Назва курсу	**«Безпека комп'ютерних та кіберфізичних систем»**
Викладач (-і)	Яцків Василь Васильович
Профайл викладача (-ів)	https://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
Контактний тел.	+380352-475050 ext. 56501
E-mail:	**v.yatskiv(@)wunu.edu.ua**
Сторінка курсу в moodle	https://moodle.wunu.edu.ua
Консультації	Очні консультації: вівторок: 14-00, ауд. 6501. Онлайн- консультації (zoom): вівторок з 15 -00 до 16-00.

1. Анотація до курсу.

Даний курс розширює кругозір аспірантів в області передових підходів та методів захисту комп'ютерних та кіберфізичних систем шляхом проведення досліджень, розробки відповідних заходів та їх впровадження.

2. Пререквізити.

Раніше вивчені дисципліни необхідні для освоєння курсу: базовий обсяг знань з апаратного комп'ютерного, мережного та програмного забезпечення, систематичних та ґрунтовних знань із суміжних курсів «Методологія та організація наукових досліджень», «Методи оптимізаці», «Математичне моделювання та обчислювальні методи» а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

Постреквізити. Матеріал даної дисципліни може бути використаний при написанні дисертаційної роботи.

3. Мета та цілі курсу.

Мета курсу «Безпека комп'ютерних та кіберфізичних систем» полягає в навчанні аспірантів:

- розробляти та презентувати обґрунтований план досліджень, планувати та проводити експерименти щодо розробки методів забезпечення кібербезпеки інформаційних і комп'ютерних систем, віртуальних систем та критичних інфраструктур;
- визначати, аналізувати та поєднувати інформацію з різних джерел та підготовлювати нову форму вторинної інформації, зокрема, щодо забезпечення загальних та спеціальних вимог до кібербезпеки;
- ініціювати та виконувати оригінальні дослідження в напрямку освоєння методів забезпечення кібербезпеки інформаційних і комп'ютерних систем у звичайних та надзвичайних ситуаціях та досягати наукових результатів, які створюють нові знання;
- управляти науковими проектами або писати пропозиції на фінансування наукових досліджень, зокрема наукових досліджень методів і систем запобігання, виявлення, обробки та усунення наслідків інцидентів кібербезпеки, а також методики попередження та розслідування кіберзлочинів;
- використовувати сучасні математичні методи, моделі, інформаційні технології та техніки для забезпечення кібернетичної та інформаційної безпеки інформаційних і комп'ютерних систем;

- визначати місію, прогнозувати та планувати цілі і задачі технологій кібербезпеки інформаційних і комп'ютерних систем.

Результати навчання:

В результаті вивчення дисципліни аспірант повинен:

Знати сучасні методи проведення досліджень в галузі кібербезпеки.

Вміти розв'язувати задачі синтезу та аналізу об'єктів професійної діяльності кібербезпеки.

Вміти досліджувати проблеми кібербезпеки критичної інфраструктури.

Вміти синтезувати науково обгрунтовані рішення по захисту інформації в кіберсистемах та кіберфізичних системах

4 Загальна інформація про дисципліну

Ступінь вищої освіти	**доктор філософії**
Спеціальність	**125 Кібербезпека**
Курс (рік навчання)	**перший**
Семестр	**2**
Рік викладання	**2023/2024**
Формат курсу	**Очний (offline)**
Нормативна \ вибіркова	**вибіркова**
Загальна кількість год/ кредитів	**150/5**
Лекції, год.	**20**
Лабораторні, год	**20**
Самостійна робота, год.	**110**

5. Перелік тем

1. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення.
2. Поширені атаки на комп'ютерні системи.
3. Типи атак на комп'ютерні системи.
4. Атаки на службові протоколи.
5. Захист кінцевих пристроїв.
6. Безпека хмарних технологій.
7. Моніторинг мережі і засоби моніторингу.
8. Аналіз даних вторгнень.
9. Реагування на інциденти.
10. Обробка інцидентів.

Рекомендовані джерела

1. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка 2019. – 580.

2. Messier, R. CEH V10 Certified Ethical Hacker Study Guide. John Wiley & Sons. 2019. – 584 с.
3. Warsinske, J., Graff, M., Henry, K., Hoover, C., Malisow, B., Murphy, S., & Vasquez, M. The Official (ISC) 2 Guide to the CISSP CBK Reference. John Wiley & Sons. 2019. – 928 с.
4. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), № 45, ст.403 зі змінами від 28.07.2022 року. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
5. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.
6. Hamdani, Syed Wasif Abbas, et al. "Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons." *ACM Computing Surveys (CSUR)* 54.3, 2021. – pp.1-36
7. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. – 341 p.
8. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
9. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
10. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.
11. Cisar, P., & Pinter, R. Some ethical hacking possibilities in Kali Linux environment. *Journal of Applied Technical and Educational Sciences*, *9*(4), 2019, pp.129-149.
12. Teixeira, D. Metasploit Penetration Testing Cookbook - Third Edition. Packt Publishing Ltd. 2018.
13. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.

Політика оцінювання

● Політика щодо дедлайнів та перескладання: Роботи, які здаються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-20 балів). Перескладання екзамену відбувається із дозволу проректора з наукової роботи за наявності поважних причин (наприклад, лікарняний).

● Політика щодо академічної доброчесності: Усі письмові роботи перевіряються на наявність плагіату і допускаються до захисту із коректними текстовими запозиченнями не більше 20%.

●Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання, за яке нараховуються бали. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Оцінка за курс визначається наступним чином:

Види оцінювання	% від остаточної оцінки
Екзамен	100

Шкала оцінювання аспірантів:

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