МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

**ЗАТВЕРДЖУЮ**
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«__» _____ 2024 р.

**ЗАТВЕРДЖУЮ**
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«__» _____ 2024 р

# РОБОЧА ПРОГРАМА

з дисципліни

# «КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ»

ступінь вищої освіти - **бакалавр**
галузь знань - **12 - «Інформаційні технології»**
спеціальність – **125 - «Кібербезпека»**
освітньо-професійна програма – **«Кібербезпека»**

Кафедра кібербезпеки

| Форма навчання | Курс | Семестр | Лекції (год.) | Лабор. (семін.) (год.) | ІРС (год.) | Тренінг (год) | СРС (год.) | Разом (год.) | Екзамен (сем) |
|---|---|---|---|---|---|---|---|---|---|
| Денна | 4 | 8 | 30 | 30 | 4 | 8 | 78 | 150 | 8 |

30.08.2024

Тернопіль – 2024

Робоча програма розроблена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», затвердженої Вченою радою ЗУНУ (протокол № 9 від 26.05.2021р).

Робочу програму склали доцент кафедри кібербезпеки, к.т.н., доцент Тарас Цаволик, викладач кафедри кібербезпеки Володимир Драпак.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол №1 26.08.2024 р.

Завідувач кафедри
кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол № 1 від 30.08.2024 р.

Керівник групи
забезпечення спеціальності Василь ЯЦКІВ

Гарант ОП Михайло КАСЯНЧУК

## СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

### 1. Опис дисципліни „Комплексні системи захисту інформації”

| Дисципліна – Комплексні системи захисту інформації | Галузь знань, спеціальність, СВО | Характеристика навчальної дисципліни |
|---|---|---|
| Кількість кредитів – 5 | Галузь знань<br>12 «Інформаційні технології» | Статус дисципліни – обов’язкова<br>Мова навчання - українська |
| Кількість залікових модулів – 5 | Спеціальність<br>125 «Кібербезпека» | Рік підготовки: 4<br>Семестр: 8 |
| Кількість змістових модулів –3 | | Лекції: 30 год<br>Лабораторні заняття: 30 год. |
| Загальна кількість годин денна – 150 год. | | СРС: 78 год, тренінг – 8 год.<br>Індивідуальна робота -4 год. |
| Тижневих годин: 19 год., з них аудиторних – 6 год. | Ступінь вищої освіти – бакалавр | Вид підсумкового контролю – екзамен |

### 2. Мета й завдання вивчення дисципліни „ Комплексні системи захисту інформації”

**2.1. Мета завдання дисципліни**

Метою викладання дисципліни “Комплексні системи захисту інформації” є навчання студентів принципам побудови комплексних систем захисту інформації на основі синтезу організаційних і технічних заходів щодо забезпечення захисту інформації з обмеженим доступом, основ ведення електронного документообігу в умовах сучасних кіберзагроз та витоку технічними каналами, забезпечення захисту інформації від несанкціонованого доступу на основі вимог міжнародних стандартів з інформаційної безпеки, державних нормативних документів з технології захисту інформації.

**2.2 Завдання вивчення дисципліни полягає у**:

- ознайомленні студентів із головними питаннями курсу;
- викладенні студентам у відповідності з програмою та робочим планом основних питань курсу «Комплексні системи захисту інформації»;
- формуванні у студентів цілісної системи теоретичних знань з курсу «Комплексні системи захисту інформації».

**2.3.Найменування та опис компетентностей, формування котрих забезпечує вивченя дисципліни**

– Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах.

– Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

– Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.)

**2.4 Передумови для вивчення дисципліни.**

Вивчення курсу „Комплексні системи захисту інформації” передбачає наявність систематичних та ґрунтовних знань із суміжних дисциплін («Основи кібербезпеки», «Криптографія»), а також цілеспрямованої роботи на лекційних та практичних заняттях, самостійної роботи студентів.

**2.5. Результати навчання**

1) Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій.

2) Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно телекомунікаційних системах.

3) Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

4) Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків

5) Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

6) Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.

7) Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

Предмет навчальної дисципліни " Комплексні системи захисту інформації " включає в себе розгляд теоретичних та правових аспектів проектування та створення криптонадійних систем, вивчення компонент систем захисту інформації, опанування алгоритмів кодування та шифрування інформації з метою подальшого проектування та створення криптостійких систем.

**2.6 Завдання лекційних занять**

Проведення лекційних занять забезпечує викладення методологічних основ комплексних систем захисту інформації у відповідності з програмою та робочим планом та формуванні у студентів цілісної системи теоретичних знань з курсу «Комплексні системи захисту інформації».

**2.7. Завдання проведення практичних занять**

Проведення практичних занять забезпечує формування у студентів практичних навичок щодо визначення джерел та наслідків дестабілізуючого впливу на інформацію та способів їх попередження та усунення. Здатність моделювання, технологічної побудови, кадрового забезпечення КСЗІ.

## 3. Програма навчальної дисципліни „ Комплексні системи захисту інформації ”

### *Змістовний модуль 1. Завдання та методологічні основи КСЗІ.*

**Тема 1. Сутність і завдання комплексної системи захисту інформації**

1.1. Поняття комплексної системи захисту інформації
1.2. Сутність комплексної системи захисту інформації
1.3. Призначення комплексної системи захисту інформації
1.4. Принципи побудови комплексної системи захисту інформації
1.5. Цілі системного підходу до захисту інформації
1.6. Стратегії захисту інформації
1.7. Розробка політики безпеки підприємства
1.8. Основні вимоги, що пред'являються до комплексної системи захисту інформації

Література: [1], с. 5-20, 34-39, [5], с. 1–10, [7]

**Тема 2. Методологічні основи комплексної системи захисту інформації**

2.1. Основні поняття теорії захисту інформації
2.2. Методологія захисту інформації як теоретичний базис комплексної системи захисту інформації
2.3. Основні поняття теорії систем
2.4. Системний аналіз і системний підхід
2.5. Основні системні уявлення

Література: [1-15]

### *Змістовний модуль 2. Інформація, як основне джерело захисту.*

**Тема 3. Визначення складу інформації, що захищається**

3.1. Методика визначення складу інформації, що захищається
3.2. Класифікація інформації за видами таємниці і ступенями конфіденційності
3.3. Визначення об'єктів захисту
3.4. Сховища носіїв інформації як об'єкт захисту
3.5. Методи оцінки захищеності підприємства

Література: [1], с. 5–60, [3], с. 18–27

**Тема 4. Джерела, способи і результати дестабілізуючого впливу на інформацію**

4.1. Оцінка загроз безпеки інформації

4.2. Явища, фактори і умови дестабілізуючого впливу на захищає інформацію
4.3. Джерела дестабілізуючого впливу на інформацію
4.4. Види і способи дестабілізуючого впливу на інформацію з боку людей
4.5. Види і способи дестабілізуючого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ
4.6. Визначення причин, обставин і умов дестабілізуючого впливу на інформацію з боку людей
4.7. Причини, обставини і умови дестабілізуючого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ
Література: [1], с. 5–60, [3], с. 18–27, [26,27]

***Змістовний модуль 3. Моделювання, технологічна побудова, кадрове забезпечення КСЗІ***

**Тема 5. Канали і методи несанкціонованого доступу до інформації**
5.1. Методика виявлення каналів несанкціонованого доступу до інформації
5.2. Визначення можливих методів несанкціонованого доступу до інформації, що захищається
5.3. Ділова розвідка як канал несанкціонованого доступу для отримання інформації
5.4. Інформаційний продукт як наслідок реалізації несанкціонованих дій
5.5. Модель потенційного порушника
Література: [2], с. 4–26, [8], с. 11–57, [26,27]

**Тема 6. Моделювання процесів комплексної системи захисту інформації**
6.1. Поняття моделі об'єкта. Моделювання як інструмент аналізу об'єкта КСЗІ
6.2. Значення моделювання процесів КСЗІ
6.3. Архітектурне побудова комплексної системи захисту інформації
Література: [2], с. 4–26, [8], с. 11–57, [26,27]

