Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут *електронних та інформаційних технологій*
Кафедра *кібербезпеки та математичного моделювання*

СИЛАБУС
Забезпечення безперервності бізнесу

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М._____
(підпис) (прізвище та ініціали)

«__26___» __08__ 2024 р.

Розробник (-и): Мехед Дмитро Борисович, доцент КБММ, п.пед.н., доц._ _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання____
(назва кафедри)

Протокол від «__26___»____08_____2024р. №_7

Узгоджено з гарантом освітньої програми: _____ Ткач Ю.М._____
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*вибіркова*
Мова викладання	українська
Рік навчання та семестр	1 рік, 1 семестр 125 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Мехед Дмитро Борисович, доцент КБММ, к.пед.н., доц.
Профайл викладача (-ів)	Web: https://mmi.stu.cn.ua/personal-kafedry/ ORCID: 0000-0003-3905-3620
Контакти викладача	Чернігів, вул. Шевченка, 95, корп.1, каб. 108; E-mail: d.mekhed@stu.cn.ua

2. Анотація курсу. Курс «Забезпечення безперервності бізнесу» спрямований на формування у здобувачів знань та практичних навичок з організації, планування та підтримки стабільного функціонування підприємства в умовах ризиків, кризових ситуацій та надзвичайних подій. У межах курсу розглядаються ключові концепції та стандарти забезпечення безперервності бізнесу (Business Continuity Management, BCM), методології оцінки ризиків та впливу на діяльність, а також сучасні інструменти й практики розробки планів безперервності (BCP) та планів відновлення після збоїв (DRP).

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=4461&notifyeditingon=1

3. Мета та цілі курсу.

Метою дисципліни **«Забезпечення безперервності бізнесу»** є формування у студентів системного розуміння концепцій, методів та інструментів управління безперервністю діяльності організації в умовах надзвичайних ситуацій, криз та кіберзагроз. Студенти навчаться визначати критичні бізнес-процеси, оцінювати вплив ризиків на діяльність, розробляти та впроваджувати плани безперервності бізнесу (BCP) та плани відновлення після збоїв (DRP), а також застосовувати міжнародні стандарти для забезпечення стійкості організації.

Завдання курсу

- Ознайомлення з основними принципами та концепціями забезпечення безперервності бізнесу.
- Вивчення процесів і методів проведення аналізу впливу на бізнес (BIA) та оцінки ризиків.
- Визначення критичних ресурсів та бізнес-процесів організації.
- Ознайомлення з міжнародними стандартами та кращими практиками (ISO 22301, NIST тощо).
- Розробка стратегій реагування на кризові ситуації та відновлення після інцидентів.
- Формування практичних навичок складання та тестування планів BCP і DRP.
- Розвиток умінь організації навчання персоналу та управління кризовими комунікаціями.

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 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності)

КФ 5. 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

За результатами вивчення курсу студенти повинні:

Знати:

- Основні поняття та принципи забезпечення безперервності бізнесу (BCM).
- Етапи та методи проведення аналізу впливу на бізнес (Business Impact Analysis, BIA).
- Ключові підходи до розробки планів безперервності бізнесу (BCP) та відновлення після збоїв (DRP).

● Міжнародні стандарти та практики забезпечення безперервності (ISO 22301, NIST SP 800-34, ITIL).
● Особливості управління кризовими ситуаціями та організації кризових комунікацій.
● Методи оцінки ризиків для критичних бізнес-процесів та інформаційних ресурсів.
Вміти:
● Визначати критичні бізнес-процеси та ресурси організації.
● Проводити аналіз впливу на бізнес та оцінювати ризики для його безперервності.
● Розробляти та документувати плани BCP і DRP.
● Організовувати та проводити тестування планів безперервності й відновлення.
● Використовувати інструменти оцінки ризиків та моделювання кризових сценаріїв.
● Організовувати навчання персоналу та відпрацювання сценаріїв реагування.

Під час вивчення дисципліни ЗВО має досягти або вдосконалити наступні програмні результати навчання (ПРН), передбачені освітньою програмою:

ПРН 10 – Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

5. Пререквізити

Дисципліна є складовою частиною вибіркових дисциплін циклу професійної підготовки.
Вивчення курсу передбачає наявність систематичних та ґрунтовних знань із курсу:
ОК 4. Методологія та організація наукових досліджень.

6. Обсяг курсу

Загальний обсяг дисципліни – 4 кредити ЄКТС (120 годин), у тому числі:
лекційні заняття – 30 годин,
практичні (семінарські) заняття – 30 годин,
самостійна робота – 60 годин.

Вид заняття	Загальна кількість годин денне/заочне
Лекції	16/6
Практичні заняття	14/6
Самостійна робота	90/108
Індивідуальне завдання –	
Всього кредитів – *вказати кількість кредитів*	4

7. Тематика курсу

Змістовий модуль 1. Основи забезпечення безперервності бізнесу

Тема 1. Вступ до забезпечення безперервності бізнесу
Основні поняття та визначення (BCM, BCP, DRP). Історія розвитку та актуальність. Роль безперервності бізнесу в системі управління організацією.

Тема 2. Ключові елементи та принципи BCM
Життєвий цикл забезпечення безперервності бізнесу. Критичні бізнес-процеси та ресурси. Ролі та відповідальність персоналу.

Тема 3. Аналіз впливу на бізнес (BIA) Призначення та завдання BIA. Методи виявлення критичних процесів. Оцінка впливу збоїв на організацію.

