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

РОБОЧА ПРОГРАМА
Забезпечення безперервності бізнесу

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

«26» серпня 2025 р.

Розробник (-и): Мехед Д.Б., доцент, кандидат педагогічних наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26» серпня 2025 р. № 6

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	2025-2026 навчальний рік, І семестр, ОП Кібербезпека за спеціальністю F5 Кібербезпека та захист інформації галузь знань F Інформаційні технології
Викладач (-і)	Мехед Дмитро Борисович, доцент кафедри кібербезпеки та математичного моделювання, кандидат педагогічних наук.
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	Т.м. +38(063) 690-80-00, E-mail: d.mekhed@stu.cn.ua

2. Анотація курсу.

Дисципліна "Забезпечення безперервності бізнесу" є частиною програми підготовки магістрів за спеціальністю "Кібербезпека та захист інформації" (F05) в галузі знань "Інформаційні технології". Курс забезпечує студентів знаннями та навичками з розробки та впровадження стратегій для забезпечення безперервності бізнесу (BCP) та відновлення після катастроф (DRP). Основна увага приділяється виявленню критичних бізнес-процесів, розробці планів їх підтримки, впровадженню ефективних інструментів для моніторингу ризиків і реагування на надзвичайні ситуації.

3. Мета та цілі курсу.

Мета курсу: Формування в студентів системного розуміння концепцій та методів забезпечення безперервності бізнесу, розробки планів відновлення та мінімізації ризиків, а також здатність до їх впровадження та оцінки ефективності.

Цілі курсу:

- Розуміння основних принципів забезпечення безперервності бізнесу та планування відновлення після катастроф.
- Розробка та оптимізація планів безперервності для різних бізнес-процесів.
- Вивчення технологій і засобів для моніторингу ризиків, зниження потенційних загроз і підвищення стійкості організацій до кризових ситуацій.
- Розробка практичних рекомендацій для створення інфраструктури, здатної забезпечити безперервну роботу бізнесу навіть в умовах аварій чи зовнішніх загроз.

4. Результати навчання:

Після завершення курсу студент має:

- Знати методи та стратегії для забезпечення безперервності бізнесу, включаючи оцінку та ідентифікацію критичних процесів.
- Вміти розробляти плани відновлення після катастроф, забезпечувати тестування та вдосконалення таких планів.
- Оцінювати потенційні ризики для бізнесу та вживати необхідних заходів для зниження їх впливу на роботу організації.
- Вміти використовувати спеціалізовані інструменти для моніторингу та управління безперервністю бізнесу.

ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН 4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.

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.

ПРН 14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.

5. Пререквізити. Відсутні.

6. Обсяг курсу:

Вид заняття	Загальна кількість годин
Лекції	16/6

Лабораторні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахунково-графічна робота	
Всього кредитів	4

Лекційні, семінарські заняття, розрахунково-графічна робота, самостійна робота – з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16 годин):

Вступ до забезпечення безперервності бізнесу (2 год)

Основні поняття та принципи забезпечення безперервності бізнесу.Важливість та роль планування безперервності бізнесу в сучасному світі.Визначення ключових компонентів стратегій безперервності бізнесу.

Аналіз ризиків та визначення критичних бізнес-процесів (2 год)

Оцінка та ідентифікація ризиків для організації.Методи аналізу ризиків: аналіз загроз та уразливостей.Визначення критичних бізнес-процесів для забезпечення безперервності.

Розробка плану безперервності бізнесу (BCP) (4 год)

Структура та етапи розробки плану безперервності бізнесу.Ключові елементи плану: аналіз потреб, стратегія відновлення, заходи для підтримки.Розробка плану кризових комунікацій та координації дій під час надзвичайних ситуацій.

Плани відновлення після катастроф (DRP) (3 год)

Визначення цілей і завдань плану відновлення після катастроф.Основні етапи відновлення інфраструктури, даних і ключових бізнес-процесів.Інструменти для реалізації DRP: резервне копіювання, відновлення даних, відновлення доступу до критичних систем.

Методи та інструменти моніторингу ризиків і загроз для бізнесу (2 год)

Використання спеціалізованих інструментів для моніторингу ризиків і загроз. Як здійснюється безперервний моніторинг бізнес-процесів.Впровадження ефективних методів реагування на виявлені ризики.

