МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЕКОНОМІКО-ТЕХНОЛОГІЧНИЙ ІНСТИТУТ ІМЕНІ Р.ЕЛЬВОРТІ

Кафедра інформаційних технологій

"ЗАТВЕРДЖУЮ"
Завідувач кафедри

_____/О.П. Бондар/
30 серпня 2024 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

# «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА КІБЕРБЕЗПЕКА»

Спеціальність: 122 Комп'ютерні науки

Освітньо-професійна програма: Комп'ютерні науки

| Нормовані дані / Форма навчання | Курс | Семестр | Всього годин за планом | Кількість кредитів ECTS | Всього аудит (год.) | Аудиторних годин, (у тому числі КЗ) | | | Самостійна робота (год.) | Курсове проектування (семестр/ кредити) | Контрольний підсумок (семестр) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Лекції | Лабораторні роботи | Практичні заняття | | | Екзамен | Залік |
| Денна | 2 | 2 | 120 | 4 | 72 | 36 | 36 | 0 | 48 | | 4 | |

Кропивницький 2024 рік

Робочу програму складено на основі освітньо-професійної програми за спеціальністю: 122 Комп'ютерні науки

Робочу програму складено: викладач Сурков К.Ю.

Робочу програму затверджено на засіданні кафедри інформаційних технологій.

Протокол № 1 від "30" серпня 2024 року

Завідувач кафедри _____ /О.П. Бондар/

«30» 08 2024 р.

Схвалено Вченою радою ЕТІ ім. Р.Ельворті

Протокол № 15 від "24" вересня 2024 року

Голова Вченої ради _____ /Штець Т.Ф./

© Сурков К.Ю., 2024 рік

# 1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, ступінь вищої освіти</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 4</td><td rowspan="5">Галузь: 12– Комп’ютерні науки Спеціальність або освітня програма 122 Комп’ютерні науки</td><td colspan="2">Статус дисципліни нормативна</td></tr>
<tr><td colspan="2">Рік підготовки</td></tr>
<tr><td>Змістових модулів -</td><td>2</td><td></td></tr>
<tr><td>Індивідуальне завдання студента</td><td colspan="2">Семестр</td></tr>
<tr><td>Загальна кількість годин -120</td><td>4</td><td></td></tr>
<tr><td rowspan="12">Тижневих годин для денної форми навчання: аудиторних:<br>4 семестр – 4 години</td><td rowspan="12">Ступінь вищої освіти: бакалавр</td><td colspan="2">Лекції (год.)</td></tr>
<tr><td>36</td><td></td></tr>
<tr><td colspan="2">Практичні, семінарські (год.)</td></tr>
<tr><td>-</td><td></td></tr>
<tr><td colspan="2">Лабораторні (год.)</td></tr>
<tr><td>36</td><td>-</td></tr>
<tr><td colspan="2">Самостійна робота (год.)</td></tr>
<tr><td>48</td><td></td></tr>
<tr><td colspan="2">Індивідуальне завдання (год.)</td></tr>
<tr><td>-</td><td>-</td></tr>
<tr><td colspan="2">Вид контролю:</td></tr>
<tr><td>4 сем – екзамен</td><td></td></tr>
</table>

## Примітка.

Співвідношення кількості годин аудиторних занять та самостійної роботи становить (%): 60% до 40% .

### 2. Мета та завдання навчальної дисципліни

2.1. МЕТА ВИКЛАДАННЯ ДИСЦИПЛІНИ

Інформаційна безпека та кібербезпека є ключовими аспектами сучасних інформаційних технологій. Оволодіння технологіями захисту інформації є необхідною передумовою для створення безпечних інформаційних систем та ефективного протистояння кіберзагрозам.

Метою викладання дисципліни є формування у студентів знань і навичок щодо захисту інформації, зокрема оволодіння основами інформаційної безпеки, технологіями захисту мережевої інфраструктури, принципами структурної організації та архітектури комп'ютерних систем, а також методами забезпечення безпеки в телекомунікаційних та комп’ютерних мережах.

2.2. ЗАВДАННЯ ВИВЧЕННЯ ДИСЦИПЛІНИ

Вивчення теоретичних основ захисту інформації та кібербезпеки, ознайомлення з основними методами і засобами забезпечення інформаційної безпеки, оволодіння сучасними технологіями захисту даних, мережевої інфраструктури та комп’ютерних систем, а також аналізу вразливостей та оцінки ризиків у сфері кібербезпеки.

