МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра кібербезпеки та DATA-технологій, факультет №6

РОБОЧА ПРОГРАМА

навчальної дисципліни «**Моделі ризик-орієнтованого аналізу в кібербезпеці**»
обов'язкових компонент
освітньої програми другого (магістр) рівня вищої освіти

125 «Кібербезпека» (безпека інформаційних та комунікаційних систем)

Харків 2023

ЗАТВЕРДЖЕНО
Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 22.12.2023 № 11

СХВАЛЕНО
Вченою радою факультету № 6
Протокол від 20.12.2023 № 11

ПОГОДЖЕНО
Секцією Науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 21.12.2023 № 11

Розглянуто на засіданні кафедри кібербезпеки та DATA-технологій факультету № 6 *(протокол від 15.12.2023 №12)*

Розробник:
Доцент кафедри, к. т. н., доцент Хавіна І.П.

Рецензенти:
1. Професор кафедри комп'ютерних наук та інформаційних технологій Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» д. т. н., професор Малєєва О. В.

2. Професор кафедри інформаційних технологій та кібербезпеки ХНУВС, к.т.н., доцент Носов В. В.

1. Опис навчальної дисципліни

Найменування показників	Шифри та назви галузі знань, код та назва спеціальності, ступень вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS – 3 Загальна кількість годин – 90 Кількість тем – 7	12 Інформаційні технології; (шифр галузі) (назва галузі знань) 125 – Кібербезпека Магістр з кібербезпеки та захисту інформації (назва СВО)	Навчальний курс – 1 Семестр – 2 Види підсумкового контрою: – залік
Розподіл навчальної дисципліни за видами занять:		
денна форма навчання Лекції – 20 годин; Практичні заняття – 0 годин; Лабораторні заняття – 20 години; Самостійна робота – 50 годин; Індивідуальні завдання: -		заочна форма навчання Лекції – 4 годин; Практичні заняття – 0 годин; Лабораторні заняття – 4 години; Самостійна робота – 82 годин; Індивідуальні завдання: -

2. Мета та завдання навчальної дисципліни

Метою викладання дисципліни «Моделі ризик-орієнтованого аналізу в кібербезпеці» є формування компетентності в області оцінювання ризиків інформаційної безпеки підприємства на основі аналізу базових понять, методів, моделей, засобів та міжнародних нормативних документів, пов’язаних з оцінюванням і управлінням ризиками.

Основними завданнями вивчення дисципліни «Моделі ризик-орієнтованого аналізу в кібербезпеці» є отримання знань та навичок щодо аналізу, оцінки, управління та моніторингу стану захищеності об'єктів інформатизації на основі сучасних моделей та методів ризик-орієнтованого підходу. Отримання студентами необхідних знань щодо теоретичної та практичної підготовки з впровадження необхідних знань про принципи і методи ідентифікації та обробки ризиків, інструментальні засоби та нормативні документи з аналізу ризиків ІБ, що дозволяють успішно ідентифікувати, управляти та здійснювати моніторинг ризиків інформаційної безпеки організації в умовах активного використання сучасних інформаційних технологій; необхідна для курсового та дипломного проектування.

Міждисциплінарні зв’язки: дисципліна «Моделі ризик-орієнтованого аналізу в кібербезпеці» базується на викладання дисциплін «Методика наукових досліджень», «Моделювання складних нелінійних процесів в кібербезпеці», «Розвідувально-аналітична робота у кіберсфері» та освітньої програми першого (бакалаврського) рівня вищої освіти **125 «Кібербезпека».**

Очікувані результати навчання: дисципліна формує компетенції з проблем теорії та практики щодо аналізу, оцінки, методів управління та моніторингу стану захищеності об'єктів інформатизації на основі сучасних моделей та методів ризик-орієнтованого підходу. У результаті вивчення навчальної дисципліни здобувач вищої освіти повинен:

***знати*:**

- основні поняття і визначення управління інформаційними ризиками;
- основні етапи забезпечення режиму інформаційної безпеки.
- компоненти аналізу ризиків: ідентифікація ризиків (ідентифікація активів, погроз, вразливостей, впливу, засобів контролю) та інше;
- технології аналізу інформаційних ризиків;
- розробку корпоративної методики аналізу ризиків;
- програмні засоби, що використовуються для аналізу і управління ризиками;
- аудит безпеки і аналіз інформаційних ризиків.

