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

СИЛАБУС
Управління ризиками інформаційної безпеки

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

«__26___» __08__ 2024 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)
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)	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 "Управління ризиками інформаційної безпеки" присвячений вивченню методів і принципів аналізу, оцінки та управління ризиками в сфері інформаційної безпеки. Основна увага приділяється ідентифікації загроз, оцінці вразливостей та розробці стратегій мінімізації ризиків у кіберпросторі. Студенти отримають практичні навички використання математичних моделей оцінки ризиків, аналізу загроз та розробки ефективних заходів щодо захисту інформаційних активів. Дисципліна базується на міжнародних стандартах управління ризиками, таких як ISO 27001, NIST та COBIT.

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

3. Мета та цілі курсу.

Метою дисципліни "Управління ризиками інформаційної безпеки" є надання студентам фундаментальних знань та практичних навичок у сфері оцінки та управління ризиками в інформаційній безпеці. Студенти навчаться розпізнавати, оцінювати та мінімізувати ризики, пов’язані з кіберзагрозами, аналізувати інформаційну безпеку організації та розробляти стратегії управління ризиками.

Завдання курсу

- Ознайомлення з основними принципами управління ризиками в інформаційній безпеці.
- Вивчення методів і моделей оцінки інформаційних ризиків.
- Аналіз вразливостей інформаційних систем і оцінка загроз.
- Вивчення міжнародних стандартів управління ризиками.
- Розвиток навичок використання програмних засобів для аналізу ризиків.
- Розробка планів реагування на кіберінциденти та стратегії зменшення ризиків.
- Використання математичних методів для моделювання ризиків.

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

4. Результати навчання.

За результатами вивчення курсу студенти повинні:

Знати:

- Основні характеристики ризику та методи його оцінки.
- Числові показники (характеристики) ризику та способи їх розрахунку.
- Найпоширеніші методики оцінки інформаційних ризиків.
- Основні принципи побудови моделей інформаційних систем в умовах ризику.

- Міжнародні стандарти оцінки ризиків: ISO 27001, NIST, COBIT.
- Основи ризик-менеджменту та управління інцидентами інформаційної безпеки.

Вміти:

- Аналізувати та оцінювати ризики інформаційної безпеки.
- Використовувати інструменти оцінки вразливостей та ймовірностей атак.
- Розробляти політики управління ризиками та плани реагування на інциденти.
- Проводити аудит безпеки та оцінювати відповідність стандартам.
- Впроваджувати заходи щодо мінімізації інформаційних ризиків.
- Використовувати математичні та статистичні методи для оцінки ризиків.

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

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 управління ризиками інформаційної безпеки

Тема 1. Вступ до управління ризиками
Основні поняття та визначення ризиків. Види ризиків у кіберпросторі. Основні підходи до управління ризиками.

Тема 2. Методи та інструменти аналізу ризиків
Кількісні та якісні методи оцінки ризиків. Використання моделей ймовірностей для оцінки загроз.

Тема 3. Виявлення та класифікація ризиків інформаційної безпеки
Типи загроз та вразливостей інформаційних систем. Визначення ступеня впливу загроз на організацію.

Тема 4. Оцінка вразливостей інформаційних систем
Методи тестування безпеки. Виявлення слабких місць у захисті інформаційних активів.

Змістовий модуль 2. Методи аналізу та зменшення ризиків

Тема 5. Міжнародні стандарти оцінки ризиків
Огляд основних міжнародних стандартів управління ризиками (ISO 27001, NIST, COBIT). Ризик-орієнтований підхід до забезпечення безпеки.

Тема 6. Методи аудиту та тестування безпеки
Методи аудиту інформаційної безпеки. Використання інструментів пентестингу та оцінки вразливостей.

Тема 7. Управління інцидентами та реагування на кіберзагрози
Розробка планів реагування на кіберінциденти. Критерії оцінки ефективності заходів кіберзахисту.

Тема 8. Розробка стратегій управління ризиками
Методи мінімізації ризиків. Формування політик та заходів управління ризиками інформаційної безпеки.

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/IEC 27005:2022** – міжнародний стандарт управління ризиками інформаційної безпеки.
2. **NIST Special Publication 800-30 Revision 1** – Guide for Conducting Risk Assessments (2022).
3. **Stallings, W.** *Effective Cybersecurity: A Guide to Using Best Practices and Standards* – Addison-Wesley, 2023.
4. **Anderson, R.** *Security Engineering: A Guide to Building Dependable Distributed Systems* – Wiley, 2021.
5. **Pfleeger, C. P., Pfleeger, S. L.** *Security in Computing* – Pearson, 2023.
6. **Shostack, A.** *Threat Modeling: Designing for Security* – Wiley, 2022.
7. **Bowen, P.** *A Guide to Cyber Threat Intelligence* – Springer, 2023.
8. **Kuznetsov, S. O.** *Risk-Based Approach to Cybersecurity Management* – Springer, 2023.
9. **Chapple, M., Seidl, D.** *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide* – Wiley, 2023.
10. **Kaspersky Lab** – *Cybersecurity Threat Intelligence Report*, 2023.

Допоміжна література:

1. **Johnson, T.** *Digital Risk Assessment and Cybersecurity Analytics* – Routledge, 2023.
2. **Smith, R.** *Cyber Risk Management Strategies* – O'Reilly, 2023.
3. **National Institute of Standards and Technology (NIST)** – *Risk Management Framework*, 2024.
4. **Bowen, P. A.** *Enterprise Risk Management for Information Security* – Springer, 2023.
5. **Microsoft Security Team** – *Zero Trust Security Model: Implementation Guide*, 2023.
6. **ISO/IEC 31000:2023** – стандарт з управління ризиками.
7. **Verizon Data Breach Investigations Report (DBIR)** – щорічний звіт про кіберзагрози та управління ризиками, 2024.
8. **World Economic Forum** – *Global Cybersecurity Outlook 2024*.
9. **IBM X-Force Threat Intelligence Index 2023** – аналіз глобальних кіберзагроз.
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: Управління ризиками ІБ. – [Електронний ресурс]. – Режим доступу: https://eln.stu.cn.ua/course/view.php?id=4461&notifyeditingon=1