Тестування та вдосконалення планів безперервності бізнесу (3 год)

Практичні методи тестування планів відновлення після катастроф.Підготовка до кризових ситуацій: навчання персоналу, проведення тренувань та симуляцій.Оцінка ефективності та постійне вдосконалення планів безперервності бізнесу.

Семінарські (16 годин):

Огляд основних принципів забезпечення безперервності бізнесу (2 год)

Обговорення ключових понять та принципів забезпечення безперервності бізнесу.Визначення цілей та завдань дисципліни для конкретних організацій.Аналіз важливості безперервності бізнесу для ефективного управління підприємством.

Ідентифікація та оцінка ризиків для організації (3 год)

Практичне виконання аналізу ризиків на прикладі реальної організації.Визначення потенційних загроз та вразливостей для бізнес-процесів.Розгляд методів та інструментів оцінки ризиків, застосування їх для визначення критичних бізнес-процесів.

Розробка та вдосконалення плану безперервності бізнесу (4 год)

Створення проекту плану безперервності бізнесу для конкретної організації.Розгляд різних стратегій та підходів до відновлення бізнесу.Групова робота: розробка основних елементів плану (перелік критичних бізнес-процесів, план дій у надзвичайних ситуаціях).

Планування та тестування відновлення після катастроф (4 год)

Визначення ключових етапів плану відновлення після катастроф.Створення та тестування плану відновлення для конкретних випадків (наприклад, втрата даних або природна катастрофа).Обговорення методів та інструментів відновлення та збереження даних після катастроф.

Кризове управління та комунікація під час надзвичайних ситуацій (3 год)

Розробка ефективної стратегії комунікації в умовах кризи.Розгляд прикладів з реального життя щодо управління комунікацією в надзвичайних ситуаціях.Обговорення важливості чітких комунікацій між командами та вищим керівництвом під час відновлення бізнесу.

Підготовка до тестування та вдосконалення планів безперервності (3 год)

Аналіз методів тестування планів безперервності та відновлення.Проведення симуляцій та обговорення результатів тестування на прикладах.Визначення напрямків для вдосконалення існуючих планів безперервності бізнесу на основі тестів.

Розрахунково-графічна робота (РГР)

Тема: Аналіз безперервності бізнес-процесів та відновлення після катастроф

Аналіз критичних бізнес-процесів

- Визначення та ідентифікація критичних бізнес-процесів організації.
- Аналіз впливу різних загроз на безперервність діяльності організації.

Оцінка ризиків та вразливостей

- Проведення оцінки ризиків для бізнес-процесів.
- Визначення вразливостей у планах відновлення та їх усунення.

Розробка плану відновлення після катастроф

- Створення плану відновлення після катастрофи для критичних бізнес-процесів.
- Визначення методів та інструментів для мінімізації простоїв після надзвичайних ситуацій.

Тестування плану відновлення бізнесу

- Проведення тестів на відновлення бізнесу та оцінка їх ефективності.
- Аналіз результатів тестування та внесення коректив у план відновлення.

Аналіз кризових ситуацій та управління комунікацією

- Оцінка кризових ситуацій на основі сценаріїв реальних катастроф.

- ➢ Визначення основних принципів управління комунікацією під час кризових ситуацій для забезпечення безперервності бізнесу.

Самостійна робота (88 годин):

Аналіз та ідентифікація критичних бізнес-процесів (20 годин)

- Ознайомлення з методами ідентифікації критичних бізнес-процесів.
- Виконання завдання з аналізу бізнес-процесів в організації.
- Оцінка потенційного впливу їх переривання на організацію.

Оцінка ризиків для безперервності бізнесу (20 годин)

- Самостійне дослідження різних типів ризиків для організацій (наприклад, природні катастрофи, кіберзагрози, технічні збої).
- Розробка та заповнення матриці ризиків.
- Прогнозування можливих наслідків для бізнесу та оцінка вразливих місць в організаційних процесах.

Розробка стратегії відновлення після катастрофи (20 годин)

- Самостійне вивчення методів розробки планів відновлення.
- Створення власного плану відновлення для конкретної організації, враховуючи різні сценарії катастроф.
- Оцінка необхідних ресурсів для відновлення роботи бізнесу.

