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

РОБОЧА ПРОГРАМА
Методологічні засади кібербезпеки

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

«26» 08.2025 р.

Розробник (-и): Ткач Юлія Миколаївна, завкафедри КБММ, д.пед.н., к.т.н., проф. _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Робочу програму навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання_____
(назва кафедри)

Протокол від «26»08.2025р. №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	1 рік, 1 семестр F5 Кібербезпека та захист інформації ОПП Кібербезпека
Викладач (-і)	Ткач Юлія Миколаївна, завкафедри КБММ, д.пед.н., к.т.н., проф.
Профайл викладача (-ів)	Web: https://mmi.stu.cn.ua/personal-kafedry/ ORCID: 0000-0002-8565-0525
Контакти викладача	Чернігів, вул. Шевченка, 95, корп.1, каб. 108; E-mail: tkachym@stu.cn.ua

2. Анотація курсу. Курс «Методологічні засади кібербезпеки» спрямований на формування у студентів комплексного розуміння основ кібербезпеки, методів та засобів захисту інформації. Дисципліна охоплює теоретичні та практичні аспекти інформаційної безпеки, забезпечуючи здобувачів вищої освіти знаннями та навичками, необхідними для аналізу ризиків, впровадження стратегій кіберзахисту та дотримання нормативно-правових вимог у сфері інформаційної безпеки.

Основні теми курсу

Змістовий модуль 1: Основи методології захисту інформації

- Основні поняття та визначення у сфері кібербезпеки
- Методологічні засади кібербезпеки
- Джерела загроз та їх класифікація

Змістовий модуль 2: Технології та методи захисту інформації

- Моделі захисту інформації та модель порушника
- Методи технічного, криптографічного захисту інформації тощо
- Засоби моніторингу та реагування на інциденти

Посилання на курс в MOODLE: https://eln.stu.cn.ua/course/view.php?id=4444

3. Мета та цілі курсу.

Метою дисципліни «Методологічні засади кібербезпеки» є надання студентам фундаментальних знань і практичних навичок щодо захисту інформації, розробки та впровадження заходів кібербезпеки, аналізу загроз та оцінки вразливостей інформаційних систем.

Завдання курсу

- Вивчення основних концепцій та принципів кібербезпеки.
- Ознайомлення з нормативно-правовими актами та стандартами у сфері інформаційної безпеки.
- Аналіз загроз та вразливостей інформаційних систем.
- Розвиток навичок використання засобів захисту інформації.
- Впровадження заходів управління ризиками у кіберпросторі.
- Формування компетенцій у розробці стратегій безпеки та планів реагування на інциденти.
- Ознайомлення з сучасними технологіями та методами захисту інформації

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 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

4. Результати навчання.

За результатами вивчення курсу студенти повинні:

Знати:

- Основні принципи кібербезпеки та інформаційного захисту.
- Законодавчу та нормативну базу у сфері кібербезпеки.
- Класифікацію загроз та їх вплив на інформаційні системи.
- Методи оцінки ризиків та стратегії кіберзахисту.
- Технології шифрування та аутентифікації.
- Політики управління інформаційною безпекою.

Вміти:

- Виявляти та аналізувати загрози інформаційній безпеці.
- Використовувати сучасні методи та інструменти захисту інформації.
- Розробляти та впроваджувати заходи кібербезпеки.
- Здійснювати аудит та тестування інформаційних систем.
- Використовувати технічні засоби моніторингу кіберзагроз.
- Працювати з інструментами криптографічного захисту інформації.

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

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

ПРН 3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі;

ПРН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН 9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.

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. Зазначте загальну кількість кредитів, кількість занять та годин самостійної роботи.

Вид заняття	Загальна кількість годин денне/заочне
Лекції	16/6
Практичні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – контрольна робота	
Всього кредитів – *вказати кількість кредитів*	4

7. Тематика курсу.

Змістовий модуль 1. Основи методології захисту інформації

Тема 1.1. ОСНОВИ МЕТОДОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ У КІБЕРПРОСТОРІ. Методологія захисту інформації як організація продуктивної діяльності людини. Понятійний апарат інформаційної безпеки та кібербезпеки. Складові забезпечення інформаційної безпеки та кібербезпеки. Проблеми теорії і практики забезпечення інформаційної безпеки та кібербезпеки. Поняття, сутність та цілі захисту інформації. Характеристика інформації як об'єкта захисту. Інформація як об'єкт права власності.Поняття, сутність, цілі захисту інформації. Моделі у галузі захисту інформації. Модель інформаційної безпеки та кібербезпеки.

