КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних систем та технологій

«ЗАТВЕРДЖУЮ»
Заступник декана з навчально-виховної роботи
_____ Наталія ТМЄНОВА
«____» _____2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРНЕТИЧНА БЕЗПЕКА ПІДПРИЄМСТВА

для студентів

галузь знань	**12 Інформаційні технології**
спеціальність	**126 Інформаційні системи та технології**
освітній рівень	**бакалавр**
освітня програма	**«Програмні технології інтернет речей»**
вид дисципліни	**обов'язкова**
Форма навчання	**денна**

Навчальний рік	**2024/2025**
Семестр	**7**
Кількість кредитів ECTS	**5**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладач: Борисенко Ірина Ігорівна, к.т.н.

Пролонговано: на 2025/2026 н.р. _____ (Ожружний) «25» 06 2025 р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____) «__»___ 20__р.
(підпис, ПІБ, дата)

КИЇВ – 2024

Розробник: Борисенко Ірина Ігорівна, к.т.н., доцент кафедри інформаційних систем та технологій

ЗАТВЕРДЖЕНО
«____» _____ 20___ р.

Завідувач кафедри інформаційних систем та технологій

_____ д.т.н., професор Володимир ДРУЖИНІН

Протокол № 20_23/24 від 27 червня 2024 року

Схвалено науково - методичною комісією факультету інформаційних технологій

Протокол №9 від «27» ___червня___ 2024 року

Голова науково-методичної комісії ФІТ _____ (Ганна КРАСОВСЬКА)

Програму перевірено

«_____» _____ 20___ року

ВСТУП

Мета дисципліни «Кібернетична безпека підприємства» – ознайомлення з основними підходами, принципами та методами організації кібернетичного захисту підприємства; набуття практичних павичок щодо створення та підтримки реальної системи кібернетичного захисту ;формування у студентів активної позиції, спрямованої на практичну реалізацію важливого завдання – захист інформації в державі..

2. Попередні вимоги до опанування або вибору навчальної дисципліни (*за наявності*):
Успішне опанування дисциплін:

- «Побудова, безпека і автоматизація корпоративних мереж»;
- «Організація баз даних»;
- «Основи інформаційної безпеки»;
- «Розподілені системи збору інформації».

3. Анотація навчальної дисципліни:

В сучасному підприємстві, створення, зберігання та авторизована передача інформації відіграють важливу роль. Переважна кількість інформації циркулює в кібернетичному просторі, тому забезпечення цілісності, доступності та конфіденційності інформації набуває надзвичайної важливості. Дисципліна присвячена вивченню підходів, методів, принципів та отриманню практичних навичок організації кібернетичного захисту інформації на підприємстві для підготовки студентів до належного виконання своїх посадових обов'язків в компаніях , підприємствах та інститутах телекомунікаційного та інформаційного сектору держави.

4. Завдання (навчальні цілі):
Дисципліна спрямована на формування:
здатності до абстрактного мислення, аналізу та синтезу, а також застосування знань у практичних ситуаціях; здатності застосовувати, впроваджувати та експлуатувати сучасні системи кібернетичного захисту інформації на підприємстві; здатності до аналізу можливих загроз інформації на підприємстві, визначення характеристик порушника безпеки та визначення протидій загрозам; здатності створювати комплексну систему кібернетичного захисту інформації на підприємстві з застосуванням підходів та методів системного аналізу, планування технологічних процесів та проектування складних систем; навичок використання інформаційних і комунікаційних технологій..

5. Результати навчання за дисципліною:

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання (за необхідності)	Відсоток у підсумковій оцінці з дисципліни
Код	**Результат навчання**			
1	*2*	*3*	*4*	*5*
1.1	Знати аспекти захисту інформації та критерії оцінки інформаційної безпеки.	лекція	Тест, 60% правильних відповідей. Результат проходження курсу академії CyberOps Associate.	4%
1.2	Знати основні вітчизняні нормативні документи в галузі захисту інформації та міжнародні стандарти з інформаційної безпеки, процеси які визначаються ними при побудові кібернетичних систем захисту інформації.			4%
1.3	Знати принципи побудови сучасних систем забезпечення інформаційної безпеки.			4%
1.4	Знати основні типи, призначення та характеристики технологічних рішень направлених на забезпечення інформаційної безпеки.			4%
1.5	Знати загальні методології організаційного забезпечення інформаційної безпеки на рівні великих постачальників інформаційних систем..			4%
1.6	Знати основи реагування на інциденти інформаційної безпеки.			4%
1.7	Знати формування політики інформаційної безпеки на підприємстві.			4%
2.1	Вміти розробити та визначити загальні принципи побудови систем інформаційної та кібернетичної безпеки сучасного підприємства, завдання, вихідні дані та фактори, які необхідно врахувати при проектуванні інфраструктури.	Практична робота	Звіт з практичної роботи. Модульні контрольні роботи	5%
2.2	Вміти працювати з сучасними систем забезпечення інформаційної безпеки.			5%
2.3	Вміти здійснити аналіз та оцінку параметрів інформаційної та кібернетичної безпеки сучасного підприємства.			5%
2.4	Вміти здійснити аналіз та формування політики безпеки елементів систем інформаційної та кібернетичної безпеки сучасного підприємства: визначити основні складові політики безпеки, розробити систему документів, що забезпечують реалізацію політики безпеки, визначити гарантії правильності реалізації політики безпеки та її забезпечення..			5%
2.5	Вміти здійснити формування базових положень політики безпеки, розробити правила забезпечення інформаційної та кібербезпеки.			5%