Тестування плану відновлення бізнесу (15 годин)

- Ознайомлення з практиками тестування планів відновлення.
- Проведення симуляції на основі створеного плану.
- Оцінка результатів тестування та формулювання пропозицій щодо вдосконалення плану.

Оцінка ефективності заходів щодо безперервності бізнесу (13 годин)

- Дослідження існуючих кейсів відновлення бізнесу в реальних компаніях.
- Оцінка їх ефективності та виявлення потенційних недоліків.
- Самостійний аналіз того, як можна удосконалити процеси в організації.

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 40 балів, **проміжний модульний контроль** – 10 балів, **виконання індивідуального завдання (РГР)** – 10 балів **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.

Вимоги до РГР, КР, КП тощо	**Критерії оцінювання РГР:** 1) відповідність завдання вимогам курсу – **2 балів;** 2) обґрунтування вибору стандартів та методів захисту – **2 балів;** 3) якість аналізу ризиків та оцінка відповідності – **2 балів;** 4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;** 5) своєчасність здачі роботи – **2 бали.**
Практичні заняття	Оцінка кожного практичного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **3 бали;** 2) аналіз отриманих результатів – **1 бал**; 3) належне оформлення звіту – **1 бал.**
Умови допуску до підсумкового контролю	1. Виконання та захист **не менше 50% практичних робіт** (щонайменше 4 із 8). 2. Проходження проміжного модульного контролю. 3. Виконання **розрахунково-графічної роботи** (РГР).

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1. Оцінка ризиків та планування безперервності бізнесу		**30**
1	Оцінка та ідентифікація критичних бізнес-процесів.	**5**
2	Аналіз ризиків і визначення уразливих місць.	**5**
3	Розробка стратегій та планів відновлення після катастроф.	**5**
4	Визначення критичних ресурсів для безперервності бізнесу.	**15**
Змістовий модуль 2. Тестування, підтримка та вдосконалення планів безперервності бізнесу		**30**
1	Проведення тестування планів відновлення.	**5**
2	Оцінка ефективності реалізації планів безперервності бізнесу.	**15**
3	Вдосконалення заходів для забезпечення безперервності бізнесу на основі тестування.	**5**
4	Управління кризовими ситуаціями та оперативне реагування на загрози для безперервності бізнесу.	**5**
Усього поточний і проміжний модульний контроль		**60**
Семестровий контроль (Диференційований залік)		**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.

При вивченні курсу використовується наступне **обладнання та програмне забезпечення**:

І. Апартне забезпечення:

Персональні комп'ютери або ноутбуки з підтримкою віртуалізації та можливістю роботи з образами дисків та цифровими доказами.

Операційні системи: Windows 10/11 Pro, Linux (Ubuntu, Kali Linux – для аналізу вразливостей), macOS.

Серверне обладнання для моделювання атак, аналізу мережевого трафіку та логів.

Мережеве обладнання (маршрутизатори, комутатори, мережеві екрани) для дослідження атак та аналізу цифрових слідів.

Зовнішні накопичувачі (HDD, SSD, USB-флешки) для роботи з криміналістичними копіями та створення дампів пам'яті.

Мобільні пристрої (Android, iOS) для дослідження мобільної криміналістики.

ІІ. Програмне забезпечення:

1. Для збору та збереження цифрових доказів:

FTK Imager – створення криміналістичних копій дисків.

Autopsy, Sleuth Kit – аналіз файлових систем та структури дисків.

Guymager – криміналістичне копіювання дисків у Linux.

2. Для аналізу файлових систем та метаданих:

X-Ways Forensics – глибокий аналіз файлових систем, відновлення даних.

ExifTool – витягнення метаданих із файлів (зображень, документів, відео).

Bulk Extractor – автоматичний пошук артефактів у файлах (номери кредитних карт, паролі).

3. Для дослідження операційних систем та лог-файлів:

Registry Explorer – аналіз реєстру Windows.

Event Log Explorer – дослідження журналів подій Windows.

Plaso, Timesketch – створення хронологій подій на основі логів системи.

4. Для мережевої криміналістики та аналізу трафіку:

Wireshark – аналіз мережевого трафіку.

Zeek (Bro IDS) – моніторинг і розслідування мережевих атак.

NetworkMiner – вилучення артефактів із трафіку.