2.3. За результатами вивчення дисципліни здобувач повинен опанувати наступні компетентності:

**Інтегральна компетентність**. Здатність розв’язувати складні спеціалізовані задачі та

практичні проблеми у галузі комп'ютерних наук або у процесі навчання, що передбачає застосування теорій та методів інформаційних технологій і характеризується комплексністю та невизначеністю умов.

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК2. Здатність застосовувати знання у практичних ситуаціях.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.

ЗК6. Здатність вчитися й оволодівати сучасними знаннями.

ЗК7. Здатність до пошуку, оброблення та аналізу інформації з різних джерел

ЗК13. Здатність діяти на основі етичних міркувань.

СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури.

*СК19. Здатність застосовувати технології та інструментальні засоби для створення інтерактивних веб-додатків та інтеграції бекенд-функціоналу, розробки адаптивного дизайну, забезпечувати конфіденційність даних.*

2.4. За результатами вивчення навчальної дисципліни студент повинен:

**знати:**

- основи захисту інформації, принципи конфіденційності, цілісності та доступності даних;
- методи криптографічного захисту інформації та основи криптоаналізу;
- механізми автентифікації, контролю доступу та управління правами користувачів;
- сучасні технології захисту мережевої інфраструктури, телекомунікаційних та комп'ютерних мереж;
- види кіберзагроз, методи їх виявлення та протидії;
- правові та організаційні аспекти інформаційної безпеки та кібербезпеки.

**вміти:**

- застосовувати сучасні методи та засоби захисту інформації у комп'ютерних системах і мережах;
- аналізувати вразливості інформаційних систем та оцінювати ризики кібербезпеки;
- використовувати криптографічні алгоритми для забезпечення безпеки даних;
- налаштовувати засоби автентифікації, управління доступом та моніторингу інформаційної безпеки;
- виявляти та протидіяти кіберзагрозам, застосовуючи методи етичного хакінгу та тестування на проникнення.

2.5. Програмні результати навчання

ПР1. Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.

ПР9. Розробляти програмні моделі предметних середовищ, вибирати парадигму програмування з позицій зручності та якості застосування для реалізації методів та алгоритмів розв'язання задач в галузі комп'ютерних наук.

ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.

*ПР20. Застосовувати технології та інструментальні засоби для створення інтерактивних веб-додатків та інтеграції бекенд-функціоналу, розуміти принципи розробки адаптивного дизайну та забезпечення конфіденційності даних.*

**2.6. Структурно-логічне місце дисципліни в освітній програмі**

| Попередні дисципліни: | Наступні дисципліни: |
|---|---|
| Теорія алгоритмів | Хмарні технології |
| Програмування | Комп'ютерні мережі |
| Операційні системи та системне програмування | |

Програма навчальної дисципліни складається з 2 модулів

## 3. Програма навчальної дисципліни

**Змістовий модуль 1. Моделі, механізми та засоби забезпечення інформаційної та кібербезпеки**

**Тема 1.1. Законодавча та нормативно-правова база України в галузі інформаційної та кібербезпеки**

1. Основні закони України у сфері інформаційної безпеки (Закон України «Про інформацію», «Про захист інформації в ІКС», «Про кібербезпеку»)
2. Регулювання захисту персональних даних (Закон України «Про захист персональних даних»)
3. Вимоги до систем захисту інформації (ДСТУ, НД ТЗІ, державні стандарти та нормативи)

**Тема 1.2. Міжнародні стандарти в галузі інформаційної та кібербезпеки**

1. Міжнародні стандарти управління інформаційною безпекою (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 15408)
2. Регламенти ЄС та роль міжнародних організацій (GDPR, NIST, ENISA)
3. Методи оцінки ризиків та забезпечення відповідності стандартам безпеки

**Тема 1.3. Моделі безпеки в інформаційній та/або кібербезпеці**

1. Модель порушника
2. Модель загроз
3. Модель вразливостей

**Тема 1.4. Інструментальні та прикладні застосунки в інформаційній та кібербезпеці**

1. Програмно-апаратні засоби захисту інформації (файрволи, антивірусні системи, системи виявлення вторгнень)
2. Засоби аналізу уразливостей та тестування на проникнення (Metasploit, Nmap, Wireshark)
3. Інструменти цифрової криміналістики та моніторингу подій безпеки

**Тема 1.5. Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ)**

1. Антивіруси
2. Міжмережеві екрани
3. IDS, IPS
4. Системи контролю та управління доступом у мережі (Active Directory, ACL)
5. Системи контролю та управління фізичним доступом (СКУД)

**Тема 1.6. Механізми безпеки комп'ютерних мереж**

1. Віртуальні приватні мережі (VPN)
2. Протоколи автентифікації RADIUS
3. Протоколи SSL/TLS