вміти:

- знаходити організаційно-управлінські рішення в нестандартних ситуаціях і нести за них відповідальність;
- складати огляд з питань забезпечення інформаційної безпеки за профілем своєї діяльності;
- організовувати і підтримувати виконання комплексу заходів щодо інформаційної безпеки;
- управляти процесом їх реалізації з урахуванням вирішуваних задач і організаційної структури об'єкта захисту, зовнішніх впливів, ймовірних загроз і рівня розвитку технологій захисту інформації;
- здійснювати підбір, вивчення і узагальнення науково-технічної літератури, нормативних та методичних матеріалів з питань забезпечення інформаційної безпеки.

Програмні компетентності, які формуються при вивченні навчальної дисципліни:		
Інтегральна компетентність	Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.	
загальні компетентності (КЗ)	КЗ.1	Здатність застосовувати знання у практичних ситуаціях..
	КЗ.2	Здатність проводити дослідження на відповідному рівні.
	КЗ.3	Здатність до абстрактного мислення, аналізу та синтезу.

	КЗ.4	Здатність оцінювати та забезпечувати якість виконуваних робіт.
	КЗ.5	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
Фахові Компетентності (КФ)	КФ.1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
	КФ.2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
	КФ.3	Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури
	КФ.4	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
	КФ.5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ.6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ.7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури

		управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
	КФ.8	Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
	КФ.9	Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
	КФ.10	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
	КФ.11	Здатність управляти системою попередження, розкриття та розслідування правопорушень, здійснених з використанням можливостей кіберсфери.
Програмні результати навчання (РН)	РН.6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення
	РН.10	Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації
	РН.16	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень
	РН.21	Використовувати методи натурного, фізичного і комп’ютерного моделювання для дослідження

		процесів, які стосуються інформаційної безпеки та/або кібербезпеки

3. Програма навчальної дисципліни

Тема № 1. Вступ до теорії ризиків ІБ. Базові поняття управління ризиками інформаційної безпеки. Загальні положення щодо оцінки і управління ризиками кібер- і інформаційної безпеки. Критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки.

Тема № 2. Технології аналізу ризиків. Ідентифікація ризиків. Оцінка ризиків. Вимірювання ризиків. Вибір допустимого рівня ризику. Вибір контрзаходів та оцінка їх ефективності.

Тема № 3. Міжнародні стандарти в галузі аналізу та оцінювання ризиків. Стандарт ISO 27005:2019. Методи і засоби аналізу та оцінювання ризиків. Аналіз та порівняння методики управління ризиками інформаційної безпеки NIST, OCTAVE, CRAMM.

Тема № 4. Методичний підхід до управління ризиками безпеки інформації. Ідентифікація активів. Ідентифікація загроз. Визначення ймовірності виникнення. Визначення впливу від реалізації загрози. Оброблення ризиків ІБ та вибір рекомендованих контролів. Документація.

Тема № 5. Оцінка ризиків експертними методами.

Оцінка суб'єктивної ймовірності. Методи оцінок безперервних розподілів. Розв’язання завдання оцінки ризиків за допомогою теорії ігор.

Тема № 6. Метод оцінки ризиків на основі моделі загроз і вразливостей.

Основні поняття та припущення моделі. Розрахунок ризиків за загрозою. Завдання контрзаходів. Ефективність введення контрзаходу. Приклад застосування.

Тема № 7. Методика аналізу ризиків інформаційної безпеки на основі нечіткої логіки.

Введення у нечітку логіку. Нечіткі множини. Методи побудови функцій приналежності нечітких множин. Операції над ними. Моделювання нечіткої системи оцінки ризиків ІБ. Нечітка та лінгвістична змінна. Нечіткий висновок.