**Тема 7. Технологічна побудова комплексної системи захисту інформації**
7.1. Технологічне побудова організаційної системи КСЗІ
7.2. Структура організаційної системи підприємства
7.3. Загальний вміст робіт з проектування КСЗІ
7.4. Основні стадії проектування КСЗІ
7.5. Фактори, що впливають на вибір складу КСЗІ
7.6. Модель системи автоматизованого проектування захисту інформації
Література: [2], с. 4–26, [8], с. 11–57, [26,27]

**Тема 8. Кадрове забезпечення комплексної системи захисту інформації**
8.1. Кадрова політика підприємства при створенні КСЗІ
8.2. Етапи роботи з персоналом
8.3. Комплексний захист інформації та персонал
8.4. Мотивація
8.5. Розробка кодексу корпоративної поведінки
Література: [2], с. 4–26, [8], с. 11–57, [9-15]

***Змістовний модуль 4. Нормативно-методичне забезпечення та планування діяльності КСЗІ.***

**Тема 9. Нормативно-методичне забезпечення КСЗІ**
9.1. Значення нормативно-методичного забезпечення
9.2. Склад нормативно-методичного забезпечення
9.3. Порядок розробки і впровадження документів підприємства
Література: [9], с. 3–47, [5], с. 6–40, [6-15]

**Тема 10. Управління комплексною системою захисту інформації**
10.1. Загальні закони кібернетики
10.2. Сутність організації процесів управління КСЗІ
10.3. Технологія організаційного управління КСЗІ
10.4. Структуризація процесів технології управління
10.5. Вимоги до системи управління як об'єкту дослідження
10.6. Основи методології прийняття управлінського рішення
10.7. Загальні вимоги до прийняття управлінського рішення
10.8. Роль психологічної теорії прийняття управлінського рішення
Література: [9], с. 3–47, [5], с. 6–40, [6-15]

**Тема 11. Планування діяльності комплексної системи захисту інформації**

11.1. Цілі планування діяльності КСЗІ

11.2. Принципи планування

11.3. Способи планування

11.4. Основні положення розроблення плану

11.5. Стадії планування

11.6. Контроль діяльності

Література: [9], с. 3–47, [5], с. 6–40, [6-15]

**Тема 12. Управління комплексною системою захисту інформації в умовах надзвичайних ситуацій**

12.1. Поняття і основні види надзвичайних ситуацій

12.2. Технологія прийняття рішення в умовах надзвичайної ситуації

12.3. Фактори, що впливають на прийняття рішення

12.4. Забезпечення управління КСЗІ в умовах надзвичайних ситуацій

12.5. Підготовка заходів на випадок виникнення надзвичайної ситуації

Література: [9], с. 3–47, [5], с. 6–40, [6-15]

**4. Структура залікового кредиту дисципліни „Комплексні системи захисту інформації”**

| | Кількість годин | | | | | |
|---|---|---|---|---|---|---|
| | Лекції | Лабор. заняття | СРС | ІРС | Тренінг | Контрольні заходи |
| Змістовий модуль 1. Завдання та методологічні основи КСЗІ | | | | | | |
| Тема 1. Сутність і завдання комплексної системи захисту інформації | 2 | 2 | 6 | 1 | 2 | Поточне опитування |
| Тема 2. Методологічні основи комплексної системи захисту інформації | 2 | 2 | 6 | | | |
| Змістовний модуль 2. Інформація, як основне джерело захисту. | | | | | | |
| Тема 3. Визначення складу інформації, що захищається | 3 | 2 | 6 | 1 | 1 | Поточне опитування |
| Тема 4. Джерела, способи і результати дестабілізуючого впливу на інформацію | 2 | 3 | 6 | | | |
| Змістовний модуль 3. Моделювання, технологічна побудова, кадрове забезпечення КСЗІ | | | | | | |
| Тема 5. Канали і методи несанкціонованого доступу до інформації | 2 | 2 | 6 | 1 | 2 | Поточне опитування |
| Тема 6. Моделювання процесів комплексної системи захисту інформації**.** | 3 | 3 | 6 | | | |
| Тема 7. Технологічна побудова комплексної системи захисту інформації | 2 | 2 | 7 | | | |
| Тема 8. Кадрове забезпечення комплексної системи захисту інформації | 2 | 2 | 7 | | | |
| Змістовний модуль 4. Нормативно-методичне забезпечення та планування діяльності КСЗІ | | | | | | |
| Тема 9. Нормативно-методичне забезпечення КСЗІ | 3 | 2 | 7 | 1 | | Поточне опитування |
| Тема 10. Управління комплексною системою захисту інформації | 3 | 2 | 7 | | 1 | |
| Тема 11. Планування діяльності комплексної системи захисту інформації | 3 | 2 | 7 | | 1 | |
| Тема 12. Управління комплексною системою захисту інформації в умовах надзвичайних ситуацій. | 3 | 2 | 7 | | 1 | |
| Разом | 30 | 30 | 78 | 4 | 8 | |