2.6	Вміти здійснити оцінку ефективності функціонування систем захисту елементів інформаційної та кібернетичної безпеки сучасного підприємства.			5%
2.7	Вміти застосувати національні та міжнародні стандарти для аналізу та розробки систем інформаційної та кібернетичної безпеки сучасного підприємства та (або) її елементів.			5%
2.8	Вміти оцінити ефективність впровадження перспективних засобів та систем захисту, технологій, що використовується при створенні систем інформаційної та кібернетичної безпеки сучасного підприємства.			5%
2.9	Вміти реалізовувати організаційні та технічні завдання, які виникають в процесі побудови систем інформаційної та кібернетичної безпеки сучасного підприємства.			5%
2.10	Вміти застосовувати сучасні технології для забезпечення кібернетичної безпеки підприємства.			5%
3.1	*Комунікації:* вироблення у студентів практичних навиків командної роботи та здійснення публічних доповідей.	Лекції, практичні заняття, самостійна робота	Захист практичних робіт. Тест, 60% правильних відповідей	11%
3.2	Використання навиків обробки даних, пов’язаних з захистом інформації при колективному вирішенні задач. Використання сучасних інформаційних систем та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків.	Самостійна робота	Тест, 60% правильних відповідей. Результат проходження курсу академії CyberOps Associate.	11%

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Програмні результати навчання (назва) \ Результати навчання дисципліни (код)	1.1	1.2	1.3	1.4	1.5	1.6	2.1	2.2	2.3	2.4	2.5	2.6	3.1
ПР 2. Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій.	+	+	+	+	+	+	+	+	+	+	+	+	+
ПР 4. Проводити системний аналіз об'єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях.							+	+	+	+	+	+	+
ПР 10. Розуміти і враховувати соціальні, екологічні, етичні, економічні аспекти, вимоги охорони праці, виробничої санітарії, пожежної безпеки та існуючих державних і закордонних стандартів під час формування технічних завдань та рішень..	+	+											
ПР 19. Використовувати можливості апаратного забезпечення, використовувати можливості операційних систем, використовувати можливості мережевих програмних систем, забезпечувати захищеність програм і даних від несанкціонованих дій.												+	

7.1 Схема формування оцінки.

7.1 Форми оцінювання: рівень досягнення усіх запланованих результатів навчання визначається за результатами вивчення лекційного матеріалу (додатково розміщених відеолекцій в Teams), проміжного тестування за темами в системі Cisco, захисту результатів практичних робіт. А також, підсумкового тестування з використанням фінального іспиту від Cisco.

Питома вага результатів навчання у підсумковій оцінці за умови її опанування на належному рівні така:

- результати навчання 1-(знання) РН 1.1., РН 1.2., РН 1.3., РН 1.4., РН 1.5., РН 1.6. - до 30% ;
- результати навчання 2-(вміння) РН 2.1., РН 2.2., РН 2.3., РН 2.4., РН 2.5., РН 2.6. - до 51% ;
- результати навчання 3-(комунікація) РН 3.1. - до 19%.

7.2 Організація оцінювання.

Семестрове оцінювання: ***100 балів (100%)***

Оцінка за семестр формується шляхом успішного виконання та захисту практичних робіт, успішного проходження проміжного тестування за темами курсу «CyberOps Associate» Cisco.

Обов'язковим для проміжного контролю є виконання та захист практичних робіт, передбачених робочою програмою навчальної дисципліни у визначені терміни.

Поточне оцінювання проводиться у формі опитування студентів за темами попередніх лекцій, темами практичних робіт чи темами домашнього завдання, проміжних тестувань за темами курсу «CyberOps Associate» Cisco.

Студенти виконують 4 практичних роботи, що оцінюються від 5 до 8 балів за роботу (сумарна кількість балів від 20 до 32 балів . За виконання та захист робіт у прострочені строки оцінка знижується на 1-2 бали. За один раз можна захищати не більше 2 робіт.