5. Для криміналістики мобільних пристроїв:

MOBILedit Forensic – вилучення даних із мобільних пристроїв.

Oxygen Forensic Detective – аналіз дзвінків, повідомлень, геолокаційних даних.

Cellebrite UFED – відновлення та аналіз даних із мобільних телефонів.

6. Для аналізу шкідливого програмного забезпечення:

IDA Pro – дизасемблювання та аналіз шкідливого коду.

PE Explorer – дослідження виконуваних файлів Windows.

Cuckoo Sandbox – динамічний аналіз підозрілих файлів у віртуальному середовищі.

7. Для складання криміналістичних звітів та документування:

LaTeX, MS Word – підготовка технічної документації та звітів.

CaseNotes – ведення криміналістичних нотаток.

8. Платформи для дистанційного навчання:

Moodle, Microsoft Teams – розміщення навчальних матеріалів, тестування та проведення лекцій.

Google Drive, OneDrive – спільна робота з документами та звітами.

Використання наведеного обладнання та програмного забезпечення дозволяє студентам отримати практичний досвід у сфері цифрової криміналістики та підготуватися до роботи в реальних криміналістичних розслідуваннях.

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.

Базові підручники:

1. Herbane B. Business Continuity and Crisis Management: Planning for the Unthinkable. 2nd edition. Routledge, 2023. 250 p.
2. Elliott D., Swartz E., Herbane B. Business Continuity Management: A Crisis Management Approach. Routledge, 2022. 340 p.
3. Hiles A. The Definitive Handbook of Business Continuity Management. 4th edition. Wiley, 2022. 880 p.
4. Snedaker S., Rima C. Business Continuity and Disaster Recovery Planning for IT Professionals. 3rd edition. Syngress, 2021. 450 p.
5. Smith D. Crisis Management – Practice and Future Directions. Routledge, 2022. 310 p.
6. **ISO 22301:2019** – Security and resilience – Business continuity management systems – Requirements.
7. **ISO/TS 22317:2021** – Guidelines for business impact analysis (BIA).
8. **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.
9. **Herbane, B.** Business Continuity and Crisis Management: Planning for the Unthinkable – Routledge, 2023.
10. **Hiles, A.** The Definitive Handbook of Business Continuity Management – Wiley, 2022.
11. **Snedaker, S., Rima, C.** Business Continuity and Disaster Recovery Planning for IT Professionals – Sybex, 2023.
12. **Elliott, D., Swartz, E., Herbane, B.** Business Continuity Management: A Crisis Management Approach – Routledge, 2022.
13. **Cerullo, V., Cerullo, M.** Disaster Recovery Planning: Ensuring Business Continuity – Wiley, 2021.
14. **Paton, D., Johnston, D.** Disaster Resilience: An Integrated Approach – Charles C Thomas Publisher, 2022.
15. **National Institute of Standards and Technology (NIST) SP 800-34 Rev. 1** – Contingency Planning Guide for Federal Information Systems, 2022.

Джерела:

1. Rouco J. C., Figueiredo P. C. Business Continuity Management and Resilience: Theories, Models, and Processes. IGI Global, 2024. 360 p.
2. Барський М. В. Безперервність бізнесу в контексті ланцюгів постачання. *Сталий розвиток економіки.* 2024. № 1(48). С. 302–308. DOI: https://doi.org/10.32782/2308-1988/2024-48-42
3. Baz J. E., Ruel S. Investigating the role of business continuity during COVID-19: an empirical examination. *Supply Chain Forum.* 2023. P. 1–14. DOI: 10.1080/16258312.2023.2199127.
4. Hall T. Business continuity beyond COVID-19: Lessons learned and the 'illusion of preparedness'. *Journal of Business Continuity & Emergency Planning.* 2022. Volume 16. Number 1. P. 45–52.
5. BCI Horizon Scan Report 2023. *The Business Continuity Institute (BCI).* URL: https://www.thebci.org/resource/bci-horizon-scan-report-2023.html
6. ISO 22301. Security and resilience – Business continuity management systems – Requirements. URL: https://pttweb7.pttplc.com/pttbcm/upload/media/878_ISO22301_2019.pdf
7. The Global Risks Report 2020. *The World Economic Forum.* URL: https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
8. Fragile States Index. *The Fund for Peace.* URL: https://fragilestatesindex.org/