

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ЧОРТКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ  
ПІДПРИЄМНИЦТВА І БІЗНЕСУ

ЗАТВЕРДЖУЮ  
Директор ЧННІПБ ЗУНУ

Надія КУЛЬЧИЦЬКА

28 08 \* 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-педагогічної роботи  
Віктор ОСТРОВЕРХОВ

28 08 \* 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Інформаційна безпека»  
ступінь вищої освіти – бакалавр  
галузь знань – 01 Освіта/Педагогіка  
спеціальність – 015 Професійна освіта (цифрові технології)  
Спеціалізація – 015.39 Цифрові технології  
освітньо-професійна програма – Професійна освіта.  
(Цифрові технології)

кафедра фундаментальних та спеціальних дисциплін

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	ІРС (год.)	Тренінг (год.)	Самост. робота студ. (год.)	Разом (год.)	Залік (сем.)	Екз. (сем.)
Денна	3	5	30	30	4	8	78	150		5
Заочна	3	5	8	4	-	-	138	150		5

30.08.2024

Чортків – ЗУНУ  
2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 01 «Освіта/Педагогіка», спеціальності 015 «Професійна освіта (цифрові технології)», затвердженої Вченою радою ЗУНУ (протокол № 9 від 15.06.2022 р.).

Робочу програму склала Марія ЛОСЬ

Робоча програма затверджена на засіданні кафедри фундаментальних та спеціальних дисциплін (протокол № 1 від 28.08.2024 р.)

Завідувач кафедри



Людмила ДЕРМАНСЬКА

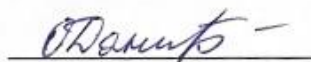
Розглянуто та схвалено групою забезпечення спеціальності 015 «Професійна освіта (цифрові технології)» (протокол № 1 від 20.08.24 р.)

Керівник групи  
забезпечення спеціальності



Лілія РЕБУХА

Гарант ОПП



Ольга ПАВЕЛЧАК-ДАНИЛЮК

## СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ "Інформаційна безпека"

### 1. Опис дисципліни "Інформаційна безпека"

Дисципліна – Інформаційна безпека	Галузь знань, спеціальність, освітньо- професійна програма, ступінь вищої освіти	Характеристика навчальної дисципліни
Кількість кредитів ECTS - 5	Галузь знань – 01 «Освіта/Педагогіка»	<b>Статус дисципліни</b> вибіркова дисципліна з циклу професійної підготовки <b>Мова навчання</b> українська
Кількість залікових модулів - 3	Спеціальність – 015 «Професійна освіта» (цифрові технології)	<b>Рік підготовки:</b> Денна – 3 Заочна- 3  <b>Семестр:</b> Денна – 5 Заочна- 5
Кількість змістових модулів - 2	Освітня програма - Професійна освіта (Цифрові технології)	<b>Лекції:</b> Денна форма – 30 год. Заочна форма- 8 год. <b>Практичні заняття:</b> Денна форма – 30 год. Заочна форма – 4 год
Загальна кількість годин – 150	Ступінь вищої освіти - бакалавр	<b>Самостійна робота:</b> Денна форма – 78 год. Заочна форма- 138 год  <b>Тренінг</b> – 8 год.  <b>Індивідуальна робота :</b> Денна – 4 год.
Тижневих годин – 10 год., з них аудиторних – 4 год.		Вид підсумкового контролю – <b>екзамен</b>

### 2. Мета й завдання дисципліни «Інформаційна безпека»

#### 2.1. Мета вивчення дисципліни

Програма та тематичний план навчальної дисципліни «Інформаційна безпека» орієнтовані на глибоке та ґрунтовне засвоєння студентами знань з теоретичних та методологічних основ є важливою складовою формування профілю фахівця у галузі публічного управління та адміністрування і належить до циклу дисциплін професійної підготовки здобувачів вищої освіти ступеня бакалавра спеціальності 015 «Професійна освіта».

Метою навчальної дисципліни є формування у здобувачів вищої освіти теоретичних знань та практичних навичок щодо забезпечення інформаційної безпеки національних інтересів у будь-якій сфері життєдіяльності суспільства.

Курс лекцій містить основні тексти лекцій, що відповідають навчальній програмі дисципліни «Інформаційна безпека». Розглянуто теоретичні засади інформаційної безпеки держави, зокрема розглянуто понятійний апарат у сфері інформаційної безпеки та кібербезпеки, з'ясовано сутність та визначено класифікації національних інтересів та загроз інформаційній безпеці. Розглянуто та проаналізовано міжнародну та вітчизняну нормативно-правову базу у сфері забезпечення інформаційної безпеки, з'ясовано напрями державної політики інформаційної безпеки, розглянуто структуру та повноваження органів, що забезпечують інформаційну безпеку та кібербезпеку в Україні. Розглянуто основні поняття національного інформаційного простору та визначено систему національних інформаційних ресурсів, проаналізовано проблеми забезпечення стійкості національного інформаційного простору.

Вивчення курсу «Інформаційна безпека» передбачає наявність систематичних та ґрунтовних знань із курсів «Моделювання бізнес-процесів», «Інтелектуальний аналіз даних», і «Дидактичні основи професійної освіти» та цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

## **2.2. Завдання вивчення дисципліни**

В результаті вивчення курсу «Інформаційна безпека» студенти повинні:

- знати основи державної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки;
- засвоїти знання щодо концептуальних засад, принципів, форм та методів забезпечення інформаційної безпеки;
- ознайомитись з ключовими загрозами інформаційної безпеки, основами управління інформаційною безпекою;
- набути навичок практичного використання знань теорії і практики інформаційної безпеки у практичній діяльності.

## **3. Програма дисципліни «Інформаційна безпека»**

### **Змістовний модуль 1. Забезпечення захисту інформаційної безпеки**

#### **Тема 1. Поняття інформаційної безпеки держави, суспільства та особи.**

Інформаційна безпека (поняття і визначення). Підходи до визначення поняття «інформаційна безпека». Інтереси особи, суспільства та держави в інформаційній сфері. Об'єкти, суб'єкти та види інформаційної безпеки.

Література: 1,2,3,4,5,6

#### **Тема 2. Загрози інформаційної безпеки.**

Характеристика інформаційної безпеки. Класифікація загроз. Сучасні загрози. Інформаційні ризики. Витік інформації.

Література: 1,2,3,4,5,6

#### **Тема 3. Принципи, форми та методи забезпечення інформаційної безпеки держави.**

Основні принципи забезпечення інформаційної безпеки держави. Основні форми забезпечення інформаційної безпеки держави. Методи забезпечення інформаційної безпеки.

Література: 1,2,3,4,5,6

#### **Тема 4. Інформаційна система персональних даних.**

Нормативні документи захисту даних. Конфіденційність персональних даних. Захист персональної інформації. Європейська система захисту персональних даних.

Література: 1,2,3,4,5,6

#### **Тема 5. Забезпечення безпеки інформації та інформаційних ресурсів.**

Основні напрями забезпечення безпеки інформації. Правовий захист. Організаційний захист. Інженерно-технічний захист.

Література: 1,2,3,4,5,6

### **Змістовний модуль 2. Управління інформаційною безпекою**

#### **Тема 6. Захист інформаційних систем.**

Джерела конфіденційної інформації. Інформаційна система як об'єкт захисту інформації. Рівні захисту інформаційних систем. Аналіз вразливостей корпоративних інформаційних систем. Основні принципи захисту інформації.

Література: 1,2,3,4,5,6

#### **Тема 7. Кіберзлочинність.**

Характеристики кіберзлочинності. Стан кіберзлочинності в Україні. Засоби протидії кіберзлочинності. Класифікація кіберзлочинів. Протидія кіберзлочинності в Україні. Боротьба з кіберзлочинами. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення.

Література: 1,2,3,4,5,6

#### **Тема 8. Інформаційне протиборство. Інформаційна війна.**

Визначення поняття інформаційне протиборство, інформаційна війна, інформаційний тероризм, інформаційна злочинність. Інформаційне протиборство як форма забезпечення інформаційної безпеки. Концепція інформаційної війни. Основні форми інформаційної війни на державному рівні. Інформаційна зброя. Засоби ураження комп'ютерних інформаційних систем.