**Тема 1.7. Моделі загроз та моделі порушника**

1. Загальні визначення й поняття моделі загроз та моделі порушника
2. Загрози цілісності
3. Загрози доступності
4. Загрози конфіденційності
5. Загрози автентичності
6. Загрози через технічні канали
7. Загрози через соціальну інженерію

**Змістовий модуль 2. Криптографічні системи та методи захисту інформації**

**Тема 2.1. Симетричні криптосистеми**
1. Модель симетричної криптосистеми
2. Класичні методи шифрування: Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування
3. Блокові шифри
4. Потокові шифри

**Тема 2.2. Несиметрична (асиметрична, з відкритим ключем) криптографія**
1. Модель асиметричної криптосистеми
2. Шифр RSA
3. Алгоритм Ель-Гамаля (EG)
4. Генерація спільних секретів Діффі-Хеллмана (DH)
5. Електронний цифровий підпис DSA
6. Криптографія на еліптичних кривих
7. Електронний цифровий підпис

**Тема 2.3. Криптографічні протоколи**
1. Протоколи захисту мережевого трафіку IPSec
2. Протоколи безпечної передачі даних прикладного рівня: https

**Тема 2.4. Цифрова стеганографія**
1. Поняття цифрової стеганографії
2. Модель стеганосистеми та класифікація методів стеганографічного захисту
3. Основні вимоги до стеганосистеми
4. Відкриті, напівзакриті, закриті стеганосистеми
5. Поняття ЦВЗ, класифікація
6. Метод модифікації найменшого значущого біта та інші методи приховання даних у зображенні, відео та аудіо
7. Атаки на стеганосистеми

**Тема 2.5. Методи і засоби обробки інформації**
1. Методи шифрування та хешування даних (AES, RSA, SHA, MD5)
2. Алгоритми стиснення та кодування інформації (Хаффман, LZW, код Хеммінга)
3. Методи захисту інформації під час передачі та зберігання (VPN, цифрові підписи, PKI)

## 4. Структура навчальної дисципліни

| Назви змістових модулів і тем | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | усього | у тому числі | | | | |
| | | л | п | лаб | інд | с.р. |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Змістовий модуль 1. Моделі, механізми та засоби забезпечення інформаційної та кібербезпеки** | | | | | | |
| **Законодавча та нормативно-правова база України в галузі інформаційної** | **7** | **1** | | | | **6** |

| | | | | | | |
|---|---|---|---|---|---|---|
| **та кібербезпеки** | | | | | | |
| **Міжнародні стандарти в галузі інформаційної та кібербезпеки** | **5** | **1** | | | | **4** |
| **Моделі безпеки в інформаційній та/або кібербезпеці** | **10** | **4** | | **4** | | **2** |
| **Інструментальні та прикладні застосунки в інформаційній та кібербезпеці** | **9** | **1** | | | | **8** |
| **Програмні та програмно-апаратні комплекси засобів захисту інформації (ЗЗІ)** | **9** | **3** | | **4** | | **2** |
| **Механізми безпеки комп'ютерних мереж** | **14** | **4** | | **6** | | **4** |
| **Моделі загроз та моделі порушника** | **10** | **4** | | **4** | | **2** |
| **Разом за змістовим модулем 1** | **64** | **18** | | **18** | | **28** |
| **Змістовий модуль 2. Криптографічні системи та методи захисту інформації** | | | | | | |
| **Симетричні криптосистеми** | **14** | **6** | | **4** | | **4** |
| **Несиметрична (асиметрична, з відкритим ключем) криптографія** | **16** | **6** | | **6** | | **4** |
| **Криптографічні протоколи** | **8** | **2** | | **4** | | **2** |
| **Цифрова стеганографія** | **11** | **3** | | **4** | | **4** |
| **Методи і засоби обробки інформації** | **7** | **1** | | | | **6** |
| **Разом за змістовим модулем 2** | **56** | **18** | | **18** | | **20** |
| **Разом** | **120** | **36** | | **36** | | **48** |