**5. Тематика лабораторних робіт.**

**Лабораторна робота 1. Дослідження системи аналізу ризиків та перевірки політики інформаційної безпеки підприємства**

**Мета роботи:** Проведення дослідження системи аналізу ризиків та перевірки політики інформаційної безпеки підприємства

1. Огляд програмних продуктів в області аналізу ризиків та перевірки організаційних заходів забезпечення інформаційної безпеки
2. Опис системи
3. Інтерфейс системи

Література:1-15

**Лабораторна робота 2. Дослідження захищеності бездротових мереж передачі даних**

**Мета роботи:** Проведення дослідження захищеності бездротових мереж передачі даних

1. Мета роботи
2. Короткі теоретичні відомості
3. Порядок виконання роботи

Література:1-15

**Лабораторна робота 3. Дослідження і адміністрування коштів забезпечення інформаційної безпеки Web-сервера Microsoft IIS Server.**

**Мета роботи:** Ознайомитися, дослідити і адмініструвати кошти забезпечення інформаційної безпеки Web-сервера Microsoft IIS Server

1. Мета роботи
2. Короткі теоретичні відомості
3. Порядок виконання роботи

Література:1-15

**Лабораторна робота 4. Дослідження і адміністрування коштів забезпечення інформаційної безпеки Microsoft ISA Security Server. Встановлювати чи налаштовувати брандмауера ISA. Побудова VPN-мережі на базі ISA**

**Мета роботи:** Забезпечення інформаційної безпеки Microsoft ISA Security Server. Встановлення чи налаштування брандмауера ISA. Побудова VPN-мережі на базі ISA

1. Мета роботи
2. Короткі теоретичні відомості
3. Порядок виконання роботи

Література:1-15

**Лабораторна робота №5 Дослідження структури об’єкту захисту**

**Мета роботи:** Придбання теоретичних знань та практичних навичок з аналізу структури об’єкта захисту.

1. Короткі теоретичні відомості.
2. Завдання на виконання лабораторної роботи

Література:1-15

**Лабораторна робота №6. Ідентифікація небезпечних чинників на об’єкт захисту**

**Мета роботи:** Придбання опанування практичних навичок з визначення та ідентифікації загроз для заданого об’єкта захисту.

1. Хід роботи
2. Завдання на виконання лабораторної роботи

Література:1-15

**Лабораторна робота №7. Оцінювання стану інформаційної безпеки об’єкту**

**Мета роботи:** Освоєння практичних навичок з моделювання стану безпеки об’єкта та ранжування загроз.

1. Стислі теоретичні відомості
2. Хід роботи

Література:1-15

**Лабораторна робота №8. Розробка політики інформаційної безпеки**

**Мета роботи:** Набуття досвіду зі створення політики інформаційної безпеки.

1. Стислі теоретичні відомості

2. Хід роботи

Література:1-15

**Лабораторна робота № 9. «Модель порушника»**

**Мета роботи:** Ознайомитись з основними моделями порушників та їх класифікацією.

1. Теоретичні відомості
2. Контрольні запитання
3. Індивідуальні завдання

Література:1-15

**Лабораторна робота № 10.** Моделі загроз. Класифікації моделі загроз.

**Мета :** Розглянути питання оцінки дій загроз в інформаційних системах

1. Теоретичні відомості
2. Контрольні запитання

Література:1-15

**Лабораторна робота № 11. «Протокол випробувань комплексних систем захисту інформації»**

1. Загальні відомості про протокол випробувань комплексних систем захисту інформації( далі КСЗІ).
2. Зразок протоколу випробувань КСЗІ
3. Завдання на лабораторну роботу

Література:1-15

**Лабораторна робота 12. Дослідження та розгортання мережевої інфраструктури Microsoft Windows Exchange Server**

1. Мета роботи
2. Короткі теоретичні відомості
3. Порядок виконання роботи

Література:1-15

**6. Самостійна робота студента.**

Самостійна робота з дисципліни «Комплексні системи захисту інформації» виконується самостійно студентом на основі одного сформованого завдання.

Самостійна робота охоплює усі основні теми дисципліни «Комплексні системи захисту інформації». Звіт оформлюється у відповідності з встановленими вимогами.

Виконання самостійної роботи з одним із обов'язкових складових модулів залікового кредиту.

Орієнтова тематика:

1. Сучасний стан нормативно-правової бази України щодо побудови КСЗІ в ІКС
2. Сучасні методики та програмні засоби налагодження параметрів політики безпеки операційних систем в ІКС
3. Опис операційних систем, що мають позитивні експертні висновки в Україні, щодо побудови КСЗІ в ІКС
4. Опис АВПЗ, що мають позитивні експертні висновки в Україні, як складової КСЗІ в ІКС
5. Опис КЗЗ від НСД, що мають позитивні експертні висновки в Україні, як складової КСЗІ в ІКС
6. Опис засобів ТЗІ, що мають позитивні експертні висновки в Україні, як складової КСЗІ в ІКС
7. Опис засобів КЗІ (крім ЕЦП), що мають позитивні експертні висновки в Україні, як складової КСЗІ в ІКС
8. Опис засобів ЕЦП, що мають позитивні експертні висновки в Україні, як складової КСЗІ в ІКС
9. Сучасні методики та програмні засоби побудови моделей загроз для інформації та порушників в ІКС
10. Опис сучасних загроз для інформації та нормального функціонування ІКС
11. Сучасні методики та програмні засоби формування ФПЗ інформації від НСД в ІКС
12. Сучасні методики та програмні засоби оцінки стану захищеності інформації Web-сайту від НСД

13. Сучасні методики та програмні засоби оцінки надійності та ефективності КСЗІ в ІКС
14. Опис стану оформлення та провадження господарської діяльності у галузі ТЗІ в Україні
15. Опис стану оформлення та провадження господарської діяльності у галузі КЗІ в Україні (крім ЕЦП)
16. Опис стану оформлення та надання послуг електронного цифрового підпису в Україні
17.
18. Розробка таблиць даних для визначення необхідності та рівня кожної послуги безпеки інформації

**7. Організація та проведення тренінгу.**

Порядок проведення тренінгу:

Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

Організаційна частина полягає у створенні робочого настрою у колективі студентів.

Практична частина реалізується шляхом виконання вибраного завдання тренінгу.

Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносились на тренінг.

Рекомендується наступні теми для проведення тренінгу:

| | |
|---|---|
| 1 | Основні принципи організації КСЗІ |
| 2 | Відкритість алгоритмів і механізмів захисту |
| 3 | Концептуальні підходи до проектування систем захисту |
| 4 | Принцип простоти застосування засобів захисту |
| 5 | Організація проведення обстеження об’єктів інформаційної діяльності |
| 6 | Організація розроблення системи захисту інформації |
| 7 | Реалізація основних технічних заходів захисту |
| 8 | Реалізація первинних технічних заходів захисту |
| 9 | Контроль функціонування та керування системою ЗІ |
| 10 | Визначення на підприємстві інформаційних і технічних ресурсів, а також об'єктів інформаційної діяльності, що підлягають захисту |
| 11 | Категоріювання об'єктів інформаційної діяльності підприємства |
| 12 | Засекречування та розсекречування матеріальних носіїв інформації |
| 13 | Рекомендації з захисту інформації, що обробляється засобами КРТ класу Б |
| 14 | Класифікатор засобів копіювально-розмножувальної техніки |
| 15 | Вимоги до захисту інформації |
| 16 | Порядок створення, впровадження, супроводу та модернізації засобів технічного захисту інформації від несанкціонованого доступу |

**8. Методи навчання.**

У навчальному процесі застосовуються: лекції, в тому числі з використання мультимедійного проектора та інших ТЗН; практичні роботи, індивідуальні заняття; робота в Інтернет.