Проміжне тестування оцінюється від 8 до 16 балів за успішне виконання тестів (з балом більше 80%) за темами 6 розділів курсу «CyberOps Associate» Cisco. Якщо проміжне тестування не пройдено, то бали не нараховуються і студент не допускається до сертифікації. Загальна сума за семестр від 48 до 80 балів.

У випадку відсутності студента з поважних причин відпрацювання та перездачі здійснюються у відповідності до «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу» від 1 жовтня 2010 року.

Для студентів, які набрали сумарно меншу кількість балів ніж критично-розрахунковий мінімум (48 балів), для допуску до заліку не допускаються. Обов'язковими є виконання та захист запланованих індивідуальних практичних робіт та проміжного тестування на бали від 60%.

Підсумкове оцінювання *у* формі заліку: складає *20 модульних балів (20% від загального рейтингу).*

На останньому занятті проводиться залікова робота у формі тестування сформованого системою навчання академії Cisco курсу «CyberOps Associate». Фінальні бали тесту, представлені у 100 бальній системі перераховуються у співвідношенні 1:5 та додаються до сумарної кількості балів за семестр. При успішному складанні тесту більше 80 балів студенти додатково отримують сертифікат на 120 годин за курсом «CyberOps Associate» Cisco.

Оцінка за залік не може бути меншою 12 балів для отримання позитивної оцінки за предмет.

Підсумкова оцінка визначається шляхом підсумовування балів семестрової роботи та залікового тестування. Якщо у підсумку студент набрав більше 60 балів, йому ставиться оцінка «зараховано».

При простому розрахунку отримаємо:

	Практичні роботи	Проміжне тестування	Залікове тестування	Підсумкова оцінка
Мінімум	20	8	12	60
Максимум	32	80	20	100

7.3 Шкала відповідності оцінок

Зараховано / Passed	60-100
Не зараховано / Fail	0-59

8. Структура навчальної дисципліни. Тематичний план лекцій і практичних занять

№ п/п	Назва теми	Кількість годин			
		лекції	ПЗ	ЛЗ	С/Р
1	**Тема 1 Сутність, задачі і методологічні основи системи кібернетичного захисту та визначення складу інформації що захищається** Загальні відомості про курс Загальні відомості про кібернетичну безпеку та її місце у загальній економічній безпеці підприємства Методологічні основи комплексної системи кібернетичного захисту підприємства Технологічна побудова комплексної системи кібернетичного захисту	4	10		20
2	**Тема 2 Технологічне, кадрове та нормативно-методичне забезпечення системи кібернетичного захисту підприємства** Нормативно-методичне забезпечення системи кібернетичного захисту підприємства Управління системою кібернетичного захисту Управління комплексною системою кібернетичного захисту підприємства в умовах надзвичайних ситуацій Кадрове забезпечення комплексної системи кібернетичного захисту)	6	12		26
3	**Тема 3 Практичні аспекти захисту підприємства** Розробка організаційно-розпорядчої і нормативної документації щодо захисту інформації Розробка підсистем комплексної системи захисту інформації підприємства	7	10		28
	Тестування	1	2		22
	Всього за семестр	**18**	**34**		**96**

Загальний обсяг 120 год., в тому числі:

лекцій 18 год
практичних 34год

консультації 2 год
самостійна робота 96 год

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна: *(Базова)*

1. Курс Cisco академії «CyberOps Associate» URL: https://www.cisco.com/site/us/en/learn/training-certifications/certifications/cyberops/cyberops-associate/index.html (дата звертання 20.08.2024).
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Магнолія 2006., К. 2021. – 450 с.
3. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). – Київ : КПІ ім. Ігоря Сікорського, 2021. – 258 с.

Додаткова:

1. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації від несанкціонованого доступу
2. НД ТЗІ Класифікація автоматизованих систем і стандартні профілі захищеності опрацьованої інформації від несанкціонованого доступу.
3. Орлов П.І.. Інформація та інформатизація. – Харків: НУВС. - 2003.- 723с.

Інформаційні ресурси

1. CyberOps

https://www.cisco.com/site/us/en/learn/training-certifications/certifications/cyberops/cyberops-associate/index.html

2. Nmap: https://nmap.org/

Публікації викладача

1. Borysenko, I., Petrenko, K., Skorobogatova, N., Ivanova, T. (2024)./ Organizational mechanism of the system of monitoring and environmental control of dangerous goods transport // Conference proceedings of the VII International Scientific-Practical Conference "Information Technology for Education, Science and Technics" (ITEST-2024), (Cherkasy, May 23-24, 2024). Cherkasy: ChSTU, 2024. 349 p. - p. 90-91
2. Borysenko, I., Petrenko, K., Skorobogatova, N., Ivanova, T. (2024). Organisational Mechanism of the System of the Monitoring and Environmental Control for the Transport of Dangerous Goods. In: Faure, E., et al. Information Technology for Education, Science, and Technics. ITEST 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 221. Springer, Cham.