Назва курсу	**«Інформаційна безпека»**
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

Анотація до курсу.

Курс «Інформаційна безпека» охоплює знання і навички, необхідні для успішної обробки завдань, обов'язків 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.

Мета та цілі курсу.

Метою є аналітика, який працює в центрі моніторингу та управління безпекою (SOC).

Загальна інформація про дисципліну

Ступінь вищої освіти	**Бакалавр**
Спеціальність	**124 – Системний аналіз**
Курс (рік навчання)	**3**
Семестр	**5**
Нормативна \ вибіркова	**вибіркова**
Загальна кількість кредитів	**5**

Перелік тем

1. Кібербезпека і центр моніторингу та управління безпекою.
2. Принципи забезпечення безпеки комп’ютерних систем.
3. Поширені атаки комп’ютерні системи.
4. Типи атак на комп’ютерні системи
5. Моніторинг мережі і засоби моніторингу.
6. Атаки на базові функції.
7. Атаки на службові протоколи.
8. Захист мережі.
9. Управління доступом.

10. Захист кінцевих пристроїв.
11. Моніторинг безпеки.
12. Аналіз даних вторгнень
13. Реагування на інциденти і їх обробка.
14. Обробка інцидентів.

Рекомендовані джерела інформації

Основна література

1. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с.
2. 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

Додаткова література

1. Курс мережевої академії Cisco: CCNA Cybersecurity Operations. 2020. Режим доступу. https://www.netacad.com/courses/security/ccna-cybersecurity-operations
2. Anu, Vaibhav. Information security governance metrics: A survey and taxonomy. Information Security Journal: A Global Perspective31. 4, 2022. – pp. 466-478.
3. 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
4. Santos, Henrique MD. Cybersecurity: A Practical Engineering Approach. CRC Press, 2022. – 341 p.
5. Grubb S. How Cybersecurity Really Works. 2021. – 219 p.
6. Grimes, Roger A. *Hacking Multifactor Authentication*. John Wiley & Sons, 2020.

Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Інформаційна безпека» визначається як середньозважена величина, залежно від питомої ваги кожної складової залікового кредиту:

Модуль 1		Модуль 2	Модуль 3
40%	40%	5%	15%
Поточне оцінювання	Модульний контроль	Тренінг	Самостійна робота
Середнє арифметичне з оцінок, отриманих на заняттях по темах 1-14	Оцінка за модульну контрольну роботу	Оцінка за виконання тренінгу	Оцінка за виконання самостійної роботи

Будь-яке завдання, за яке студент отримав оцінку, яка його не задовольняє, може бути повторно перездано протягом наступних двох тижнів.

Незадовільну оцінку за заліковий модуль студент може перездати до здачі наступного модуля.

Шкала оцінювання:

За шкалою університету	За національною шкалою	За шкалою ECTS
90–100	відмінно	A (відмінно)
85–89	добре	B (дуже добре)

75-84		C (добре)
65-74	задовільно	D (задовільно)
60-64		E (достатньо)
35-59	незадовільно	FX (незадовільно з можливістю повторного складання)
1-34		F (незадовільно з обов'язковим повторним курсом)

Навчальні ресурси

№	Найменування
1.	**Обладнання:** проектор, комп'ютери з доступом до мережі Інтернету
2.	**Програмне забезпечення:** Cisco Packet Tracer, Oracle VirtualBox, образи віртуальних машин CyberOps, Security Onion, Kali Linux, вразливий сервер Metasploitable.

Політики курсу.

Академічна доброчесність. **Дотримання академічної доброчесності студентами передбачає**:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

- посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

- дотримання норм законодавства про авторське право і суміжні права;

- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

академічний плагіат - оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та/або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;

самоплагіат - оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;

фабрикація - вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;

фальсифікація - свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;

списування - виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання.

За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності:

- повторне проходження оцінювання (контрольна робота, іспит, залік тощо);

- повторне проходження відповідного освітнього компонента освітньої програми.

Політика запізнення. За несвоєчасно виконані завдання буде накладено штраф 10 відсотків від загальної кількості балів за це завдання. Примітка. Виключення можуть бути зроблені до невчасно зданих завдань з поважних причин.

Політика щодо відвідування: Відвідування занять є обов'язковим. За об'єктивних причин (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу.