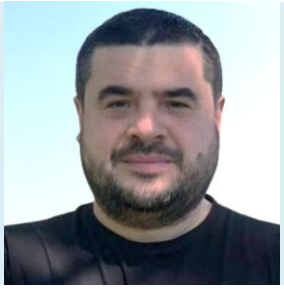
СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

НЕПЕРЕРВНІСТЬ БІЗНЕСУ ТА ВІДНОВЛЕННЯ ПІСЛЯ АВАРІЇ

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 та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-24** 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	КЗ 2. Знання та розуміння предметної області та розуміння професії. КЗ 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. КФ 3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження. 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 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	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 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності. 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 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки. ПРН 10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем. ПРН 11. Виконувати аналіз зв’язків між інформаційними процесами на віддалених обчислювальних системах. ПРН 12. Розробляти моделі загроз та порушника. ПРН 13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних. ПРН 14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень. ПРН 15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій. ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів. ПРН 17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент. ПРН 18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів. ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-

	телекомунікаційних. ПРН 20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах. ПРН 21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах. ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки. 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 31. Застосовувати теорії та методи захисту для забезпечення безпеки 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 33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків. ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки. ПРН 36. Виявляти небезпечні сигнали технічних засобів. ПРН 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації. 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 39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

	ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації. ПРН 41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур. ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки. ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів. ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами. ПРН 45. Застосовувати різні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів. ПРН 46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах. ПРН 47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації. 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: 4 кредитів (ЄКТС 120 годин). Для денної форми навчання: лекції –22 години, практичні заняття –44 години.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі

Програма дисципліни	
Тема 1.	***Загрози та ризики бізнесу в аспекті життєвих циклів корпорацій І.Адізеса.*** Щодо актуальності провадження принципів неперервності бізнесу (BCM).
Тема 2.	***Стру Основні етапи забезпечення принципів неперервності бізнесу.*** Ініціація проекту, аналіз дії на бізнес, оцінка ризиків, розробка стратегії, розробка та впровадження планів, тестування, обслуговування та оновлення планів.

Тема 3.	***Аналіз дії на бізнес (BIA).*** Місце в системі управління, ключові задачі, цінності, середовище ризиків, складові та ціна втрат. Реалізація, ключові та другорядні задачі, цінності, визначення та складові втрат.
Тема 4.	***Оцінка ризиків для бізнесу (RA).*** Цілі, інструменти, технології. Методи оцінювання та зниження ризиків.
Тема 5.	***Технології забезпечення BCM в IT.*** Класифікація IT-систем, вимоги до інфраструктури ЦОД, резервування, аналіз технологій. Вимоги до приміщень та інженерних систем.
Тема 6.	***Міжнародні практики BCM. BCI, DRI.*** Розгляд складу, напрямків діяльності, етапи планування дій в надзвичайних ситуаціях.
Тема 7.	***Вивчення міжнародних стандартів BCM.*** Британський стандарт BS25999. Дослідження основних етапів формування принципів BCM на основі стандарту BS25999.
Тема 8.	***Вивчення міжнародних стандартів BCM.*** Стандарти HB 292:2006, ISO 22301 та ISO 27002 Рекомендації, склад, опис процесу управління ризиками.
Тема 9.	***Вивчення міжнародних стандартів BCM.*** Стандарти COBIT, ITIL.
Тема 10.	***Корпоративна програма управління неперервністю бізнесу (ECP).*** Етапи, компонентний склад, пріоритети.
Тема 11.	***Адаптація принципів BCM та планів ECP до персонального та корпоративного середовища.*** Принципи Chaos Engineering.

Список рекомендованих джерел

1. Електронний комплект навчало-методичної документації курсу «Неперервність бізнесу та відновлення після аварії», Стайкуца С.В. ДУІТЗ, 2022 р.
2. Керування ризиками на підприємстві / CIDCON CONSULTING COMPANY. - Київ, 2012.
3. Стайкуца С. В. Аналіз ризиків корпоративного середовища з позиції міжнародних стандартів інформаційної безпеки / С. В. Стайкуца, С.О. Дігол, О.М. Бердніков, В.І. Верстаков // Сборник тезисов третьей всеукраинской научно-практической конференции "Перспективные направления защиты информации", ОНАС им. А.С.Попова. – 2017. – С. 68–72.
4. Кононович В.Г. Контури систем забезпечення кібербезпеки цифровізованого суспільства та кібернетизованого виробництва, бізнесу й управління / Кононович В.Г., Стайкуца С.В., Кононович І.В., Романюков М.Г. // Збірник тез VI-ї міжнародної науково-практичної конференції "перспективні напрями захисту інформації ", ОНАЗ ім. О.С. Попова. – 2020. – С. 70-76.
5. Стайкуца С. В. Актуальність впровадження принципів неперервності бізнесу в українських компаниях / С.В.Стайкуца, К.С. Сєдов, А.С. Гусак // «Современные тенденции развития науки» (м. Вінниця, 25-26 листопада 2022 р.). — Одеса : Видавництво «Молодий вчений», 2022. – С. 51-55.

6. Сім кроків до безперервності бізнесу [Електронний ресурс] // Блог компанії Softline. – 2015. – Режим доступу до ресурсу: https://habr.com/ru/company/softline/blog/261053
7. Барсуковська В. Безперервність бізнесу: новий тренд чи необхідність [Електронний ресурс] / Вікторія Барсуковська // Комп'ютерний огляд. – 2017. – Режим доступу до ресурсу: https://habr.com/ru/company/softline/blog/261053/
8. Управління неперервністю діяльності [Електронний ресурс] // Корпоративна презентація Deloitte. – 2020. – Режим доступу до ресурсу: https://www2.deloitte.com/content/dam/Deloitte/kz/Documents/risk/2%20%D0%B8%D1%8E%D0%BD%D1%8F.pdf.

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

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="10">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="9">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.</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

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.**