**9. Засоби оцінювання та методи демонстрування результатів навчання.**

У процесі вивчення дисципліни „Комплексні системи захисту інформації” використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування;
- залікове модульне тестування та опитування;
- завдання на лабораторному обладнанні, тощо;
- оцінювання тренінгів;
- оцінювання результатів самостійної роботи;
- екзамен;

- інші види індивідуальних та групових завдань.

**10. Критерії, форми поточного та підсумкового контролю**

Підсумковий бал (за 100 – бальною шкалою) з дисципліни "**Комплексні системи захисту інформації**" 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 | Модульний контроль 1 | Поточне оцінювання | Модульний контроль 2 | Тренінги | Самостійна робота | Екзамен |
| Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-6. | Підсумкове модульне тестування за темами № 1-6. | Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт № 7-12. | Підсумкове модульне тестування за темами № 7-12. | Визначається як середнє арифметичне з оцінок за завдання тренінгу. | Визначається як оцінка за наскрізне завдання самостійної роботи. | 1. Теоретичні питання: 2 питання по 20 балів. 2.Практичне завдання 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) |

**11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна**

| № | Найменування | Номер теми |
|---|---|---|
| 1 | Електронний варіант лекцій | 1-14 |
| 2 | Методичні вказівки до виконання практичних робіт (електронний варіант) | 1–14 |
| 3 | ПК Intel Core i3-540; монітор 19 Samsung; принтер лазерний Canon MF4570. | 1-14 |
| 4 | Засіб захисту інформації від несанкціонованого доступу «Лоза-1» версія 3, Екрануюча настільна шкатулка Фарадея для телефонів, автобрелків, NFC карт LockerBox RF MAXI. Генератор електромагнітних завад «Базальт-5ГЕШ», Мережевий завадозаглушувальний фільтр «ФЗП 103-2», Генератор шумових сигналів – МАРС ТЗО-4-2, Вібровипромінювач ВИ-3,ВИ-4, Акустичний випромінювач МАРС-АК, МАРС-АКЗ. Пристрій захисту телефонних ліній «Базальт – 3». | 1-14 |

## РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ


1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/ show/80
2. Комплекс засобів захисту від НСД в АС класу 1 «Рубіж-РСО» версія 2 [Електронний ресурс] / ТОВ «Технічний захист інформації» // 2019 - Режим доступу: http://tzi.com.ua/rubzh-rso-versya-20.html
3. Комплексні системи захисту інформації: проектування, впровадження, супровід. Збірник лекцій [Електронний ресурс] / Гребенніков В.В. // 2019 - Режим доступу:

http://www.cryptohistory.ru/for students/ 03-KSZI
4. Операційна система «OpenBSD, шифр BBOS» [Електронний ресурс] / Кампанія «ATMNIS» // 2012 - Режим доступу: http://www.atmnis.com/files/user files/BBOS overview.pdf
5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку / 2023 - Режимдоступу :
https://cip.gov.ua/ua/news/normativni-dokumenti-sistemi-tzi
6. Закон України "Про національну безпеку (2019)
7. НД ТЗІ 1.6-004-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що становить державну таємницю.
8. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e
9. "Комплексна безпека інформації та захист інформаційних ресурсів" автора Олександра С. Горбачова. Видавництво: Каравела. Рік видання: 2019. с. - 127.
10. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. пос. [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahystu_informaciyi/index.html 2024.
11. Комплексні системи захисту інформації в інформаційнотелекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин: ФОП Лук'яненко В.В., ТПК «Орхідея», 2019. – 144 с.