Силабус курсу
КІБЕРНЕТИЧНА БЕЗПЕКА

Ступінь вищої освіти – бакалавр
Рік навчання: 3
Семестр: 5
Кількість кредитів: 6
Мова викладання: українська

Керівник курсу

ПІП	Василь Яцків
Контактна інформація	vy@wunu.edu.ua

Опис дисципліни

Курс «Кібернетична безпека» охоплює знання і навички, необхідні для успішної обробки завдань і зон обов'язків аналітика безпеки молодшого рівня, який працює в центрі моніторингу та управління безпекою (SOC).

Після проходження курсу студенти зможуть виконувати такі завдання: аналізувати роботу мережевих протоколів і служб; пояснити принципи роботи мережевої інфраструктури; класифікувати різні типи мережевих атак; використовувати засоби мережевого моніторингу для визначення атак на мережеві протоколи і служби; застосовувати різні способи запобігання несанкціонованому доступу до комп'ютерних мереж, хостів і даними; знати способи визначення вразливостей кінцевих пристроїв і атаках на них; виявляти попередження безпеки мережі; аналізувати дані про вторгнення в мережу для перевірки потенційних загроз; застосовувати моделі реагування для усунення інцидентів безпеки.

Метою курсу «Кібернетична безпека» аналітика, який працює в центрі моніторингу та управління безпекою (SOC).

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
3/3	Кібербезпека і центр моніторингу та управління безпекою	Розуміти структуру та функції сучасного центру моніторингу та управління безпекою	Поточне опитування,
3/3	Принципи забезпечення безпеки комп’ютерних систем	Знати інструменти зловмисників та завдання кібербезпеки	Поточне опитування,
3/3	Поширені атаки комп’ютерні системи.	Знати типи шкідливого програмного забезпечення	Поточне опитування,
3/3	Типи атак на комп’ютерні системи	Розрізняти иипи атак на комп’ютерні системи	Поточне опитування,
3/3	Моніторинг мережі і засоби моніторингу.	Знати методи та засоби моніторингу мережі	Поточне опитування
3/3	Атаки на базові функції.	Розуміти принципи здійснення поширених атак.	Поточне опитування
3/3	Атаки на службові протоколи.	Розуміти атаки на службові протоколи	Поточне опитування
3/3	Захист мережі.	Знати політики безпеки. Відповідність нормативним вимогам і стандартам.	Поточне опитування, тестування
3/3	Управління доступом.	Знати концепції управління доступом та моделі управління доступом.	Поточне опитування
3/3	Захист кінцевих пристроїв.	Знати методи захисту від вторгнень на рівні хоста	Поточне опитування,
3/3	Моніторинг безпеки.	Здійснювати аналіз файли журналів кінцевих	Поточне

		пристроїв та мережеві журнали.	опитування
3/3	Аналіз даних вторгнень.	Проводити дослідження мережевих даних	Поточне опитування
3/3	Реагування на інциденти і їх обробка.	Знати моделі реагування на інциденти та ланцюг кібервбивства	Поточне опитування
3/3	Обробка інцидентів.	Знати життєвий цикл реагування на інциденти NIST. Проводити дії після інцидентів	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Курс мережевої академії Cisco: CyberOps Associate.. 2020. Режим доступу. https://www.netacad.com/courses/cybersecurity/cyberops-associate
2. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. – 580.
3. 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
4. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.
5. 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
6. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. – 341 p.
7. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
8. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.
9. Maurushat, Alana. *Ethical hacking*. University of Ottawa Press, 2019.
10. 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.
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, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Заліковий модуль 1	Заліковий модуль 2	Заліковий модуль 3	Заліковий модуль 4
20%	20%	20%	40%
1. Усне опитування на заняттях – max 21 балів. 2. Письмова робота – max 55 балів.	1. Усне опитування на заняттях – max 21 балів. 2. Письмова робота – max 55 балів.	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг	1. Розв'язання 20 тестів по 3 бали = max 60 балів. 2. Практичне завдання = max 40 балів

3. Практичне завдання – max 24 балів	3. Практичне завдання – max 24 балів	– max 30 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