4. Структура навчальної дисципліни

4.1.1. Розподіл часу навчальної дисципліни за темами (денна форма навчання)

Номер та назва навчальної теми	Кількість годин, відведених на вивчення навчальної дисципліни						Вид контролю
	Всього	з них:					
		лекції	Семінарські заняття	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр № 2							
Тема № 1. Вступ до теорії ризиків ІБ.	**10**	**2**			**2**	**6**	
Тема № 2. Технології аналізу ризиків.	**10**	**2**			**2**	**6**	
Тема № 3. Міжнародні стандарти в галузі аналізу та оцінювання ризиків	**16**	**4**			**4**	**8**	
Тема № 4. Методичний підхід до управління ризиками безпеки інформації.	**8**	**2**			**2**	**4**	
Тема № 5. Оцінка ризиків експертними методами.	**14**	**2**			**4**	**8**	
Тема № 6. Метод оцінки ризиків на основі моделі загроз і вразливостей.	**14**	**4**			**2**	**8**	
Тема № 7. Методика аналізу ризиків інформаційної безпеки на основі нечіткої логіки.	**18**	**4**			**4**	**10**	
Всього по дисципліні	**90**	**20**			**20**	**50**	**Залік**

4.2. Завдання на самостійну роботу

Завдання що виносяться на самостійну роботу студента			Література:
Семестр № 2			
	Тема 1. Вступ до теорії ризиків ІБ.		
		Базові поняття управління ризиками інформаційної безпеки	Конспект лекцій, література [1-18]
		Загальні положення щодо оцінки і управління ризиками кібер- і інформаційної безпеки	Конспект лекцій, література [1-18]
		Критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки	Конспект лекцій, література [1-18]
	Тема 2. Технології аналізу ризиків.		
		Ідентифікація ризиків. Оцінка ризиків. Вимірювання ризиків	Конспект лекцій, література [1-18]
		Вибір допустимого рівня ризику. Вибір контрзаходів та оцінка їх ефективності.	Конспект лекцій, література [1-18]
	Тема 3. Міжнародні стандарти в галузі аналізу та оцінювання ризиків.		
		Методи і засоби аналізу та оцінювання ризиків	Конспект лекцій, література [1-18]
		Стандарт ISO 27005:2019.	Конспект лекцій, література [1-18]
	Тема 4. Методичний підхід до управління ризиками безпеки інформації.		
		Ідентифікація активів. Ідентифікація загроз.	Конспект лекцій, література [1-18]
		Визначення ймовірності виникнення.	Конспект лекцій, література [1-18]
		Визначення впливу від реалізації загрози.	Конспект лекцій, література [1-18]
		Оброблення ризиків ІБ та вибір рекомендованих контролів.	Конспект лекцій, література [1-18]
	Тема 5. Оцінка ризиків експертними методами.		
		Основні поняття та припущення моделі.	Конспект лекцій, література [1-18]
		Методи оцінок безперервних розподілів.	Конспект лекцій, література [1-18]
	Тема 6. Метод оцінки ризиків на основі моделі загроз і вразливостей.		
		Основні поняття та припущення моделі.	Конспект лекцій, література [1-18]
		Розрахунок ризиків за загрозою.	Конспект лекцій, література [1-18]
		Завдання контрзаходів. Ефективність введення контрзаходу.	Конспект лекцій, література [1-18]
	Тема 7. Методика аналізу ризиків інформаційної безпеки на основі нечіткої логіки.		
		Введення у нечітку логіку. Нечіткі множини. Методи побудови функцій приналежності нечітких множин. Операції над ними.	Конспект лекцій, література [1-18]
		Моделювання нечіткої системи оцінки ризиків ІБ. Нечітка та лінгвістична змінна. Нечіткий висновок	Конспект лекцій, література [1-18]

5. Індивідуальні завдання

6. Методи навчання

Вивчення курсу дозволить здобувачам вищої освіти оволодіти необхідними теоретичними знаннями щодо побудови та принципів функціонування комплексних систем захисту інформації. В навчальному плані для вивчення дисципліни передбачені такі організаційні форми занять як лекції, практичні та лабораторні заняття.

На лекційних заняттях викладаються теоретичні засади тем, що вивчаються, а також приклади їх використання для розв'язання конкретних навчальних задач.

На практичних заняттях під керівництвом викладача слухачі відпрацьовують прийоми виконання типових задач. Практичні заняття проводяться в комп'ютерному класі. Практичні заняття проводяться у здвоєному форматі, що дозволяє більш ефективно використовувати комп'ютерну техніку.

