Силабус курсу
ОЦІНКА ТА УПРАВЛІННЯ РИЗИКАМИ

Ступінь вищої освіти – бакалавр
Галузь знань – 12 Інформаційні технології
Спеціальність - 125 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Рік навчання: 3
Семестр: 5
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	д.т.н., професор Роман Пасічник
Контактна інформація	roman.pasichnyk@gmail.com, +380964575089

Опис дисципліни

Предметом дисципліни є **методологія та інструментарій** виявлення, аналізу, кількісної та якісної оцінки, моніторингу та контролю **ризиків** у різних сферах діяльності, а також розробка та реалізація ефективних стратегій і заходів, спрямованих на мінімізацію негативних наслідків ризикових подій

Мета та цілі курсу

Мета вивчення дисципліни “Оцінка та управління ризиками” полягає у формуванні у майбутніх спеціалістів умінь та компетенцій для забезпечення ефективної оцінки ризиків та управління ними у кібербезпеці, необхідних для подальшої роботи, навчити їх застосуванню методів та засобів оцінки ризиків та управління ними у кібербезпеці в умовах широкого використання сучасних інформаційних технологій

Завдання дисципліни В результаті вивчення курсу „Оцінка та управління ризиками ” студенти повинні:

– засвоїти основні фундаментальні поняття і закони теорії ризиків для їх використання в сучасних кіберсистемах;

– знати принципи побудови алгоритмів оцінки ризиків та управління ними у кібербезпеці, основних стандартів оцінки ризиків та їх використання в задачах захисту інформації;

– використовувати основний математичний апарат та закони оцінки та управління ризиками у професійній діяльності;

– вміти використовувати програмні засоби, які реалізують основні функції оцінки та управління ризиками;

– програмно реалізовувати основні алгоритми оцінки та управління ризиками для вирішення типових задач захисту інформації;

– проектувати різного рівня системи оцінки та управління ризиками;

– вміння використовувати методи та засоби оцінки та управління ризиками у кібербезпеці.

Результати навчання:

В результаті освоєння курсу студенти повинні отримати навички:

Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.

Загальна інформація про дисципліну

Ступінь вищої освіти	**Бакалавр**
Спеціальність	**125 «Кібербезпека та захист інформації»**
Курс (рік навчання)	**3**
Семестр	**5**
Рік викладання	
Формат курсу	**Очний *(offline)***
Нормативна \ вибіркова	**нормативна**
Загальна кількість год/ кредитів	**150/5**
Лекції, год.	**30**

Перелік тем

1. Концепції оцінки ризику.
2. Види інформаційних систем. Активи та загрози.
3. Системи безпеки та управління ризиками.
4. Розробка інноваційного проєкту інформаційної системи
5. Системна реалізація проекту розроблення інформаційної системи
6. Моделювання системних подавачів даних
7. Системне управління даними
8. Системна візуалізація.
9. Засоби системної безпеки.
10. Підтримка безпеки інформаційних систем.

Рекомендовані джерела інформації

1. Лісовська Ю. Кібербезпека. Ризики та заходи. – К.: Кондор, 2019. – 272 с.
2. Курс мережевої академії Cisco: Управління загрозами у кібербезпеці 2024. Режим доступу: https://www.netacad.com/courses/cyber-threat-management?courseLang=uk-UA
3. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
4. NIST. Framework for Improving Critical Infrastructure Cybersecurity. April 16, 2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf
5. Fagan M, Marron, J, Brady KG, Jr, Cuthill BB, Megas KN, Herold R (2021) IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-213A. https://doi.org/10.6028/NIST.SP.800-213A
6. Stine K, Quinn S, Witte G, Gardner R (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8286. https://doi.org/10.6028/NIST.IR.8286
7. Soni, Arun. The Cybersecurity Self-Help Guide. CRC Press, 2021.
8. Ulven, J.B.; Wangen, G. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 2021,13,39. https://doi.org/ 10.3390/fi13020039
9. ISO 31010 2019. Risk management -Risk assessment techniques. Management du risque -Techniques. – 268 p.
10. Wangen, G. Quantifying and Analyzing Information Security Risk from Incident Data; Graphical Models for Security; Albanese, M., Horne, R., Probst, C.W., Eds.; Springer International. Publishing:

Cham, Switzerland, 2019, pp. 129–154.
11. Radanliev P., et al. "Cyber Risk in IoT Systems." (2019).
12. Lee, In. "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management." Future Internet 12.9, 2020: 157.
13. Wilhelmsen, Cheryl A., and Lee T. Ostrom. Risk assessment: tools, techniques, and their applications. John Wiley & Sons, 2019.
14. Fagan, Michael, et al. "IoT Device Cybersecurity Guidance for the Federal Government." NIST Special Publication 800 (2021): 213.
15. Burnap, Pete. "Risk Management & Governance Knowledge Area Issue." (2021). Version 1.1.1. https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf
16. Django. Tutorials Point. 2015. // https://www.tutorialspoint.com/django/django_tutorial.pdf.
17. Django Tutorial: The Local Library website // https://developer.mozilla.org/en-US/docs/Learn/Server-side/Django/Tutorial_local_library_website
18. Roman Pasichnyk, Ludmila Babala, Mykhaylo Machulyak, Yurii Yakymenko. Modeling Vegetation Index Dynamics in GIS Based on Remote Observations. 2025. 7pp., https://ceur-ws.org/Vol-3974/short03.pdf

Система оцінювання та вимоги

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за роботу на практичних заняттях №1-5	Підсумкова письмова робота за темами №1-5	Оцінка за даний модуль визначається як середнє арифметичне за роботу на практичних заняттях №6-10.	Підсумкова письмова робота за темами №6-10	Визначається як середнє арифметичне за виконання завдань за темами №1-5 тренінгу.	Оцінка за виконаний і представлений звіт із оброблення отриманих даних	1. Теоретична частина: 2 запитання по 20 балів (40 балів) 2. Практична частина 2 задачі по 30 балів кожна (60 балів).

Шкала оцінювання:

За шкалою ЗУНУ	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)
75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

Політики курсу

Академічна доброчесність. Дотримання академічної доброчесності студентами передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- дотримання норм законодавства про авторське право і суміжні права;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;
самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;
фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;
фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;
списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);
- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.