Назва курсу	**«Системи та технології кібернетичної безпеки»**
Викладач (-і)	Яцків Василь Васильович
Контактний тел.	https://www.wunu.edu.ua/educational-subdivisions/fkit/department-kb-fkit/
E-mail:	+380352-475050 ext. 56501

Анотація до курсу. Основне завдання дисципліни дати студентам теоретичну та практичну підготовку з розгортання та використання систем та технологій кібернетичної безпеки.

Мета та цілі курсу.

Метою дисципліни «Системи та технології кібернетичної безпеки» є - отримання знань та умінь, які необхідні для розробки та використання систем виявлення та запобігання вторгнень.

Загальна інформація про дисципліну

Ступінь вищої освіти	**Бакалавр**
Спеціальність	**124 – Системний аналіз**
Курс (рік навчання)	**4**
Семестр	**7**
Нормативна \ вибіркова	**Вибіркова**
Загальна кількість кредитів	**5**

Перелік тем

1. Кібербезпека і центр моніторингу та управління безпекою (SOC).
2. Корпоративний SOC і послуги з управління інформаційною безпекою
3. Захист і аналіз кінцевих пристроїв.
4. Поверхні вразливі до атак.
5. Системи управління безпекою.
6. Моніторинг безпеки.
7. Джерела даних про безпеку.
8. Аналіз даних вторгнень.
9. Детермінований аналіз і імовірнісний аналіз.
10. Панелі управління і візуалізації.
11. Реагування на інциденти і їх обробка.
12. Ромбовидна модель.
13. Комп'ютерні групи реагування на надзвичайні ситуації (CERT).
14. Етапи виявлення та аналізу інцидентів.

Рекомендовані джерела інформації

Основна література

1. Akhgar B., Kavallieros D., Sdongos E. (Eds.) Technology Development for Security Practitioners. Springer, 2021. — 564 p.

2. Bhardwaj A., Sapra V. (Eds.) Security Incidents & Response Against Cyber Attacks. Springer, 2021. — 250 p.
3. Chapple M., Shelley J. IAPP CIPP / US Certified Information Privacy Professional Study Guide. Sybex, John Wiley & Sons, Inc., 2021. — 307 p.

Додаткова література

4. Di Pietro R., Raponi S., Caprolu M., Cresci S. New Dimensions of Information Warfare. Springer, 2021. — 262 p.
5. Karamagi Robert. Information Technology Security Planning and Management. Independently published, 2021. — 168 p.
6. Messier Ric. CEH v11 Certified Ethical Hacker Study Guide. Wiley, 2021. — 701 p.
7. Nielsen Aileen. Practical Fairness: Achieving Fair and Secure Data Models. O'Reilly Media, Inc., 2021. — 346 p.

Система оцінювання та вимоги.

Підсумковий бал (за 100-бальною шкалою) з дисципліни «Системи та технології кібернетичної безпеки» 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.	Електронний варіант лекцій
3.	Методичні вказівки до виконання лабораторних робіт

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.