Перед практичним заняттям слухач повинен вивчити певний теоретичний матеріал і (можливо) виконати практичне завдання у відповідності до методичних вказівок до практичних занять з дисципліни. Після закінчення практичного заняття слухач отримує домашнє завдання для закріплення практичних навичок розв'язання задач.

Основним видом інформаційно-методичного забезпечення дисципліни є:

- конспект лекцій;
- методичні вказівки до практичних занять;
- навчальні посібники з дисципліни.

Перелічені складові елементи інформаційно-методичного забезпечення існують як у друкованому вигляді, так і в електронній формі у вигляді роздаткових матеріалів, відповідного розділу сайту кафедри кібербезпеки та інформаційних систем, а також у вигляді електронного навчального комплексу з дисципліни у системі ДО ХНУВС.

7. Перелік питань та завдань, що виносяться на підсумковий контроль

1. Мета аналізу та управління ризиками.
2. Ідентифікація ризиків і Реєстр ризиків.
3. Оцінка ризиків. Вимірювання ризиків.
4. Вибір допустимого рівня ризику.
5. Вибір контрзаходів та оцінка їх ефективності.
6. Етапи процесу аналізу та управління ризиком.
7. Правила управління ризиками.
8. Ідентифікація активів.
9. Ідентифікація загроз.
10. Визначення ймовірності виникнення загроз.
11. Визначення впливу від реалізації загрози.
12. Оброблення ризиків ІБ та вибір рекомендованих контролів.
13. Критерії вибору методів оцінки і управління ризиками інформаційної і кібербезпеки.

14. Сутність кількісного аналізу ризиків.
15. Методи кількісного оцінювання ризику.
16. Сутність якісного аналізу ризиків та групування якісних методів оцінювання ризику.
17. Імовірнісний метод оцінювання ризику.
18. Характеристики та типи визначеності та невизначеності.
19. Методи кількісної та якісної оцінки ризиків.
20. Основні методи оцінки та аналізу інформаційних ризиків.
21. Методи аналізу ризику та невизначеності в управлінні інформаційною безпекою.
22. Якісні та кількісні методики управління інформаційними ризиками.
23. Методики оцінки та аналізу ризиків NIST.
24. Методики оцінки та аналізу ризиків OCTAVE.
25. Методики оцінки та аналізу ризиків CRAMM.
26. Поняття, сутність та призначення управління ризиками. Стадії та принципи управління ризиками. Заходи мінімізації ризиків.
27. Методи оцінки інформаційних ризиків за стандартом ISO 27005:2019.
28. Загальна характеристика експертних процедур, їх використання для розрахунку рівня ризику проекту.
29. Оцінка ризиків експертними методами.
30. Методи оцінок безперервних розподілів.
31. Нечіткі множини.
32. Методи побудови функцій приналежності нечітких множин.
33. Операції над нечіткими множинами.
34. Моделювання нечіткої системи оцінки ризиків ІБ.
35. Нечітка та лінгвістична змінна.
36. Нечіткий висновок.
37. Які змінні називаються лінгвістичними?
38. Які етапи включає в себе процес проектування нечітких систем?
39. У чому полягає процес фазифікації?
40. У чому полягає процес дефаззіфікації?
41. Які методи дефаззіфікації можуть використовуватися при побудові нечітких систем?
42. Як сформулюються правила нечіткого висновку для випадку однієї вхідної змінної, для випадку двох вхідних змінних?
43. Які є функцій приналежності нечітких множин?
44. Наведіть опис трикутної функції приналежності в аналітичному та графічному вигляді.

45. Наведіть опис трапецієподібної функції належності в аналітичному та графічному вигляді.
46. Наведіть структуру нечіткої системи моделювання.
47. У чому полягає суть методології нечіткого моделювання?
48. Які правила мають системи типу Мамдані і Сугено?
49. З яких кроків складається процес створення нечітких систем?
50. Які операції необхідно виконати для визначення чіткого виходу функції?

8. Розподіл балів, які отримують здобувачі вищої освіти з навчальної дисципліни

Контрольні заходи включають у себе поточний та підсумковий контроль.

Поточний контроль.

До форм поточного контролю належить оцінювання:

- рівня знань під час практичних, лабораторних занять;
- якості виконання індивідуальної та самостійної роботи.

