СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КЕРУВАННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Перший (бакалаврський)
Факультет	Інформаційних технологій і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	ОК-28 ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Василіу Євген Вікторович			
	Професор кафедри кібербезпеки та технічного захисту інформації		

Загальна інформація

Анотація	Дисципліна «Керування ризиками інформаційної безпеки» направлена на отримання студентами теоретичних знань в області керування ризиками інформаційної безпеки підприємства, а також практичних навичок , що дозволяють визначити та мінімізувати витрати на інформаційну безпеку
Мета дисципліни	– отримання студентами теоретичних знань в області керування ризиками інформаційної безпеки підприємства, а також практичних навичок, що дозволяють визначити та мінімізувати витрати на інформаційну безпеку ;
Компетентності, формуванню яких сприяє дисципліна	КЗ 1. Здатність застосовувати знання у практичних ситуаціях. КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.

	КЗ 7. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.КФ 34 КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.). КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності. 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	3 5 7 9 15 18 23-24 28 30 32 34 38 40 43 48-49 ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності. ПРН 5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат. ПРН 7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки. ПРН 9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та кібербезпеки. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 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). ПРН 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. ПРН 30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем. ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки. ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації. ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів,

	контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах. ПРН 49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
Обсяг дисципліни	Загальний обсяг дисципліни: 3 кредити ЄКТС (90 год.).
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається: у 8-му семестрі

Програма дисципліни

Тема 1.	**Розподіл обов'язків по управлінню безпекою. Підхід "зверху-вниз".**
Тема 2.	**Адміністрування безпеки і захисні заходи. Основні принципи безпеки. Визначення безпеки. Безпека через невідомості.**
Тема 3.	**Організаційна модель безпеки. Компоненти програми безпеки. Стандарти безпеки. Управління безпекою на стратегічному рівні.**
Тема 4.	**Управління інформаційними ризиками. Компетенції в управлінні ризиками. Політика управління інформаційними ризиками. Група управління ризиками (IRM-група).**
Тема 5.	**Аналіз ризиків. Група аналізу ризиків. Цінність інформації та активів. Визначення вартості та цінності. Ідентифікація загроз. Аналіз збоїв та дефектів. Кількісний аналіз ризиків. Якісний аналіз ризиків. Вибір кількісного або якісного аналізу. Захисні механізми. Дії спрямовані на проведення аналізу ризиків. Загальний ризик і залишковий ризик. Обробка ризику.**
Тема 6.	**Політика безпеки. Стандарти. Базиси. Методичні вказівки. Процедури. Впровадження.**
Тема 7.	**Класифікація інформації. Управління класифікованими даними.**
Тема 8.	**Рівні відповідальності. Рада директорів. Вище виконавче керівництво. Власник даних. Відповідальний за зберігання даних. Власник системи. Адміністратор безпеки. Аналітик з безпеки. Власник додатку. Супервізор. Аналітик управління змінами. Аналітик даних. Власник процесу. Постачальник рішення. Користувач. Менеджер з технологій. Аудитор. Обґрунтованість великої кількості ролей.**

Тема 9.	**Персонал. Структура. Правила прийому на роботу. Контроль співробітників. Звільнення.**
Тема 10.	**Навчання (тренінги) з питань безпеки. Різні типи навчання (тренінги) з питань безпеки. Оцінка результатів навчання. Спеціалізоване навчання з безпеки.**

Список рекомендованих джерел

1. 1. Лахно В.А., Василіу Є.В., Гладких В.М., Домрачев В.М., Сивкова Н.М. Методи та засоби захисту інформації. Одеса, 2020. 445 с.
2. Богуш В. М., Юдін О. К. Інформаційна безпека держави. МК-Пресс, 2005. 432 с.
3. Богуш В. М., Кривуца В. Г., Кудін А. М. . Інформаційна безпека: Термінологічний навчальний довідник. Київ, 2004. 508 с.
4. Хорошко В.О., Чередниченко В.С., Шелест М.Є. Основи інформаційної безпеки. К. : ДУІКТ, 2008. 186 с.
5. Abhishek Chopra, Mukund Chaudhary. Implementing an Information Security Management System. Security Management Based on ISO 27001 Guidelines. Apress, 2020. 284 p.
6. Kuan-Ching Li, Xiaofeng Chen, Willy Susilo. Advances in Cyber Security: Principles,Techniques, and Applications. Springer Nature Singapore Pte Ltd., 2019. 270 p.
7. Nathan House. The Complete Cyber Security Course. Volume I. London: Published by StationX Ltd., 2017. 282 p.

Інформація про консультації

Щопонеділка у січні-червні 2023 року з 13^{00} до 14^{30} год., ауд. 108 або zoom

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нарахування балів**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** При оформленні документів за екзаменаційну сесію використовується таблиця відповідності оцінювання знань здобувачів вищої освіти за різними системами
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		

0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях, лабораторних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.

Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**