



## Силабус курсу ОЦІНКА ТА УПРАВЛІННЯ РИЗИКАМИ

Ступінь вищої освіти – бакалавр

Рік навчання: 3

Семестр: 5

Кількість кредитів: 5

Мова викладання: українська

ППП

Контактна інформація

### Керівник курсу

Василь Яцків

vy@wunu.edu.ua

### Опис дисципліни

Курс "Оцінка та управління ризиками" спрямований на навчання студентів сучасним методам та стратегіям оцінки, виявлення та управління ризиками в області кібербезпеки. Ця анотація висвітлює ключові аспекти та мету цього курсу.

Головні аспекти курсу включають наступне:

1. **Оцінка кіберризиків:** Учасники курсу навчаються визначати потенційні загрози та ризики, яким піддається інформаційна система чи організація, і проводити оцінку їх потенційного впливу.

2. **Методи виявлення ризиків:** Курс розглядає різні методи та інструменти для виявлення ризиків, включаючи аналіз вразливостей, тестування на проникнення, аудит безпеки та інші.

3. **Управління ризиками:** Учасники дізнаються, як розробляти та впроваджувати стратегії управління ризиками, включаючи вибір імовірних ризикових подій та заходів їх запобігання.

4. **Стандарти та норми:** Курс оглядає актуальні стандарти та норми у галузі кібербезпеки, такі як ISO 27001, NIST Cybersecurity Framework, та їхнє використання в управлінні ризиками.

5. **Аналіз і відслідковування ризиків:** Учасники навчаються використовувати дані та метрики для аналізу ризиків та відслідковування їх стану з часом.

6. **Кейси та практичні завдання:** Курс включає в себе розв'язання кейсів та практичні завдання, що допомагають студентам застосовувати набуті знання на практиці.

Цей курс допомагає студентам та фахівцям розробити компетенції у сфері оцінки та управління кіберризиками, що є критичними в умовах постійно зростаючих загроз кібербезпеці. Він дозволяє підготувати кваліфікованих фахівців для роботи в області кібербезпеки та забезпечити безпеку інформаційних ресурсів організацій.

**Мета курсу «Оцінка та управління ризиками»** полягає у формуванні у майбутніх спеціалістів професійних компетенцій з ефективною оцінки та управління ризиками.

### Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Концепції оцінки ризику	Розуміти поняття ризику та концепції оцінки ризику	Поточне опитування
2/2	Ідентифікація активів	Вміти проводити ідентифікацію активів	Поточне опитування

2/2	Ідентифікація загрози	Вміти ідентифікувати загрози. Знати модель загрози STRIDE	Поточне опитування
2/2	Ідентифікація вразливості	Вміти Ідентифікувати вразливості. Проводити оцінку вразливостей.	Поточне опитування
2/2	Підходи до оцінки ризиків	Проводити кількісну та якісну оцінку ризику	Поточне опитування
2/4	Оцінка імовірності ризику	Оцінювати імовірність ризику	Поточне опитування
2/4	Визначення ризику	Визначати потенційні загрози	Поточне опитування, тестування
2/0	Методологія оцінки ризику	Проводити вимірювання рівня ризику	Поточне опитування
2/4	Обробка ризиків	Розуміти процес оцінки інформаційних ризиків	Поточне опитування
2/0	Концепції управління ризиками	Знати політику управління ризиками інформаційних систем.	Поточне опитування
2/2	Відповідь на ризики	Здійснювати вибір та впровадження контрзаходів	Поточне опитування
2/2	Моніторинг ризиків	Проводити моніторинг ефективності оцінки ризиків	Поточне опитування
2/4	Управління ризиками ланцюга постачання.	Знати ризики, пов'язані з обладнанням, програмним забезпеченням та послугами. Інші ризики третіх сторін. Мінімальні вимоги безпеки. Угоди про рівень обслуговування.	Поточне опитування
2/0	Безперервність бізнесу	Знати стандарти та передовий досвід оцінки ризиків	Поточне опитування, тестування

### 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](https://www.cybok.org/media/downloads/Risk_Management_Governance_v1.1.1.pdf)

### Політика оцінювання

**Політика щодо дедлайнів та перескладання:** Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

**Політика щодо академічної доброчесності:** Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

**Політика щодо відвідування:** Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

### Оцінювання

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10 %	10 %	10 %	10 %	5 %	10 %	40 %
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-5.	Підсумкова письмова робота за темами №1-7.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 6-10.	Підсумкова письмова робота за темами №8-14	Визначається як середнє арифметичне з оцінок за виконання трьох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання вибраного наскрізного завдання.	1. 15 тестів по 4 бали - max 60 балів. 2. Практичне завдання - max 40 балів

### Шкала оцінювання:

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