



## Силабус курсу ПРАКТИКУМ ЗІ СПЕЦІАЛЬНОСТІ

Ступінь вищої освіти – бакалавр

Рік навчання: 4

Семестр: 8

Кількість кредитів: 6

Мова викладання: українська

### Керівник курсу

ПП

Василь Яцків

Контактна інформація

vy@wunu.edu.ua

### Опис дисципліни

Курс «Практикум зі спеціальності» є незамінною складовою навчального процесу для студентів, які готуються до висококваліфікованої роботи у галузі кібербезпеки.

Головні аспекти курсу включають наступне:

1. Практичний досвід. Курс розроблений з метою забезпечити студентам можливість отримати реальний практичний досвід у обраній галузі. Він допомагає застосовувати теоретичні знання в практичних ситуаціях та набувати навички, необхідні для подальшої професійної кар'єри.

2. Закріплення знань. Учасники курсу можуть вдосконалити свої навички та глибше зрозуміти основні концепції та методи, які вивчаються в теоретичних предметах. Практикум дозволяє закріпити отримані знання через практичні завдання та проекти.

Цей курс спрямований на те, щоб підготувати студентів до успішної кар'єри в галузі кібербезпеки, допомагаючи їм розвивати практичні навички, отримувати цінний досвід та створювати основу для подальшого професійного розвитку.

Метою дисципліни «Практикум зі спеціальності» є – здобуття компетентностей, які формуються під час вивчення комплексу обов'язкових освітніх компонент упродовж всього терміну навчання та підготовки до успішного складання екзамену.

### Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
6/4	Законодавча та нормативно-правова база, державні та міжнародні вимоги, практики і стандарти в галузі інформаційної та/або кібербезпеки	Знати законодавча та нормативно-правова база України в галузі інформаційної та/або кібербезпеки. Знати міжнародні стандарти в галузі інформаційної та/або кібербезпеки	Поточне опитування
4/4	Інформаційні технології в інформаційній та/або кібербезпеці	Знати інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці.	Поточне опитування

4/4	Безпека інформаційно-комунікаційних систем	Знати механізми захисту інформації, що обробляється та зберігається в ІКС	Поточне опитування
4/6	Комплексні системи захисту інформації	Оцінювати захищеність інформації в ІКС	Поточне опитування, тестування
4/4	Управління інформаційною та / або кібербезпекою	Розробляти політики інформаційної безпеки	Поточне опитування
4/4	Криптографічний захист інформації	Знати математичні основи криптографії та стеганографії	Поточне опитування
4/4	Тема 7. Технічний захист інформації	Знати методи та засоби технічного захисту інформації	Поточне опитування, тестування

### Рекомендовані джерела інформації

1. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403, зі змінами від 28.07.2022 року. Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
2. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарев А. Видавництво Львівська політехніка, 2019. – 580.
3. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. *Information Security Journal: A Global Perspective* 31. 4, 2022. – pp. 466-478.
4. 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
5. Santos, Henrique MD. *Cybersecurity: A Practical Engineering Approach*. CRC Press, 2022. – 341 p.
6. Grubb S. *How Cybersecurity Really Works*. 2021. – 219 p.
7. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
8. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.
9. 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.
10. Teixeira, D. *Metasploit Penetration Testing Cookbook - Third Edition*. Packt Publishing Ltd. 2018.
11. Stallings, W. *Effective Cybersecurity: Understanding and Using Standards and Best Practices*. Addison-Wesley. 2019. – 893 p.
12. 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 c.

### 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, військовий 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%	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 захист лабораторних робіт №1-6.	Підсумкове модульне тестування за темами № 1-4.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 7-12.	Підсумкове модульне тестування за темами № 5-7.	Визначається як оцінка за виконання одного із завдань тренінгу.	Визначається як оцінка за виконання наскрізного завдання самостійної роботи.	1. Теоретичні питання. 2. Питання по 10 балів. 2. 20 тестів по 4 бали.

### Шкала оцінювання

За шкалою ЗУНУ (сума балів за всі види навчальної діяльності в межах модуля)	За національною шкалою	За шкалою ECTS
90-100	відмінно	<b>A</b> (відмінно)
85-89	добре	<b>B</b> (дуже добре)
75-84		<b>C</b> (добре)
65-74	задовільно	<b>D</b> (задовільно)
60-64		<b>E</b> (достатньо)
35-59	незадовільно	<b>FX</b> (незадовільно з можливістю повторного складання)
1-34		<b>F</b> (незадовільно з обов'язковим повторним курсом)