Тема 4. Оцінка ризиків у забезпеченні безперервності Методи ідентифікації ризиків. Взаємозв'язок BIA і risk assessment. Кількісні та якісні підходи до оцінки загроз і вразливостей.

Змістовий модуль 2. Стратегії та плани забезпечення безперервності бізнесу

Тема 5. Міжнародні стандарти та кращі практики Огляд ISO 22301, NIST SP 800-34, ITIL, COBIT. Принципи ризик-орієнтованого підходу. Використання міжнародних стандартів у практиці організацій.

Тема 6. Розробка плану безперервності бізнесу (BCP) Структура та зміст BCP. Визначення сценаріїв надзвичайних ситуацій. Розробка стратегій підтримки критичних процесів.

Тема 7. План відновлення після збоїв (DRP) Особливості DRP для IT-інфраструктури та бізнес-процесів. Методи резервного копіювання та відновлення. Вибір технологій і підходів.

Тема 8. Тестування, навчання персоналу та вдосконалення планів Види тестування планів BCP/DRP. Організація навчання та тренінгів. Постійне вдосконалення системи BCM та кризові комунікації.

8. Система оцінювання та вимоги .

Загальна система оцінювання курсу	● Оцінювання курсу відбувається за 100 бальною шкалою. Протягом семестру здобувач вищої освіти може набрати 60 балів: практичні/лабораторні оцінюється в 20/10 балів, відповіді – 8/18 балів, іспит – 40 балів. Допоміжні бали виставляються за виконання макетів, виступи на конференціях, написання тез та статей.
Вимоги до РГР, КР, КП тощо	● Виконання модульних контрольних робіт ● Щонайменше за результатами контролю протягом семестру ЗВО повинен одержати 40 балів
Практичні (лабораторні) заняття	Модуль за тематичним планом дисципліни та форма контролю: ● Кількість балів - 0…60: ● 1. Виконання практичних/лабораторних робіт 0…20/10 ● 2. Модульне контрольне завдання 0…8/18 ● 3. Повнота відповідей на запитання на лекціях 0…2
Умови допуску до підсумкового контролю	● Оцінювання курсу відбувається за 100 бальною шкалою. Протягом семестру здобувач вищої освіти може набрати 60 балів: практичні/лабораторні

	оцінюється в 20/10 балів, відповіді – 8/18 балів, іспит – 40 балів. Допоміжні бали виставляються за виконання макетів, виступи на конференціях, написання тез та статей.

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1.		
1	Повнота відповідей на запитання на лекціях	0…2
2	Результати захисту лабораторних/практичних робіт	0…20/10
3	Самостійна робота	0…8/18
Змістовий модуль 2.		
1	Повнота відповідей на запитання на лекціях	0…2
2	Результати захисту лабораторних/практичних робіт	0…20/10
3	Самостійна робота	0…8/18
Усього поточний і проміжний модульний контроль		**0…60**
Семестровий контроль (Екзамен/диференційований залік/залік)		**0…40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення (за необхідності**).**

10. Політики курсу. У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка"». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у

відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базова література:

1. **ISO 22301:2019** – Security and resilience – Business continuity management systems – Requirements.
2. **ISO/TS 22317:2021** – Guidelines for business impact analysis (BIA).
3. **Wallace, M., Webber, L.** The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets – AMACOM, 2022.
4. **Herbane, B.** Business Continuity and Crisis Management: Planning for the Unthinkable – Routledge, 2023.
5. **Hiles, A.** The Definitive Handbook of Business Continuity Management – Wiley, 2022.
6. **Snedaker, S., Rima, C.** Business Continuity and Disaster Recovery Planning for IT Professionals – Sybex, 2023.
7. **Elliott, D., Swartz, E., Herbane, B.** Business Continuity Management: A Crisis Management Approach – Routledge, 2022.
8. **Cerullo, V., Cerullo, M.** Disaster Recovery Planning: Ensuring Business Continuity – Wiley, 2021.
9. **Paton, D., Johnston, D.** Disaster Resilience: An Integrated Approach – Charles C Thomas Publisher, 2022.
10. **National Institute of Standards and Technology (NIST) SP 800-34 Rev. 1** – Contingency Planning Guide for Federal Information Systems, 2022.

Допоміжна література:

1. **ISO/IEC 31000:2023** – Risk management – Guidelines.
2. **British Standards Institution (BSI)** – BS 25999 Business Continuity Management Standard.
3. **International Federation of Red Cross and Red Crescent Societies (IFRC)** – Business Continuity Planning Guide, 2023.
4. **Smith, D.** Business Continuity and Risk Management: Essentials of Organizational Resilience – Rothstein Publishing, 2023.
5. **Goh, S.** Organisational Resilience: Business Continuity, Crisis Management and Disaster Recovery – Springer, 2022.
6. **ENISA** – Business Continuity Planning for Critical Infrastructure, 2023.
7. **World Economic Forum** – Global Risks Report, 2024.
8. **PwC** – Building Resilient Organizations: Business Continuity in a Changing World, 2023.
9. **IBM Resiliency Services** – Cyber Resilience Report, 2023.
10. **European Union Agency for Cybersecurity (ENISA)** – Threat Landscape Report, 2023.

Інформаційні ресурси:

1. http://www.library.snu.edu.ua/ – Наукова бібліотека.
2. https://nlu.org.ua/ – Національна бібліотека України імені Ярослава Мудрого.
3. https://www.researchgate.net/ – науковий портал.
4. http://www.nbuv.gov.ua/ – Національна бібліотека ім. В.І. Вернадського.