Силабус курсу
КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

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

Керівник курсу

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

Опис дисципліни

Курс "**Кібербезпека та захист інформації**" спрямований на вивчення основних принципів, методів та інструментів забезпечення безпеки інформаційних систем. Студенти отримають знання про загрози та вразливості інформаційних ресурсів, методи їх виявлення, запобігання та реагування. Основні теми включають криптографію, захист мереж, управління доступом, тестування на проникнення, а також етичні та правові аспекти кібербезпеки. Курс поєднує теоретичні основи з практичними завданнями для розвитку навичок ефективного захисту інформації в реальних умовах.

Метою дисципліни «**Кібербезпека та захист інформації**» є формування у студентів системного розуміння основ кібербезпеки та захисту інформації, оволодіння знаннями, навичками та компетенціями для ідентифікації, аналізу та запобігання кіберзагрозам, розробки та впровадження ефективних заходів захисту інформаційних систем.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/0	Основи кібербезпеки	Розуміння базових понять і термінів кібербезпеки. Оцінювання ролі кібербезпеки в сучасному інформаційному суспільстві. Аналіз основних компонентів інформаційної безпеки.	Поточне опитування
2/0	Види захисту інформації	Знання різних підходів до захисту інформації (адміністративного, технічного, організаційного). Визначення переваг та обмежень кожного виду захисту. Вибір оптимальних методів захисту для різних сценаріїв.	Поточне опитування
2/0	Поняття конфіденційності, цілісності, доступності	Усвідомлення принципів тріади інформаційної безпеки (CIA). Аналіз взаємозв'язків між конфіденційністю, цілісністю та доступністю. Застосування цих принципів у розробці стратегій захисту інформації.	Поточне опитування

2/2	Шифрування як метод забезпечення конфіденційності	Розуміння принципів симетричного та асиметричного шифрування. Оцінювання ефективності шифрування для забезпечення конфіденційності. Практичне застосування алгоритмів шифрування.	Поточне опитування
4/2	Методи асиметричне шифрування	Знання ключових відмінностей між симетричним та асиметричним шифруванням. Оволодіння навичками роботи з алгоритмами RSA, ECC тощо. Вміння використовувати асиметричне шифрування для захисту даних.	Поточне опитування
4/2	Методи забезпечення цілісності	Визначення основних методів забезпечення цілісності даних (хешування, контрольні суми). Використання алгоритмів хешування для перевірки цілісності. Знання способів інтеграції цілісності в системи захисту.	Поточне опитування, Тестування
2/2	Цифрові підписи	Розуміння принципу роботи цифрових підписів. Застосування цифрових підписів для аутентифікації та забезпечення цілісності. Робота з інструментами для створення та перевірки цифрових підписів.	Поточне опитування
2/0	Принципи кібербезпеки	Усвідомлення ключових принципів кібербезпеки (мінімізація ризиків, багаторівневий захист). Аналіз стандартів та рекомендацій у сфері кібербезпеки. Практичне застосування принципів у розробці політик безпеки.	Поточне опитування
2/2	Кіберзагрози та кібератаки	Класифікація основних кіберзагроз та типів атак. Оцінка ризиків і впливу атак на інформаційні системи. Розробка стратегій протидії та реагування на атаки.	Поточне опитування
2/2	Кіберзлочини. Кібервійна. Кібероборона. Кібертероризм. Кіберрозвідка	Розуміння видів і характеру кіберзлочинів. Аналіз механізмів кібервійни, кібератаки та оборони. Вивчення ролі розвідки та аналітики у кіберзахисті.	Поточне опитування
2/0	Модель порушника	Знання концепції моделі порушника. Аналіз типових сценаріїв атак та методів порушників. Розробка заходів протидії на основі моделювання атак.	Поточне опитування
2/2	Поняття, сутність та основні завдання комплексної системи захисту інформації	Розуміння структури та функцій комплексної системи захисту інформації. Оцінка ефективності впроваджених систем захисту. Розробка та вдосконалення політик інформаційної безпеки.	Поточне опитування, тестування

2/0	Шкідливе програмне забезпечення	Класифікація видів шкідливого ПЗ Аналіз механізмів поширення та впливу шкідливого ПЗ. Розробка стратегій захисту від шкідливих програм.	Поточне опитування, тестування
2/0	Методи виявлення та боротьби з ШПЗ	Вивчення методів ідентифікації шкідливого ПЗ (сигнатурний, поведінковий аналіз). Використання антивірусного та аналітичного ПЗ. Розробка заходів реагування та відновлення після атак.	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

Підсумковий бал (за 100-бальною шкалою) з дисципліни «**Кібербезпека та захист інформації**» 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	Тренінги	Самостійна робота
Оцінка за даний модуль визначається як середнє арифметичне за захист практичних робіт №1-7.	Підсумкове модульне тестування за темами №1-14.	Визначається як середнє арифметичне з оцінок за виконання двох завдань тренінгу.	Визначається як оцінка за наскрізне завдання самостійної роботи.

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