Силабус курсу

ОСНОВИ КІБЕРБЕЗПЕКИ

Ступінь вищої освіти – бакалавр
Рік навчання: 1
Семестр: 1
Кількість кредитів: 8
Мова викладання: українська

Керівник курсу

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

Опис дисципліни

Курс "Основи кібербезпеки" - це вступний навчальний курс, спрямований на ознайомлення студентів та фахівців з основами та фундаментальними поняттями в галузі кібербезпеки. Ця анотація висвітлює ключові аспекти та мету цього курсу.

Головні аспекти курсу включають наступне:

1. Основи кібербезпеки: Курс надає студентам загальне уявлення про сутність кібербезпеки та її важливість в сучасному цифровому світі.
2. Загрози та ризики: Учасники дізнаються про різноманітні види кіберзагроз, включаючи хакерські атаки, віруси, фішинг, витік даних тощо, та вчаться оцінювати ризики для організацій та індивідів.
3. Захист інформації: Курс розглядає основні принципи та методи захисту інформації, включаючи шифрування, аутентифікацію, авторизацію та інші механізми.
4. Кібергігієна: Учасники навчаються про актуальні техніки та практики для виявлення та ліквідації кіберінцидентів.
5. Спостереження та моніторинг: Курс досліджує роль інструментів моніторингу та спостереження в процесі забезпечення кібербезпеки.
6. Практичні вправи: Учасники матимуть можливість застосовувати набуті знання в практичних вправах та сценаріях, що допоможе закріпити навички.

Цей курс є важливим вступом в сферу кібербезпеки та призначений для тих, хто прагне зрозуміти основи захисту від кіберзагроз та небезпек, що існують у цифровому світі. Він надає необхідну базу для подальшого вивчення та розвитку в цій важливій галузі.

Метою дисципліни «Основи кібербезпеки» є формування у студентів цілісного уявлення про спеціальність кібербезпека та базових знань в даній галузі.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/3	Кібербезпека - Світ експертів і злочинців	Класифікувати сучасні кіберзагрози та суб’єкти кіберзагроз	Поточне опитування
2/3	Куб кібербезпеки.	Пояснювати основні властивості інформації: конфіденційність, цілісність, доступність. Стани даних.	Поточне опитування
2/3	Засоби протидії кіберзлочинності	Розуміти: структуру керування IT безпекою; модель кібербезпеки ISO; використання моделі ISO для кібербезпеки; модель кібербезпеки ISO	Поточне опитування

2/3	Кібербезпека – загрози, вразливості та атаки	Класифікувати основні принципи та типи шкідливого програмного забезпечення.	Поточне опитування
2/3	Мистецтво обману	Пояснювати тактики соціальної інженерії та методи обману.	Поточне опитування
2/3	Типи кібератак	Описувати основні типи кібератак	Поточне опитування
3/3	Мистецтво захисту таємниць	Застосовувати симетричні та асиметричних методи шифрування	Поточне опитування,
2/3	Контроль доступу	Розуміти типи та стратегії контролю доступу	Поточне опитування
2/3	Приховування даних	Розуміти основні принципи стеганографія та обфускації даних	Поточне опитування, тестування
2/3	Мистецтво забезпечення цілісності	Знати властивості хешування та принципи зберігання паролів	Поточне опитування
2/3	Цифрові підписи. Сертифікати	Розуміти як працює технологія цифрового підпису	Поточне опитування
2/3	Забезпечення цілісності баз даних	Знати вимоги до цілісності баз даних	Поточне опитування
2/3	Концепція п’яти дев’яток	Застосовувати заходи для поліпшення доступності	Поточне опитування
4/3	Реагування на інциденти	Знати фази реагування на інциденти	Поточне опитування
2/3	Відновлення після катастроф	Уміти планувати відновлення після катастроф	Поточне опитування
4/3	Захист домену кібербезпеки	Знати способи захисту систем та пристроїв	Поточне опитування
2/3	Укріплення захисту серверів	Знати способи організації безпечного віддаленого доступу	Поточне опитування
2/3	Укріплення захисту мережі	Знати принципи роботи мережевого обладнання: комутаторів та маршрутизаторів	Поточне опитування
2/3	Фізична безпека	Знати підходи до організації фізичного контролю доступу	Поточне опитування
2/3	Як стати спеціалістом з кібербезпеки	Розуміти керівні принципи кібербезпеки. Кіберзакони та відповідальність. Мати розуміння етики роботи у кібербезпеці.	Поточне опитування, тестування

Рекомендовані джерела інформації

1. Курс мережевої академії Cisco: Основи кібербезпеки, 2024. Режим доступу: https://www.netacad.com/courses/cybersecurity-essentials?courseLang=uk-UA
2. 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
3. Інформаційна безпека. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. – 580 с.
4. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. – 128 с.
5. Stallings, W. Effective Cybersecurity: Understanding and Using Standards and Best Practices. Addison-Wesley. 2019. – 893 p.
6. Messier Ric. CEH v10 Certified Ethical Hacker Study Guide. John Wiley & Sons, 2019. – 584 p.
7. Yaacoub, Jean-Paul A., et al. A Survey on Ethical Hacking: Issues and Challenges. arXiv preprint arXiv:2103.15072, 2021.
8. Priyadarshini I. Introduction on cybersecurity. Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies, 2019.– P. 1-37

9. The NIST Cybersecurity Framework (CSF) 2.0 National Institute of Standards and Technology. This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29. February 26, 2024

10. National Institute of Standards and Technology Special Publication 800-53A Revision 5 Natl. Inst. Stand. Technol. Spec. Publ. 800-53A, Rev. 5, 733 pages (January 2022) CODEN: NSPUE2. This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53Ar5

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

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10 %	10 %	10 %	10 %	5 %	10 %	40 %
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 1	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-10.	Підсумкова письмова робота за темами №1-13.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №11-20.	Підсумкова письмова робота за темами №14-27	Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу.	Оцінка за даний модуль виставляється за виконання вибраного наскрізного завдання.	1. 20 тестів по 3 бали - max 60 балів. 2.Практичне завдання - max 40 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