Література: 1,2,3,4,5,6

#### **Тема 9. Основи управління інформаційною безпекою.**

Політика інформаційної безпеки організації. Основні правила інформаційної безпеки організації. Заходи управління інформаційною безпекою.

Література: 1,2,3,4,5,6

#### **Тема 10. Інформаційна безпека України**

Забезпечення інформаційної безпеки України. Система та політика забезпечення інформаційної безпеки України. Інформаційна безпека України у сфері прав і свобод людини.

Література: 1,2,3,4,5,6

**4. Структура залікового кредиту дисципліни «Інформаційна безпека»  
Денна форма навчання**

	Кількість годин					
	Лекції	Практичні заняття	Самостійна робота	Індивід. робота	Тренінг	Контр. заходи
<b>Змістовий модуль 1. Забезпечення захисту інформаційної безпеки</b>						
<b>Тема 1.</b> Поняття інформаційної безпеки держави, суспільства та особи	4	4	8	2	4	Усне опитування Тестові завдання
<b>Тема 2.</b> Загрози інформаційної безпеки.	4	4	8			Усне опитування
<b>Тема 3.</b> Принципи, форми та методи забезпечення інформаційної безпеки держави.	4	4	8			Усне опитування Тестові завдання
<b>Тема 4.</b> Інформаційна система персональних даних.	2	2	8			Усне опитування
<b>Тема 5.</b> Забезпечення безпеки інформації та інформаційних ресурсів.	2	2	8			Змістовний модуль По темах 1-5
<b>Змістовий модуль 2. Управління інформаційною безпекою</b>						
<b>Тема 6.</b> Захист інформаційних систем.	4	4	8	2	4	
<b>Тема 7.</b> Кіберзлочинність	2	2	8			Усне опитування
<b>Тема 8.</b> Поняття та зміст інформаційного протиборства. Інформаційна війна.	2	2	8			Усне опитування
<b>Тема 9.</b> Основи управління інформаційною безпекою.	2	2	6			Тестові завдання
<b>Тема 10.</b> Інформаційна безпека України	2	2	8			Змістовний модуль по темах 6-10
<b>ВСЬОГО: 150</b>	<b>30</b>	<b>30</b>	<b>78</b>	<b>4</b>	<b>8</b>	<b>екзамен</b>

**Структура залікового кредиту дисципліни «Інформаційна безпека»  
Заочна форма навчання**

	Кількість годин				Контр. Заходи
	Лекції	Практичні заняття	Самостійна робота	Індивідуальна робота	
<b>Змістовий модуль 1. Теоретичні основи інформаційної безпеки</b>					
Тема 1. Поняття інформаційної безпеки держави, суспільства та особи	1	1	12		Тестові завдання Усне опитування
Тема 2. Загрози інформаційної безпеки	1		12		
Тема 3. Інформаційна система персональних даних.	1		12		
<b>Змістовий модуль 2. Управління інформаційною безпекою</b>					
Тема 4. Принципи, форми та методи забезпечення інформаційної безпеки держави.	1	1	18		Тестові завдання
Тема 5. Забезпечення безпеки інформації та інформаційних ресурсів.	1		16		
Тема 6. Захист інформаційних систем. Кіберзлочинність	1	1	18		Тестові завдання
Тема 7. Кіберзлочинність.	1		16		
Тема 8. Поняття та зміст інформаційного протиборства. Інформаційна війна. Тема 9. Основи управління інформаційною безпекою.	1	1	16		Тестові завдання Усне опитування
Тема 10. Інформаційна безпека України			18		
<b>ВСЬОГО:</b>	<b>8</b>	<b>4</b>	<b>138</b>		

## 5. Тематика практичних занять.

### Практичне заняття 1.

**Тема.** Поняття інформаційної безпеки держави, суспільства та особи.

**Мета:** Засвоїти необхідність і сутність основних понять у сфері інформаційної безпеки.

#### Питання для обговорення:

1. Понятійний апарат інформаційної безпеки.
2. Захист інформації.
3. Об'єкти, суб'єкти та види інформаційної безпеки.
4. Класифікація загроз безпеки.
5. Інформаційна безпека особи та суспільства.