Поточний контроль здійснюється під час проведення практичних та лабораторних занять і має за мету перевірку засвоєння знань, умінь і навичок здобувачем вищої освіти з навчальної дисципліни.

У ході поточного контролю проводиться систематичний вимір приросту знань, їх корекція. Результати поточного контролю заносяться викладачем до журналів обліку роботи академічної групи за національної системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Оцінки за самостійну та індивідуальну роботи виставляються в журнали обліку роботи академічної групи в окрему графу за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»). Результати цієї роботи враховуються під час виставлення підсумкових оцінок.

При розрахунку успішності здобувачів вищої освіти в Університеті враховуються такі види робіт: навчальні заняття (практичні, лабораторні тощо); самостійна та індивідуальна роботи (виконання домашніх завдань, ведення конспектів першоджерел та робочих зошитів, виконання розрахункових завдань, підготовка рефератів, наукових робіт, публікацій, розроблення спеціальних технічних пристроїв і приладів, моделей, комп'ютерних програм, виступи на наукових конференціях, семінарах та інше); контрольні роботи (виконання тестів, контрольних робіт у вигляді, передбаченому в робочій програмі навчальної дисципліни). Вони оцінюються за національною системою оцінювання («відмінно», «добре», «задовільно», «незадовільно»).

Результат навчальних занять за семестр розраховується як середньоарифметичне значення з усіх виставлених оцінок під час навчальних занять протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи в окрему графу.

Результат самостійної роботи за семестр розраховується як

середньоарифметичне значення з усіх виставлених оцінок з самостійної роботи, отриманих протягом семестру та виставляється викладачем в журналі обліку роботи академічної групи в окрему графу.

Здобувач вищої освіти***, який отримав оцінку «незадовільно» за навчальні заняття або самостійну роботу, зобов'язаний його відпрацювати.***

Загальна кількість балів (оцінка), отримана здобувачем за семестр перед підсумковим контролем, розраховується як середньоарифметичне значення з оцінок за навчальні заняття та самостійну роботу, та для переводу до 100-бальної системи помножується на коефіцієнт **10**.

Загальна кількість балів (перед підсумковим контролем)	***=((***	***Результат навчальних занять за семестр***	***+***	***Результат самостійної роботи за семестр***	***) /***	***2)***	****10***

Підсумковий контроль.

Підсумковий контроль проводиться з метою оцінки результатів навчання на певному ступені вищої освіти або на окремих його завершених етапах.

Для обліку результатів підсумкового контролю використовується поточно-накопичувальна інформація, яка реєструються в журналах обліку роботи академічної групи. Результати підсумкового контролю з дисциплін відображуються у відомостях обліку успішності, навчальних картках курсантів (студентів, слухачів), залікових книжках. ***Присутність курсантів (студентів, слухачів) на проведенні підсумкового контролю (заліку, екзамену) обов'язкова.*** Якщо здобувач вищої освіти не з'явився на підсумковий контроль (залік, екзамен), то науково-педагогічний працівник ставить у відомість обліку успішності відмітку «не з'явився».

Підсумковий контроль (екзамен, залік) оцінюється за національною шкалою. Для переводу результатів, набраних на підсумковому контролі (екзамені, заліку), з національної системи оцінювання в 100-бальну вводиться коефіцієнт **10**, таким чином максимальна кількість балів на підсумковому контролі (екзамені, заліку), які використовуються при розрахунку успішності курсантів (студентів, слухачів), становить – **50.**

Підсумкові бали з навчальної дисципліни визначаються як сума балів, отриманих здобувачем протягом семестру та балів, набраних на підсумковому контролі (екзамені, заліку).