Тема 1.2. Джерела загроз та їх класифікація. Сутність потенційних та реальних загроз інформації. Джерела виникнення загроз та шляхи їх реалізації. Класифікація загроз інформації в комп'ютерній системі. Моделі захисту інформації та модель порушника. Класифікація автоматизованих систем в НД ТЗІ. Модель захисту інформації. Модель порушника інформаційної безпеки

Змістовий модуль 2. Технології та методи захисту інформації

Тема 2.1. Методи захисту інформації

Методи забезпечення інформаційної безпеки. Методи протидії загрозам. Методи контролю ефективності захисту. Канали витоку інформації. Класифікація каналів витоку. Технічні канали витоку. Організаційні канали витоку.

Тема 2.2. Несанкціонований доступ

Загальні положення про НСД. Методи та засоби НСД. Захист від НСД.

Тема 2.3. Технічний захист інформації

Електромагнітні канали. Акустичні канали. Оптичні канали. Організаційні заходи захисту. Адміністративні заходи. Політика безпеки. Розподіл повноважень і відповідальності.

Тема 2.4. Криптографічні методи захисту. Стеганографія.

Симетричні алгоритми. Асиметричні алгоритми. Протоколи з відкритим ключем. Стеганографія та цифрові водяні знаки. Методи приховування інформації. Використання цифрових водяних знаків.

Тема 2.5. Захист персональних даних та державної таємниці

Правові основи захисту інформації з обмеженим доступом. Захист персональних даних. Захист державної таємниці.

Тема 2.6. Управління системою захисту інформації

Принципи управління системами захисту. Політики та стратегії. Моніторинг і аудит. Сертифікація систем захисту. Порядок сертифікації КСЗІ. Національні й міжнародні стандарти.

Тема 2.7. Методи дослідження у сфері інформаційної безпеки

Статистичні методи. Моделювання. Аналіз ефективності систем захисту.

Тема 2.8. Проєктування та випробування КСЗІ в АС

Розроблення технічного завдання. Комплекс засобів захисту інформації. Вимоги до організаційних заходів. Проєктна та експлуатаційна документація. Випробування та дослідна експлуатація.

Курс спрямований на формування комплексного підходу до кібербезпеки, що включає технічні, організаційні та правові аспекти інформаційного захисту.

Теми практичних:

Практична робота 1. Основні поняття та визначення у сфері кібербезпеки
Практична робота 2. Методологічні засади кібербезпеки та ISMS
Практична робота 3. Джерела загроз та їх класифікація
Практична робота 4. Моделі порушника та моделі безпеки
Практична робота 5. Технічні та криптографічні контролі
Практична робота 6. Аутентифікація та авторизація
Практична робота 7. SOC та реагування на інциденти

Самостійна робота

1. Еволюція підходів до інформаційної безпеки: від класичних до сучасних моделей.
2. Сутність і завдання кібербезпеки як науки та практики.
3. Поняття активів, загроз, вразливостей і ризиків: сучасні трактування.
4. Триада CIA та її розширення: конфіденційність, цілісність, доступність, аутентичність, незаперечність.
5. Методи аналізу контексту організації для побудови ISMS.
6. Огляд міжнародних і національних стандартів у сфері ІБ та кіберзахисту (ISO/IEC 27001, NIST, ДСТУ).
7. Ризик-орієнтований підхід у кібербезпеці: принципи та практики.
8. Модель порушника: класифікація, мотивація, ресурси та обмеження.
9. Методи моделювання загроз: STRIDE, PASTA, LINDDUN.
10. Проблеми впровадження комплексних систем захисту в організаціях України.
11. Методи технічного захисту інформації: класифікація та приклади застосування.
12. Технічні канали витоку інформації та методи їх блокування.
13. Організаційні канали витоку інформації та способи протидії.
14. Проблематика несанкціонованого доступу: методи й засоби атак.
15. Методи протидії НСД: організаційні, програмні, апаратні.
16. Системи контролю доступу: DAC, MAC, RBAC, ABAC, PBAC.
17. Технічний захист від електромагнітних, акустичних та оптичних каналів.
18. Криптографічні методи захисту: симетричні й асиметричні алгоритми.
19. Цифрові підписи та протоколи з відкритим ключем.
20. Стеганографія та цифрові водяні знаки як методи приховування інформації.
21. Правові основи захисту персональних даних в Україні та ЄС (GDPR).
22. Правове регулювання захисту державної таємниці.
23. Управління системами захисту: принципи, політики та стратегії.
24. Сертифікація КСЗІ: національні та міжнародні вимоги.
25. Моніторинг і аудит у системах кібербезпеки.
26. Планування безперервності бізнесу (BCP) і відновлення після катастроф (DRP).
27. Методи оцінки ефективності систем захисту.
28. Роль SOC у сучасних організаціях: моніторинг, реагування, автоматизація.

