровий контроль проводиться по екзаменаційних білетах в письмовій формі за контрольними завданнями, а також шляхом тестування з використанням технічних засобів.

Результати поточного контролю враховуються як допоміжна інформація для виставлення оцінки з даної дисципліни.

Студент вважається допущеним до семестрового екзамену з навчальної дисципліни за умови повного відпрацювання усіх лабораторних робіт,

виконання контрольних робіт та тестових опитувань, що передбачено навчальною програмою з дисципліни.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ, ТА ШКАЛА ОЦІНЮВАННЯ ЗНАНЬ ТА УМІНЬ (НАЦІОНАЛЬНА ТА ECTS)

Таблиця 1 – Розподіл балів для оцінювання успішності студента для іспиту

Контрольні роботи	Лабораторні роботи	КП	РГЗ	Індивідуальні завдання	Тощо	Іспит	Сума
18	42	–	–	–	–	40	100

Критерії та система оцінювання знань та вмінь студентів.

Згідно основних положень ЄКТС, під **системою оцінювання** розуміють сукупність методів (письмові, усні і практичні тести, екзамени, проекти, тощо), що використовуються при оцінюванні досягнень особами, що навчаються, очікуваних результатів навчання.

Успішне оцінювання результатів навчання є передумовою присвоєння кредитів особі, що навчається. Тому твердження про результати вивчення компонентів програм завжди повинні супроводжуватися зрозумілими та відповідними **критеріями оцінювання** для присвоєння кредитів. Це дає можливість стверджувати, чи отримала особа, що навчається, необхідні знання, розуміння, компетенції.

Критерії оцінювання – це описи того, що як очікується, має зробити особа, яка навчається, щоб продемонструвати досягнення результату навчання.

Основними концептуальними положеннями системи оцінювання знань та вмінь студентів є:

1. Підвищення якості підготовки і конкурентоспроможності фахівців за рахунок стимулювання самостійної та систематичної роботи студентів протягом навчального семестру, встановлення постійного зворотного зв'язку викладачів з кожним студентом та своєчасного коригування його навчальної діяльності.

2. Підвищення об'єктивності оцінювання знань студентів відбувається за рахунок контролю протягом семестру із використанням 100 бальної шкали (табл. 2). Оцінки обов'язково переводять у національну шкалу (з виставленням державної семестрової оцінки “відмінно”, “добре”, “задовільно” чи “незадовільно”) та у шкалу ECTS (A, B, C, D, E, FX, F).

Таблиця 2 – Шкала оцінювання знань та умінь: національна та ЄКТС

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	2	3	4	5
90-100	A	Відмінно	<ul style="list-style-type: none"> - Глибоке знання навчального матеріалу, що містяться в основних і додаткових літературних джерелах; - вміння аналізувати явища, які вивчаються, в їхньому взаємозв'язку і розвитку; - вміння проводити теоретичні розрахунки; - відповіді на запитання чіткі, лаконічні, логічно послідовні; - вміння вирішувати складні практичні задачі. 	Відповіді на запитання можуть містити незначні неточності
82-89	B	Добре	<ul style="list-style-type: none"> - Глибокий рівень знань в обсязі обов'язкового матеріалу, - вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; - вміння вирішувати складні практичні задачі. 	Відповіді на запитання містять певні неточності ;
75-81	C	Добре	<ul style="list-style-type: none"> - Міцні знання матеріалу, що вивчається, та його практичного застосування; - вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; - вміння вирішувати практичні задачі. 	- невміння використовувати теоретичні знання для вирішення складних практичних задач .
64-74	D	Задовільно	<ul style="list-style-type: none"> - Знання основних фундаментальних положень матеріалу, що вивчається, та їх практичного застосування; - вміння вирішувати прості практичні задачі. 	Невміння давати аргументовані відповіді на запитання; <ul style="list-style-type: none"> - невміння аналізувати викладений матеріал і виконувати розрахунки;

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	2	3	4	5
				- невміння вирішувати складні практичні задачі.
60-63	E	Задовільно	- Знання основних фундаментальних положень - вміння вирішувати найпростіші практичні задачі.	Незнання окремих (непринципови х) питань з матеріалу модуля; - невміння послідовно і аргументовано висловлювати думку; - невміння застосовувати теоретичні положення при розв'язанні практичних задач
35-59	FX (потрібне додаткове вивчення)	Незадовільно	Додаткове вивчення матеріалу може бути виконане в терміни, що передбачені навчальним планом.	Незнання основних фундаменталь них положень навчального матеріалу модуля; - істотні помилки у відповідях на запитання; - невміння розв'язувати прості практичні задачі.
1-34	F (потрібне повторне вивчення)	Незадовільно	-	- Повна відсутність знань значної частини навчального матеріалу модуля; - істотні помилки у відповідях на запитання;

Рейтингова Оцінка, бали	Оцінка ECTS та її визначення	Національна оцінка	Критерії оцінювання	
			позитивні	негативні
1	2	3	4	5
				-незнання основних фундаментальн их положень; - невміння орієнтуватися під час розв'язання простих практичних задач

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Стандарт вищої освіти галузі знань 12 “Інформаційні технології” для першого (бакалаврського) рівня вищої освіти, який затверджено наказом Міністерства освіти і науки України від 04.10.2018 р. № 1074 та введено в дію з 2018/2019 навч. року.

2. Робоча програма навчальної дисципліни.

3. Силабус навчальної дисципліни

4. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ” [Електроннийресурс]. – Режим доступу: https://iiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fua1%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1	Обґрунтування господарських рішень і оцінювання ризиків : навч. посіб. / Т. С. Клебанова, О. В. Мілов, С. В. Мілевський та ін. – Харків : Вид. ХНЕУ, 2010. – 262 с.
2	Корченко О.Г. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. [Електронний ресурс] / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. –К.: Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. – 190 с.
3	Писаревський І. М. Управління ризиками: навч. посіб. / І. М. Писаревський, О. Д. Стешенко. – Харків: ХНАМГ, 2008. – 124 с.

Допоміжна література

4	ISO / IEC 31010:2009 Risk management – Risk assessment techniques [Electronic resource]. – Access mode: http://www.iso.org/iso/ru/catalogue_detail?csnumber=51073
5	ISO/IEC 27004:2016 (E). Information technology — Security techniques — Information security management — Measurement.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. The Open Web Application Security Project (OWASP) Електронний ресурс]. Режим доступу: <https://www.owasp.org>
2. Threat Modeling [Електронний ресурс]. Режим доступу: <https://msdn.microsoft.com/enus/library/ff648644.aspx>.
3. Персональні навчальні системи кафедри кібербезпеки НТУ “ХПІ” [Електроннийресурс]. – Режим доступу: https://iiii-my.sharepoint.com/personal/serhii_yevseiev_khpi_edu_ua1/_layouts/15/onedrive.aspx?ga=1&id=%2Fpersonal%2Fserhii%5Fyevseiev%5Fkhpi%5Fedu%5Fu%2FDocuments%2F%D0%9F%D0%9D%D0%A1%20%D0%BA%D0%B0%D1%84%D0%B5%D0%B4%D1%80%D0%B8