**Силабус курсу**

# Інформаційна безпека

**Ступінь вищої освіти – бакалавр**
**Спеціальність – 015 Професійна освіта**
**Спеціалізація – 015.39 Цифрові технології**
**Освітньо–професійна програма – "Професійна освіта (Цифрові технології)"**

**Рік навчання:** 3, **Семестр:** I

**Кількість кредитів:** 5 **Мова викладання:** українська

## Керівник курсу


| | |
|---|---|
| **ПІП** | к.ф.-м.н., доцент Хома Надія Григорівна |
| **Контактна інформація** | n.khoma@wunu.edu.ua, +380352-475050 ext. 12 217 |


## Опис дисципліни

Метою вивчення дисципліни «Інформаційна безпека» розкриття сучасних методів захисту інформації в комп'ютерних системах та мережах, ознайомлення з особливостями їх програмної реалізації; у формуванні умінь та навичок для визначення місця і ролі інформаційної безпеки у загальній схемі національної безпеки, принципів забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації, необхідних для оволодіння навичками застосування методів і засобів безпекового поводження з інформацією в умовах використання новітніх інформаційних технологій.

Важливою складовою курсу є формування комплексу знань щодо підходів до визначення джерел загроз та об'єктів захисту, методів та механізмів захисту інформаційних ресурсів, нормативно-методичної бази в галузі захисту інформації, набуття студентом теоретичних знань та практичних навичок, необхідних для творчого підходу в питанні управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки та оперативного застосування заходів та засобів, спрямованих на технічний захист інформації на об'єктах інформаційної діяльності та у випадку інцидентів, швидкого відновлення працездатності систем.

В результаті вивчення навчальної дисципліни студенти повинні набути компетенцій ефективно реалізовувати знання у своїй практичній та професійній діяльності.

## Структура курсу

| № п/п | Тема | Результати навчання | Завдання |
|---|---|---|---|
| 1. | Основи інформаційної безпеки | Знати термінологію, володіти теоретичними основами для досягнення високого рівня професійної майстерності. Уміти класифікувати, систематизувати інформацію та правильно вибирати комп'ютерні засоби та програмне забезпечення для захисту інформації. | Тести, питання |
| 2. | Загрози інформаційній безпеці | Знати основні поняття, вміти визначати загрози доступності, цілісності, конфіденційності інформації та класифікувати загрози. Класифікувати сучасні загрози та суб'єкти загроз | Питання, тести |
| 3. | Безпека даних | Знати характеристики основних видів безпеки. Розуміти принципи забезпечення безпеки в інформаційній сфері. Вміти застосовувати модель CIA для вирішення задач забезпечення цілісності, доступності, конфіденційності | Питання, тести |
| 4. | Політика безпеки інформації | Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації | Питання, тести |
| 5. | Симетричні системи | Уміти застосовувати симетричні методи шифрування та перевіряти шифрування даних | Завдання, питання, тести |
| 6. | Асиметричні системи | Уміти застосовувати асиметричних методи шифрування та перевіряти шифрування даних | Завдання, питання, тести |
| 7. | Сучасні криптографічні протоколи | Розуміти як працює технологія цифрового підпису<br>Знати властивості хешування та принципи зберігання паролів | Завдання, питання, тести |
| 8 | Соціальна інженерія та фішинг | Володіти поняттям соціотехнічної системи та її властивостей, методів соціального інжинірингу. Знання основних алгоритмів соціотехнічних атак на інформаційні ресурси, етапів проведення. Вміти здійснювати захист інформації від соціотехнічних атак | Завдання, питання, тести |
| 9 | Управління ризиками та відповідальність | Здатність здійснювати професійну діяльність на основі впровадженої систем управління інформаційною безпекою. | Завдання, питання, тести |
| 10 | Концепція побудувати віртуальних приватних мереж VPN | Уміти використовувати віртуальні приватні мережі для віддаленого доступу користувачів до робочої мережі, для безпечного підключення різних відділів організації, для обходу блокування сайтів, для забезпечення анонімності | Завдання, питання, тести |

## Рекомендовані джерела інформації


1. 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
2. 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.
3. Вишняков В.М. Захист інформації в комп'ютерних системах: навч. посіб. Київ: КНУБА, 2022. 120 с.
4. Інформаційна безпека. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. 580 с.
5. Костюченко А.О., Горошко Ю.В. Віртуалізація операційних систем: навчально-методичний посібник. Ч.: ФОП Баликіна С.М., 2021. 56 с.
6. Методичні вказівки до виконання лабораторних робіт з курсу “Основи кібербезпеки” для студентів спеціальностей “Кібербезпека” / Укл.: Яцків В. В. Тернопіль: Економічна думка, 2018. 44 с.
7. Методичні вказівки до лабораторних робіт з дисципліни “Програмно-апаратне забезпечення та захист мобільних пристроїв” укл. Лаптєв О.А., Гришанович Т. О., Жолоб Я. В., Жигаревич О. К. [Електронний ресурс]; ВНУ імені Лесі Українки. Електронні текстові данні (1 файл: 859 КБ). Луцк. 2022. 99 с.
8. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
9. AlFardan, N. (2023). Cyber threat hunting. Manning, 2023. 442 p.
10. Adedoyin, F. F., & Christiansen, B. (2023). Effective cybersecurity operations for Enterprise-Wide systems. Information Science Reference. 2023. 344 p.
11. Alexandrou, A. (2021). Cybercrime and internet technology: Theory and Practice. CRC Press, 2022. 455p.
12. Dr. Hidaia Mahmood Alassouli. (2021). Common Windows, Linux and Web Server Systems Hacking Techniques, 2021. 171 p.


## Політика оцінювання

У процесі вивчення дисципліни «Інформаційна безпека» використовуються такі засоби оцінювання та методи демонстрування результатів навчання: стандартизовані тести; поточне опитування, виконання лабораторних робіт та їх захист; оцінювання результатів модульної контрольної роботи; залікове модульне тестування; презентації результатів виконаних завдань; оцінювання результатів самостійної роботи; модульна контрольна робота; екзамен.

*Політика щодо дедлайнів і 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 та екзаменів 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 он-лайн формі за погодженням із керівником курсу з дозволу дирекції факультету.

## Оцінювання

Підсумковий бал (за 100-бальної шкалою) з дисципліни «Інформаційнна безпека» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

| Модуль 1 | | Модуль 2 | | Модуль 3 | Модуль 4 | Модуль 5 |
|---|---|---|---|---|---|---|
| 10% | 10% | 10% | 10% | 5% | 15% | 40% |

| Поточне оцінювання | Модульна контрольна робота | Поточне оцінювання | Модульна контрольна робота | Тренінги | Самостійна робота | Екзамен |
|---|---|---|---|---|---|---|
| Оцінка визначається як середнє арифметичне з оцінок, отриманих на практичних заняттях (теми 1-5) | Письмова робота по темах 1-5 | Оцінка визначається як середнє арифметичне з оцінок, отриманих на практичних заняттях (теми 6-10) | Письмова робота по темах 6-10 | Оцінка визначається як середнє арифметичне з оцінок, отриманих на тренінгу | Оцінка визначається як середнє арифметичне з оцінок, отриманих за написання реферату, виступ та захист | 1. Тестові завдання (2 тестів по 2 бали) – max 40 балів<br>2. Практичні завдання (2) – max 60 балів. |

**Шкала оцінювання:**

| **За шкалою ЗУНУ** | **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) |