Література: 1,2,3,4,5,6

### Практичне заняття 2.

**Тема:** Основи національної безпеки держави. Види національної безпеки.

**Мета:** вивчення основних понять та основних категорій інформаційної безпеки.

#### Питання для обговорення:

1. Вивчення основних категорій теорії національної безпеки
2. Проведення класифікації загроз національній безпеці держави
3. Визначення факторів та засобів забезпечення національної безпеки
4. Класифікація базових рівнів національної безпеки;
5. Основні види національної безпеки;
6. Система забезпечення національної безпеки.

Література: 1,2,3,4,5,6

### Практичне заняття №3

**Тема:** Принципи, форми та методи забезпечення інформаційної безпеки.

**Мета:** Вивчення та дослідження загроз безпеці інформації.

#### Питання для обговорення:

1. Основні поняття і класифікація загроз.
2. Основні загрози доступності.
3. Основні загрози цілісності.
4. Основні загрози конфіденційності.

Література: 1,2,3,4,5,6

### Практичне заняття №4

**Тема:** Загрози інформаційній безпеці.

**Мета:** вивчення основних понять та основних категорій національної безпеки.

#### Питання для обговорення

1. Вивчення основних положень Концепції інформаційної безпеки України;
2. Класифікація базових загроз інформаційній безпеці;
3. Вивчення основних джерел загроз безпеці особистості, суспільства та держави;
4. Ознайомлення з методами та засобами забезпечення інформаційної безпеки.



Література: 1,2,3,4,5,6

### **ПРАКТИЧНЕ ЗАНЯТТЯ №5**

**Тема: Основні напрями національної інформаційної політики**

**Мета:** вивчення основних положень державної інформаційної політики.

**Питання для обговорення**

1. Вивчення основних положень державної інформаційної політики;
2. Вивчення основних напрямів національної інформаційної політики;
3. Визначення особливостей забезпечення інформаційної безпеки.

Література: 1,2,3,4,5,6

### **ПРАКТИЧНЕ ЗАНЯТТЯ №6**

**Тема: Види та властивості інформації як предмета захисту.**

**Мета:** вивчення основних видів та властивостей інформації.

**Питання для обговорення**

1. Вивчення поняття інформації та дані;
2. Визначення форм адекватності інформації;
3. Проведення класифікації мір інформації;
4. Характеристика якості інформації;
5. Дослідження основних властивостей інформації.

Література: 1,2,3,4,5,6

### **Практичне заняття №7.**

**Тема: Інформаційна система персональних даних.**

**Мета:** Вивчення та дослідження загроз державної інформаційної політики та сформулювати в них відповідні знання й навички з питань захисту персональних даних та інформаційної безпеки.

**Питання для обговорення:**

1. Інформаційна безпека в системі національної безпеки України.
2. Загрози, що виникають під час роботи з інформацією та персональними даними в сучасному кіберпросторі.
3. Вітчизняний та зарубіжний досвід розповсюдження та оприлюднення публічної інформації та захисту персональних даних.
4. Особливості захисту персональних даних в сучасному кіберпросторі.

Література: 1,2,3,4,5,6

### **Практичне заняття №8.**

**Тема: Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.**

**Мета:** вивчення концептуальних положень захисту інформації та інформаційних ресурсів.

**Питання для обговорення:**

1. Визначення базових загроз безпеці інформації та інформаційних ресурсів;
2. Класифікація уразливостей безпеці інформації та інформаційних ресурсів;
3. Вивчення основних напрямів забезпечення безпеки;
4. Вивчення загальних положень правового захисту;
5. Вивчення загальних положень організаційного захисту;

6. Вивчення загальних положень інженерно-технічного захисту;
7. Вивчення архітектури захисту інформації в інформаційних системах та мережах.

Література: 1,2,3,4,5,6

### **Практичне заняття №9**

**Тема: Захист інформаційних систем.**

**Мета:** *Вивчення та дослідження системи законодавства у сфері інформаційних відносин.*

**Питання для обговорення:**

1. Характеристики основних видів безпеки.
2. Рівні та види безпеки: політична, економічна, соціальна, воєнна, науково-технологічна, інформаційна, екологічна.
3. Забезпечення безпеки в інформаційній сфері.
4. Задачі забезпечення цілісності, доступності, конфіденційності та приватності.

