СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

МЕТОДОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕС/ОПЕРАЦІЙНИХ ПРОЦЕСІВ СУЧАСНИХ ПІДПРИЄМСТВ

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-9** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Стайкуца Сергій Володимирович
s.v_staikutsa@suitt.edu.ua

Доцент кафедри кібербезпеки та технічного захисту інформації (КБ та ТЗІ), кандидат філософських наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни	Предметом вивчення навчальної дисципліни бізнес-середовище сучасного підприємства в аспекті дії на його ключові процеси внутрішніх та зовнішніх загроз та ризиків. Розглядаються основні етапи побудови стратегії неперервності бізнесу, аналіз дії загроз та ризиків на бізнес, оцінка ризиків для бізнесу в екосистемі цілей, інструментів та технологій. Приділено увагу вивченню міжнародних стандартів забезпечення неперервності бізнесу як основи для розроблення корпоративних програм управління неперервністю бізнесу (ECP).

Мета дисципліни	– формування основ знань щодо побудови на підприємстві стратегії неперервності бізнесу (BCM), розуміння базових етапів, складових та компонентного складу, ресурсів та планів дій (ECP) тощо.
Компетентності, формуванню яких сприяє дисципліна	КІ-1. Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт. КЗ5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності). КФ5. 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. КФ7. 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. КФ15. Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки.
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. РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. 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. 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. РН24. Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредитів (ЄКТС 120 годин). Для денної форми навчання: лекції –20 години, практичні заняття –20 години.
Форма підсумкового контролю	Екзамен
Терміни викладання дисципліни	Дисципліна викладається у 2-му семестрі

Програма дисципліни	
Тема 1.	***Інформаційне поле сучасного підприємства.*** Структура, складові, зв'язки, загрози та ризики
Тема 2.	***Бізнес-процеси підприємства.*** Класифікація та структурно-ієрархічна модель. Життєві цикли корпорацій
Тема 3.	***Моделювання бізнес-процесів підприємства.*** Основні відомості, методи моделювання
Тема 4.	***Оптимізація бізнес-процесів підприємства.*** Суть, принципи та критерії. Методи оптимізації. Критерії оцінки.
Тема 5.	***Аналіз рішень щодо управління бізнес-процесами підприємства.*** Системи управління, програмні рішення, сервіси
Тема 6.	***Основні етапи забезпечення принципів неперервності бізнесу.*** Базові відомості щодо BCM. Основні етапи забезпечення принципів неперервності бізнесу
Тема 7.	***Міжнародні стандарти та практики BCM*** Рекомендації, склад, опис процесу управління ризиками
Тема 8.	***Корпоративна програма управління неперервністю бізнесу (ECP).*** Етапи, компонентний склад, пріоритети.
Тема 9.	***Забезпечення неперервності бізнесу в "нетипові" періоди.*** "Черні лебеді", пандемія COVID-19, війни
Тема 10.	***Експрес-аудит стану безпеки підприємства в фокусі впровадження BCM.*** Аудит стану безпеки підприємства, радар загроз, методи та засоби захисту

Список рекомендованих джерел

1. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання: монографія/ Довгий С.О., Воробієнко П.П., Гуляєв К.Д., за загальною редакцією члена-кореспондента НАН України Довгого С.О., Київ “АзимутУкраїна”, 607 ст., 2013 р.
2. Протоколи, термінальне обладнання та інформаційна безпека у мережах наступного покоління : [навч. посібник] / М. В. Захарченко, О. О. Вараксін, В. Г. Кононович, С. О. Вараксін ; за ред. М. В. Захарченка. – Одеса: Фенікс, 2008. – 128 с. – ISBN 978-066-438-140-3
3. Захарченко М.В. Інформаційна безпека. Захист інформації у комп’ютерах та комп’ютерних мережах : навч. пос. / М. В. Захарченко, В. Г. Кононович, В. Й. Кільдишев, Д. В. Голев // За ред. М. В. Захарченка. – Одеса: ОНАЗ, 2011. – 168 с. – ISBN 978-966-7598-60-0
4. Гладиш С. В. Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки / С. В. Гладиш, В. Г. Кононович, М. Ф. Тардаскін // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науковотехнічний збірник. – Вип. 2 (15), – К., 2007. – С 31 - 39.
5. Будущие сети: целевые установки и цели проектирования – Международный союз электросвязи, Y-3001 – Глобальная информационная инфраструктура, аспекты протокола интернет и сети последующих поколений.
6. Керування ризиками на підприємстві / CIDCON CONSULTING COMPANY. - Київ, 2012.
7. Мэри Пэт Маккарти, Тимоти П. Флинн. Риск: управление риском на уровне топ-менеджеров и советов директоров. Пер. с англ. – М.: Альпина Бизнес Букс, 2005. – 234.

Інформація про консультації

Щосереди у вересні-грудні 2023 року з 14.30 до 15.30 год., ауд. 250 або зум – доц. С.В. Стайкуца

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*** 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		
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.**