## 5. Теми семінарських занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Не передбачено | |

## 6. Теми практичних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Не передбачено | |

## 7. Теми лабораторних занять

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| **Змістовий модуль 1. Моделі, механізми та засоби забезпечення інформаційної та кібербезпеки _____** | | **18** |
| 1. | Розгортання операційної системи для проведення аудиту кібербезпеки комп’ютерних мереж та систем | 4 |
| 2. | Сніфери | 4 |
| 3. | Засіб дослідження вразливостей бездротових мереж Wi-Fi – Aircrack | 6 |
| 4. | Пошук вразливостей та чутливої інформації у відкритих джерелах за допомогою засобу Maltego | 4 |
| **Змістовий модуль 2. Криптографічні системи та методи захисту інформації** | | 18 |
| 5. | Енкодери | 4 |

| | | |
|---|---|---|
| 6 | Збір інформації за допомогою Metasploit | 6 |
| 7. | Пошук вразливостей за допомогою Metasploit | 4 |
| 8. | Експлуатація вразливостей | 4 |
| | **Разом** | **36** |

## 8. Самостійна робота

| № з/п | Назва теми | Кількість годин |
|---|---|---|
| 1 | Законодавча та нормативно-правова база України в галузі інформаційної та кібербезпеки | 6 |
| 2 | Міжнародні стандарти в галузі інформаційної та кібербезпеки | 4 |
| 3 | Інструментальні та прикладні застосунки в інформаційній та кібербезпеці | 8 |
| 4 | Методи і засоби обробки інформації | 6 |
| 5 | Опрацювання лекцій та підготовка до практичних занять | 24 |
| | **Разом** | **48** |

## 9. Індивідуальні завдання

Не передбачено

## 10. Методи навчання

Лекції із застосуванням мультимедійних технологій, практичні заняття для формування навичок забезпечення інформаційної безпеки, лабораторні роботи з налаштування засобів захисту інформації та кібербезпеки, аналізу вразливостей і тестування систем, а також консультації для поглиблення теоретичних знань і відпрацювання практичних навичок.

## 11. Методи контролю

Оцінювання якості знань студентів здійснюється шляхом поточного, підсумкового (семестрового) контролю за 100-бальною шкалою оцінювання, за шкалою ECTS та національною шкалою оцінювання.

**Поточний контроль -** оцінювання засвоєння студентом навчального матеріалу під час проведення практичних занять, виконання індивідуальних домашніх завдань, консультацій. Результати поточного контролю заносяться в журнал у балах (5, 4, 3, 2, 1). Сума балів за поточний контроль максимально дорівнює 60.

**Підсумковий (семестровий) контроль** – комплексне оцінювання якості засвоєння навчального матеріалу дисципліни на екзамені. Сума балів за екзамен максимально дорівнює 40.

## 12. Розподіл балів, які отримують студенти

| Поточне оцінювання та самостійна робота | | | | | | | | | | Екзамен | Сума |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Змістовий модуль 1 | | | | | Змістовий модуль 2 | | | | | | |
| ЛБ1 | ЛБ2 | ЛБ3 | ЛБ4 | МКР1 | ЛБ5 | ЛБ6 | ЛБ7 | ЛБ8 | МКР2 | | |
| 5 | 5 | 5 | 5 | 10 | 5 | 5 | 5 | 5 | 10 | 40 | 100 |
| 30 | | | | | 30 | | | | | | |

## Шкала оцінювання: національна та ECTS

| Сума балів за всі види навчальної діяльності | Оцінка ECTS | Оцінка за національною шкалою | |
|---|---|---|---|
| | | для екзамену, курсового проекту (роботи), практики | для заліку |
| 90 – 100 | **A** | відмінно | |

| | | | |
|---|---|---|---|
| 82-89 | **B** | добре | зараховано |
| 74-81 | **C** | | |
| 64-73 | **D** | задовільно | |
| 60-63 | **E** | | |
| 35-59 | **FX** | незадовільно з можливістю повторного складання | не зараховано з можливістю повторного складання |
| 0-34 | **F** | незадовільно з обов'язковим повторним вивченням дисципліни | не зараховано з обов'язковим повторним вивченням дисципліни |

## 13. Методичне забезпечення

1. Навчально-методичний комплекс.
2. Тексти лекцій (в електронному варіанті).

## 14. Рекомендована література

### Основна


1. Остапов С.Е. , Євсеєв С.П. , Король О.Г. Кібербезпека: сучасні технології захисту., 2023 р. -678 с.
2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки: навч. посіб. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.


### Допоміжна


1. **Kevin Beaver.** Hacking for Dummies. John Wiley & Sons. 2022
2. **Alex Matrosov, Eugene Rodionov, Sergey Bratus.** Rootkits and Bootkits. No Starch Press. 2020.


## 15. Інформаційні ресурси

1. Онлайн-курси Coursera. – URL: https://www.coursera.org 77.
2. Академія Cisco. – URL: https://www.netacad.com
3. Он-лайн ресурс з кібербезпеки. – URL: https://thehackernews.com/