Література: 1,2,3,4,5,6

### **Практичне заняття №10**

**Тема: Кіберзлочинність.**

**Мета:** *Вивчення та дослідження видів кіберзлочинності їх характеристики.*

**Питання для обговорення:**

1. Основні поняття та класифікація кіберзлочинності.
2. Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.
3. Система та загальна характеристика кіберзлочинів.
4. Реалізація форм кримінальної відповідальності за кіберзлочини.

Література: 1,2,3,4,5,6

### **Практичне заняття №11 -12**

**Тема: Поняття та зміст інформаційного протиборства.**

**Мета:** *Вивчення та дослідження основних видів інформаційної програмної зброї та способів і засобів протидії.*

**Питання для обговорення:**

1. Інформаційна зброя атаки.
2. Інформаційна зброя забезпечення.
3. Інформаційна алгоритмічна (математична) зброя.
4. Інформаційна програмна зброя. інформаційна апаратна зброя. Засоби протидії.

Література: 1,2,3,4,5,6

### **Практичне заняття № 13**

**Тема: Основи управління інформаційною безпекою.**

**Мета:** *Вивчення та дослідження принципів роботи системи аналізу та управління інформаційними ризиками*

**Питання для обговорення:**

1. Принципи забезпечення інформаційної безпеки України
2. Основні засоби досягнення цілей політики інформаційної безпеки України.
2. Забезпечення інформаційної безпеки Держави.

3. Повноваження у сфері інформаційної безпеки держави.
  4. Системи органів виконавчої влади.
  5. Роль громадянського суспільства та громадян у забезпеченні інформаційної безпеки країни.
- Література: 1,2,3,4,5,6

## **ПРАКТИЧНЕ ЗАНЯТТЯ №14-15**

**Тема: Система та політика забезпечення інформаційної безпеки України**

**Мета:** вивчення основних складових та політики забезпечення інформаційної безпеки України.

**Питання для обговорення:**

1. Інформаційна безпека в Україні
2. Методи забезпечення інформаційної безпеки України
3. Система забезпечення інформаційної безпеки України
4. Політика забезпечення інформаційної безпеки України

Література: 1,2,3,4,5,6

## **6. Тренінг з дисципліни**

Тренінг (англ. training) — це запланований процес модифікації (зміни) відношення, знання чи поведінкових навичок того, хто навчається, через набуття навчального досвіду з тим, щоб досягти ефективного виконання в одному виді діяльності або в певній галузі. Тренування (від англ. to train — виховувати, навчати) — комплекс вправ для тренування в чому-небудь. Тренування — система підготовки організму людини з метою пристосування його до підвищених вимог і складних умов роботи й життя.

### **Порядок проведення тренінгу**

**Тематика тренінгу: Моніторинг інформаційного простору подій безпеки.**

1. Вступна частина проводиться з метою ознайомлення з темою тренінгового заняття.
2. Організаційна частина полягає у створенні робочого настрою у колективі студентів, визначенні правил проведення тренінгового заняття.
3. Практична частина реалізовується шляхом індивідуальних завдань.
4. Підведення підсумків. Обговорюються результати виконання завдань. Обмін думками з питань, які виносились на тренінгові заняття.

## **7. Тематика самостійної роботи студентів**

Самостійна робота студентів полягає у підготовці презентаційних виступів, що оцінюються за 100-бальною шкалою і визначається як сукупність питомої ваги кожної складової:

- 80% - підготовка презентації;
- 20% - захист презентації.

Обговорюються результати виконання завдань. Обмін думками з питань, які виносились на тренінгові заняття.

Студенти повинні дослідити та застосувати відповідні методи та алгоритми за одним із варіантів:

1. Основні положення щодо організації системи захисту інформації.

