



Силабус курсу ПРАКТИКУМ ЗІ СПЕЦІАЛЬНОСТІ

Ступінь вищої освіти – бакалавр
Галузь знань – F Інформаційні технології
Спеціальність - F5 Кібербезпека та захист інформації
Освітньо-професійна програма – «Кібербезпека»
Рік навчання: 4
Семестр: 8
Кількість кредитів: 6
Мова викладання: українська

Керівник курсу

ППП

Сергій Кулина

Контактна інформація

sersks@wunu.edu.ua

Опис дисципліни

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

Головні аспекти курсу включають наступне:

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

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

Метою курсу «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

6/6	Інформаційні технології в інформаційній та/або кібербезпеці	Знати інструментальні та прикладні застосунки в інформаційній та/або кібербезпеці.	Поточне опитування
4/6	Безпека інформаційно-комунікаційних систем	Знати механізми захисту інформації, що обробляється та зберігається в ІКС	Поточне опитування
2/2	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
6/6	Криптографічний захист інформації	Знати математичні основи криптографії та стеганографії	Поточне опитування
2/2	Технічний захист інформації	Знати методи та засоби технічного захисту інформації	Поточне опитування, тестування

Рекомендовані джерела інформації

- Опорний конспект лекцій з дисципліни «Практикум зі спеціальності» для здобувачів освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти спеціальності «Кібербезпека та захист інформації»/ Укл.: Яцків В.В., Кулина С.В. Тернопіль : ЗУНУ, 2025. 41 с.
- Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective 31. 4, 2022. – pp. 466-478.
- Breaking Down the OSI Model: A Cybersecurity Perspective - DEV ..., – URL: <https://dev.to/aditya8raj/breaking-down-the-osi-model-a-cybersecurity-perspective-22ni>
- Cybersecurity Algorithms - Meegle, – URL: https://www.meegle.com/en_us/topics/algorithm/cybersecurity-algorithms
- Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
- Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
- 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.
- ISO 27001 Implementation Phase - Iseo Blue, – URL: <https://iseoblue.com/post/iso-27001-implementation-phase/>
- Possible attacks on the TCP/IP protocol stack and countermeasures, – URL: <https://securityaffairs.com/117635/security/tcp-ip-protocol-stack-attacks.html>
- Santos, Henrique MD. *Cybersecurity: A Practical Engineering Approach*. CRC Press, 2022. 341 p.
- 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>
- Курс мережевої академії Cisco: CCNA Cybersecurity Operations. 2020. Режим доступу. <https://www.netacad.com/courses/security/ccna-cybersecurity-operations>
- Про захист інформації в інформаційно-комунікаційних системах - НТФ "Інтес", – URL: <https://qdpro.com.ua/document/18462>
- Указ президента України №447/2021 — Офіційне інтернет ..., – URL: <https://www.president.gov.ua/documents/4472021-40013>

Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання усіх видів завдань здобувачами освіти і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів проводиться в установленому порядку.

Політика щодо академічної доброчесності. Списування під час проведення контрольних заходів заборонені. Під час контрольного заходу здобувач освіти може користуватися лише дозволеними допоміжними матеріалами або засобами, йому забороняється в будь-якій формі обмінюватися інформацією з іншими учасниками, використовувати, розповсюджувати, збирати варіанти контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в дистанційній формі за погодженням із керівником курсу з дозволу дирекції факультету.

Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Практикум зі спеціальності» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

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: 3 питання по 10 балів. 2. 35 тестів по 2 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	A (відмінно)
85-89	добре	B (дуже добре)
75-84		C (добре)
65-74		D (задовільно)
60-64	задовільно	E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)