Силабус курсу
СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

Ступінь вищої освіти – бакалавр
Рік навчання: 4
Семестр: 7
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Наталія Яцків
Контактна інформація	jng@wunu.edu.ua

Опис дисципліни

Курс "Системи та технології кібербезпеки" є важливою частиною, спрямованою на вивчення методів та інструментів, які використовуються для збереження приватності та захисту конфіденційної інформації в сучасному цифровому середовищі. Ця анотація надає огляд ключових аспектів та мету цього курсу.

Головні аспекти курсу включають наступне:

1. Конфіденційність даних: Курс розглядає концепції та принципи, пов'язані з конфіденційністю даних, включаючи поняття конфіденційності, доступу до даних та захисту особистої інформації.
2. Криптографія: Учасники вивчають основи криптографії та методи шифрування, що використовуються для захисту даних в публічних та приватних мережах.
3. Управління доступом: Курс охоплює питання управління доступом до інформації, включаючи роль ідентифікації, аутентифікації та авторизації в забезпеченні конфіденційності.
4. Практичні завдання: Учасники матимуть можливість застосовувати свої знання в практичних вправах та сценаріях, що допоможе закріпити отримані навички.

Цей курс призначений для студентів і фахівців, які цікавляться забезпеченням конфіденційності даних у цифровому світі. Він надає необхідний фаховий фундамент та практичні навички для забезпечення безпеки та конфіденційності важливої інформації в сучасному інформаційному суспільстві.

Метою дисципліни «Системи та технології кібербезпеки» є – здобуття компетентностей .

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Криптографії в реальному світі	Пояснювати симетричну та асиметричну криптографію	Поточне опитування
2/1	Хеш-функції	Розуміти властивості безпеки хеш-функції	Поточне опитування
2/1	Коди автентифікації повідомлень	Використовувати коди автентифікації повідомлень на практиці	Поточне опитування
2/1	Автентифіковане шифрування	Розуміти алгоритм шифрування AES-CBC-HMAC	Поточне опитування
2/1	Обмін ключами	Використовувати стандарти обміну ключами	Поточне опитування
2/1	Асиметричне шифрування та	Знати стандарти асиметричного та	Поточне

	гібридне шифрування	гібридного шифрування	опитування, тестування
2/1	Підписи та докази з нульовим знанням.	Розуміти докази з нульовим знанням	Поточне опитування
2/1	Захищені комунікації	Оцінювати стан зашифрованого Інтернету сьогодні	Поточне опитування
2/1	Наскрізне шифрування	Використовувати масштабування довіри між користувачами за допомогою мережі довіри	Поточне опитування
2/1	Аутентифікація користувача	Застосовувати симетричний обмін ключами з автентифікацією пароля з CPace	Поточне опитування
2/1	Криптографія в децентралізованих системах	Розуміти проблема стійкості та довіри	Поточне опитування
2/1	Апаратна криптографія	Знати модель сучасного криптографічного зловмисника	Поточне опитування
2/1	Постквантова криптографія	Постквантова криптографія, захист від квантових комп'ютерів	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Wong, D. *Real-world cryptography*. Simon and Schuster. 2021
2. Курс мережевої академії Cisco: CCNA Cybersecurity Operations. 2020. Режим доступу. https://www.netacad.com/courses/security/ccna-cybersecurity-operations
3. Інформаційна безпека. // Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. – 580.
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
30 %	40 %	30 %
1. Усне опитування на заняттях – max 7*3=21 бали. 2. Письмова робота – max 55 балів. 3. Практичне завдання – max 3*8=24 балів	1. Усне опитування на заняттях – max 5*4=20 балів. 2. Письмова робота – max 56 балів. 3. Практичне завдання – max 3*8=24 бали	1. Підготовка КПІЗ – max 30 балів. 2. Захист КПІЗ – max 40 балів. 3. Оцінка за тренінг – 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