СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СИСТЕМА МЕНЕДЖМЕНТУ 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	Другого (магістерського) рівня
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-5** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Василіу Євген Вікторович

Професор кафедри «Кібербезпеки та технічного захисту інформації», доктор технічних наук, професор

Зайцева Любов Вадимівна

Викладач кафедри «Кібербезпеки та технічного захисту інформації»

Анотація до дисципліни	Предметом вивчення навчальної дисципліни є - вивчення навчальної дисципліни є стратегічні та тактичні принципи побудови систем менеджменту інформаційної безпеки та вивчення міжнародних стандартів, а також особливостей їх використання.
Мета дисципліни	формування основ знань щодо принципів побудови, аналізу та оптимізації систем менеджменту інформаційної безпеки
Компетентності, формуванню яких сприяє дисципліна	КІ-1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. 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). 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 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 12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж. КФ 16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.

Результати навчання	РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі. РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки. РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення. РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки. РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. РН16. 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. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
Обсяг дисципліни	Загальний обсяг дисципліни: ECTS – 3, 90 год
Форма підсумкового контролю	Залік

Терміни викладання дисципліни	Дисципліна викладається у 2-му семестрі

Програма дисципліни

Тема 1.	Сучасний менеджмент Визначення функції менеджменту, типи менеджменту (горизонтальні та вертикальні, їх відмінності). Різниця між ефективністю та продуктивністю.
Тема 2.	Типи інформаційних систем Різні типі інформаційних систем і тенденції в сфері інформаційних технологіях. Забезпечення інформаційними системам поточних операцій і процесів прийняття рішення.
Тема 3.	Постановка цілей і організаційне планування. Цілі і плани організації, концепції міссій організації та їх вплив на планування. Стадії процесу управління. Стадії розробки планів та дій у кризисних ситуаціях.
Тема 4.	Формулювання та впровадження стратегії. Компоненти стрегічного менеджменту, Процес стратегічного планування та SWOT- аналіз, стратегії на різних рівнях та різних підходах. Формулювання функціональних стратегій та інструментарій і впровадження.
Тема 5.	Процес стратегічного менеджменту. Сили, які впливають на отраслеву конкуренцію, Характеристики організацій у відповідності конкурентним стратегіям, стратегія лідерства та партнерства, інформаційні та контролюючи системи.
Тема 6.	Впровадження та контроль над реалізованнимі стратегіямі. Варіанти впровадження та засоби контролю над реалізованими стратегіями, засоби контролю на необхідний для цього набір інструментів.
Тема 7.	Інтернет і е-бізнес. Ключові компоненти е-бізнесу, е-комерція, стратегії є-бізнеса, електронні ринки.

Список рекомендованих джерел

Information technology. Security techniques. Information security management systems. Requirements», ISO/IEC 27001:2013, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2013.

Jason Andress "The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice».

О.О. Цвілій, Безпека інформаційних технологій: сучасний стан стандартів ISO27K системи управління інформаційною безпекою, Телекомунікаційні та інформаційні технології., №2, с. 73-79, 2014.

Й.С. Завадський, Менеджмент: «Management», 2-е. вид., К.,Українсько-фінський інститут менеджменту і бізнесу, 1998.

Інформація про консультації

Щопонеділка у лютому-травні 2024 року, 16^{00}-17^{30}, конференція ZOOM

Загальна схема оцінювання

Сума балів за всі види навчальної діяльності	**Шкала ЄКТС**	**Оцінка за національною шкалою**		**Нараховуються бали**	**Бали нараховуються таким чином:**
		для іспиту	**для заліку**		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів вищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів, за результати екзамену – до 40 балів.
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	**а л і в**	
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.
Інші умови: Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням
https://e-learning.suitt.edu.ua/course/view.php?id=25