29. Інформаційно-психологічна безпека як складова кіберзахисту.
30. Перспективи розвитку квантової криптографії та її застосування в захисті інформації.

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 оцінюється в 20 балів, сам.р. – 8 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…40 ● 2. С/р 0…8 ● 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 оцінюється в 20 балів, с/р – 8 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 практичних робіт	0…15/10
3	Самостійна робота	0…8/13

Змістовий модуль 2.		
1	Повнота відповідей на запитання на лекціях	0…2
2	Результати захисту практичних робіт	0…15/10
3	Самостійна робота	0…8/13
Контрольна робота		**10**
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**).**

При вивченні цього курсу для дистанційного навчання, тестування та обговорення питань курсу використовуються платформи Moodle та Microsoft Teams, для виконання занять застосовується комутаційне й серверне обладнання, а також ПК та програмне забезпечення навчальних аудиторій 105, 106, 110, 111 кафедри кібербезпеки та математичного моделювання.

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. **Головко, О. М.** Основи кібербезпеки: навчальний посібник. – Київ: Вид. дім «Кондор», 2021. – 312 с.
2. **Кузнецов, С. О.** Кібербезпека та захист інформації: підручник. – Харків: ХНУРЕ, 2022. – 280 с.

3. **Гуляєв, Д. О.** Системи кіберзахисту: методологія та практика. – Львів: Львівський національний університет імені Івана Франка, 2023. – 256 с.
4. **Васильєв, А. В.** Кіберзагрози та їх протидія: підручник для студентів. – Одеса: ОНАЗ, 2020. – 234 с.
5. **Тимощук, В. А.** Фундаментальні аспекти інформаційної безпеки. – Полтава: ПолтНТУ, 2023. – 198 с.
6. **Сидоренко, П. В.** Основи цифрової безпеки: концепції та технології. – Дніпро: ДНУ, 2022. – 314 с.
7. **Schneider, B.** Applied Cryptography: Protocols, Algorithms, and Source Code in C. – Wiley, 2021. – 784 p.
8. **Stallings, W.** Network Security Essentials: Applications and Standards. – Pearson, 2023. – 448 p.
9. **Anderson, R.** Security Engineering: A Guide to Building Dependable Distributed Systems. – Wiley, 2020. – 1184 p.
10. **McGraw, G.** Software Security: Building Security In. – Addison-Wesley, 2021. – 512 p.

Допоміжна література

1. **Жуковський, М. В.** Захист інформації в цифровому середовищі. – Харків: ХНЕУ, 2021. – 298 с.
2. **Дяченко, І. П.** Інформаційна безпека: підходи до аналізу ризиків. – Запоріжжя: ЗНУ, 2022. – 212 с.
3. **Smith, R.** The Internet of Risky Things: Trusting the Devices That Surround Us. – O'Reilly, 2023. – 272 p.
4. **Shostack, A.** Threat Modeling: Designing for Security. – Wiley, 2022. – 624 p.
5. **Pfleeger, C. P.** Security in Computing. – Pearson, 2023. – 848 p.
6. **National Institute of Standards and Technology (NIST)**. Cybersecurity Framework Version 2.0. – 2024.
7. **Microsoft Security Team**. Zero Trust Security Model: Implementation Guide. – Microsoft Press, 2023.
8. **Kaspersky Lab**. Cybersecurity Threat Intelligence Report 2023.
9. **Gartner Research**. Cyber Risk Management Strategies for Organizations. – 2024.
10. **European Union Agency for Cybersecurity (ENISA)**. Threat Landscape Report. – 2023.

17 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
5. Система дистанційного навчання НУ «Чернігівська політехніка». Курс: Методологічні засади кібербезпеки. – [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=4444