Підсумкові бали навчальної дисципліни	=	***Загальна кількість балів (перед підсумковим контролем)***	+	***Кількість балів за підсумковим контролем***

Здобувач вищої освіти, який під час складання підсумкового контролю отримав оцінку «незадовільно», складає підсумковий контроль (екзамен, залік) повторно. Повторне складання підсумкового контролю (екзамену, заліку) допускається не більше двох разів з кожної навчальної дисципліни, у тому числі один раз – викладачеві, а другий – комісії, що створюється навчально-науковими інститутами (факультетами). Незадовільні оцінки виставляються тільки в відомостях обліку успішності. Студентам, які отримали не більше як дві незадовільні оцінки (нижче ніж 60 балів) з навчальної дисципліни, можуть бути

встановлені різні строки ліквідації академічної заборгованості, але не пізніше як за день до фактичного початку навчальних занять у наступному семестрі. Студенти, які не ліквідували академічну заборгованість у встановлений термін, відраховуються з Університету. Особи, які одержали більше двох незадовільних оцінок (нижче ніж 60 балів) за підсумковими результатами вивчення навчальних дисциплін з урахуванням підсумкового контролю, відраховуються з Університету.

Результат вивчення дисципліни визначається як середньоарифметичне значення балів, набраних у поточному та попередньому семестрах.

$$\textit{Підсумкові бали навчальної дисципліни} = \frac{\textit{Підсумкові бали за поточний семестр} + \textit{Підсумкові бали за попередній семестр}}{2}$$

Кафедрою визначено наступні критерії оцінювання результатів роботи здобувачів вищої освіти під час поточного контролю (роботу на семінарських, практичних, лабораторних й інших аудиторних заняттях, виконання самостійних навчальних та індивідуальних творчих завдань) та підсумкового контролю.

Робота під час навчальних занять	Самостійна та індивідуальна робота	Підсумковий контроль
Отримати не менше 4 позитивних оцінок (денна форма навчання)	Підготувати реферат, підготувати конспект за темами самостійної роботи.	Отримати за підсумковий контроль не менше 30 балів

9. Шкала оцінювання: національна та ECTS

Оцінка в балах	**Оцінка за національною шкалою**	**Оцінка**	
		Оцінка	**Пояснення**
97-100	Відмінно («зараховано»)	A	«**Відмінно"** – теоретичний зміст курсу засвоєний **цілком,** необхідні практичні навички роботи з освоєним матеріалом сформовані, **усі** навчальні завдання, які передбачені програмою навчання **виконані** в повному обсязі, відмінна робота без помилок або з однією незначною помилкою.
94-96			
90-93			
85- 89	Добре («зараховано»)	B	«**Дуже добре"** – теоретичний зміст курсу засвоєний **цілком**, потрібні практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **більшості** з них оцінена числом балів, близьким до **максимального,** робота з двома-трьома незначними помилками.
80-84			
75-79		C	«**Добре"** – теоретичний зміст курсу засвоєний **цілком**, практичні навички роботи з освоєним матеріалом **в основному** сформовані, **усі** навчальні завдання, які передбачені програмою навчання, **виконані**, якість виконання **жодного** з них **не оцінена мінімальним** числом балів, деякі види завдань виконані **з помилками,** робота з декількома незначними помилками, або з однією-двома значними помилками.
70 -74	Задовільно («зараховано»)	D	«**Задовільно"** – теоретичний зміст курсу засвоєний **частково**, але **прогалини не носять істотний** характер, потрібні практичні навички роботи з освоєним матеріалом **в основному** сформовані,

65-69			**більшість** передбачених програмою навчання навчальних завдань **виконана, деякі** з виконаних завдань містять **помилки,** робота з трьома значними помилками.
60-64		E	«**Достатньо"** – теоретичний зміст курсу освоєний **частково, деякі** практичні навички роботи **не сформовані, частина** передбачених програмою навчання навчальних завдань **не виконана,** або якість виконання деяких з них оцінена числом балів, близьким до **мінімального**, робота, що задовольняє мінімуму критеріїв оцінки.
41-59	Незадовільно («не зараховано»)	FX	«**Умовно незадовільно"** – теоретичний зміст курсу засвоєний **частково**, потрібні практичні навички роботи **несформовані, більшість** передбачених програмою навчання, навчальних завдань **не виконано**, або якість їхнього виконання оцінено числом балів, близьким до **мінімального**; при **додатковій самостійній** роботі над матеріалом курсу **можливе підвищення якості** виконання навчальних завдань (**з можливістю повторного складання**), робота, що потребує доробки.
21-40			
1-20		F	«**Безумовно незадовільно"** – теоретичний зміст курсу **неосвоєний**, потрібні практичні навички роботи **несформовані, всі виконані** навчальні завдання містять грубі **помилки, додаткова самостійна** робота над матеріалом курсу **не приведе** до значного **підвищення якості** виконання навчальних завдань, робота, що потребує повної переробки.

10. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті

Нормативно-правові акти

1. ДСТУ ISO/IEC 27005:2022 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT), URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797 (дата звернення: 14.07.2023).

Навчальна та наукова література:

2. Архипов О. Є. Вступ до теорії ризиків: інформаційні ризики : моногр. /О. Є. Архипов. – К. : Нац. акад. СБУ, 2015. – 248.

3. Корченко О.Г. Прикладні системи оцінювання ризиків інформаційної безпеки. Монографія/ О.Г. Корченко, С.В. Казмірчук, Б.Б. Ахметов, Київ, ЦП «Компринт», 2017 – 435 с. URL http://er.nau.edu.ua/handle/NAU/40482 (дата звернення: 14.12.2023)

4. Кочетков О.В. Система оцінки ризиків інформаційної безпеки підприємства на основі нечіткої логіки. / О.В. Кочетков, Т.О. Гаур, В.М. Машін // Наукові праці ОНАЗ ім. О.С. Попова, 2019, № 1. – С. 97-104.

5. Субботін С. О. Подання й обробка знань у системах штучного інтелекту та підтримки прийняття рішень : навчальний посібник. – Запоріжжя: ЗНТУ, 2008. – 341 с.

6. Асєєва Л.А. Оцінка ризиків конфіденційності інформаційної безпеки проектів на основі нечіткої логіки/ Л.А. Асєєва, О.М. Шушура //Телекомунікаційні та інформаційні технології. 2021. № 1 (70). – С. 88-95.

7. Сальник В.В. Методика оцінки порушень захищеності інформаційних ресурсів в інформаційно-телекомунікаційних системах / В.В. Сальник, О.А. Гуж, В.С. Закусіло, С.В. Сальник, П.В. Бєляєв // Збірник наукових праць Харківського національного університету Повітряних Сил, № 4(70), 2021. – С. 77-82.

8. Гарасим Ю. Р. Аналіз процесу управління ризиками інформаційної безпеки в процесі забезпечення властивості живучості систем / Ю. Р. Гарасим, В. А. Ромака, М. М. Рибій // Вісник Національного університету "Львівська політехніка". Сер. : Автоматика, вимірювання та керування. – 2013. - № 753. – С. 90-99.

9. Методичні вказівки до виконання лабораторних робіт з дисципліни "Нечітке програмування" “Програмне забезпечення систем” усіх форм навчання / Уклад.: С.О. Субботін. – Запоріжжя: ЗНТУ, 2013. – 50 с.

Додаткова література з навчальної дисципліни

10. Потій О. Аналіз методів оцінки та управління кіберризиками та інформаційною безпекою./ О. Потій, Ю. Горбенко, О. Замула, К. Ісірова // *Радіотехніка*. – 2021 - № 3 (206). С. 5-24. https://doi.org/10.30837/rt.2021.3.206.01.

11. Ю. Лісовська. Книга Кібербезпека. Ризики та заходи. – Вид-во «Кондор», 2019. – 272 с.

12. Гуменюк В. Я. Управління ризиками : навч. посіб. / В. Я. Гуменюк, Г. Ю. Міщук, О. О. Олійник. – Рівне : НУВГП. - 2009. 156 с.

13. Машина Н.І. Ризик і методи його вимірювання: Навчальний посібник. - К.: ЦНЛ, 2003. - 188 с.

14. Василевич Л.Ф. Юртин І.І. Прийняття рішень за умов конфлікту та невизначеності середовища. Навчальний посібник – К. : Київ. ун-т ім.. Б. Грінченка. 2013. 128 с.

Інформаційні ресурси в Інтернеті:

15. Національна база даних вразливостей. https://nvd.nist.gov/ (дата звернення: 14.12.2023).

16. Програмне забезпечення для проведення оцінки ризиків http://secinsight.blogspot.com/2012/01/blog-post.html (дата звернення: 14.12.2023).

Управління ризиками https://stud.com.ua/179792/informatika/upravlinnya_rizikami_model_bezpeki_povnogo_perekrittya (дата звернення: 14.12.2023)