2. Нормативно-правова база України у сфері ТЗІ.
3. Система захисту інформації у контексті системного мислення та системного підходу.
4. Визначення інформаційних ресурсів, що підлягають захисту.
5. Державна таємниця і конфіденційна інформація, що є власністю держави.
6. Недержавна конфіденційна і відкрита інформація, що потребує захисту.
7. Дослідження структури і умов функціонування інформаційної системи установи.
8. Модель системи об'єктів захисту.
9. Виявлення загроз безпеки інформаційним ресурсам, які підлягають захисту.
10. Класифікація загроз інформації.
11. Техніка на витоку інформації та НСД в комп'ютерних системах.
12. Джерела загроз і окрема модель порушника.
13. Проведення оцінки вразливості і ризиків для інформаційних ресурсів.
14. Оцінка вразливості інформаційних ресурсів.
15. Оцінка ризиків для інформаційних ресурсів.
16. Методи і засоби захисту інформації від витоку по технічних каналах.
17. Захист інформації в комп'ютерних системах від несанкціонованого доступу.
18. Основні положення «Загальних критеріїв».
19. Загальні положення щодо політики безпеки.
20. Змістословних документів політики безпеки.
21. Модель простору заходів і засобів захисту.
22. Критерій і особливості проектування оптимальної системи захисту інформації.
23. Технічне завдання на розробку СЗІ. План захисту інформації.
24. Впровадження, визначення якості і управління системою захисту інформації.
25. Визначення якості реалізованої системи захисту.
26. Контроль функціонування і управління системою захисту.
27. Поняття кіберпростору та кіберзлочинності.
28. Структура забезпечення інформаційної безпеки (Information Security Governance).
29. Загальні вимоги забезпечення інформаційної безпеки.

## **8. Засоби оцінювання та методи демонстрування результатів навчання**

У процесі вивчення дисципліни “Інформаційна безпека” використовуються наступні засоби оцінювання та методи демонстрування результатів навчання:

- поточне опитування, тестування;
- презентації результатів виконаних завдань;
- оцінювання результатів модульної контрольної роботи;
- оцінювання результатів самостійної роботи;
- аналітичні звіти, реферати, есе;
- студентські презентації та виступи на наукових заходах.

## 9. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100-бальною шкалою) з дисципліни “Інформаційна безпека” визначається як середньозважена величина, залежно 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	Тренінг	Самостійна робота	Екзамен
Оцінюється як середнє арифметичне з оцінок, отриманих по 1-5 темах	Підсумкова модульна контрольна робота по 1-5 темах Теоретичні питання (2 питання по макс 25 балів) Тестові завдання (5 тестів по 5 бали за тест) – макс. 25 балів Задача 1 – макс. 25 балів	Оцінюється як середнє арифметичне з оцінок, отриманих по 6-10 темах	Підсумкова модульна контрольна робота по 6-10 темах Теоретичні питання (2 питання по макс 25 балів) Тестові завдання (5 тестів по 5 бали за тест) – макс. 25 балів Задача 1 – макс. 25 балів	Завдання оцінюється макс. 100 балів	Сукупність питомої ваги кожної складової: 80% - підготовка презентації; 20% - захист презентації.	Завдання 1 – макс. 25 балів Завдання 2 – макс. 25 балів Тестові завдання (25 тестів по 2 бали за тест) – макс. 50 балів

### Шкала оцінювання:

За шкалою університету	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)

## 10. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1.	Мультимедійний проектор	1-10
2.	Проекційний екран	1-10
3.	Комунікаційне програмне забезпечення (Internet Explorer, Google Chrome, Firefox)	1-10
4.	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-10
5.	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-10
6.	Програмне забезпечення: ОС Windows	1-10
7.	Інструменти Microsoft Office (Word; Excel; Power Point )	1-10

## Рекомендована література

### Основна література

1. Інформаційна безпека держави: навч. посіб. / В.І.Гур'єв, Д.Б. Мехед, Ю.М.Ткач, І.В.Фірсова. Ніжин: ФОП Лук'яненко В.В.ТПК «Орхідея», 2018. 166с.
2. Інформаційна безпека держави : навч. посіб. / В. М. Рудницький [та ін.] ; Черкас. держ. технол. ун-т. Харків : ДІСА ПЛЮС, 2018. 358 с.
3. Інформаційна безпека. Підручник / В.В.Остроухов, М.М.Присяжнюк, О.І.Фармагей, М.М.Чеховська та ін.; під ред. В. В. Остроухова. К.: Видавництво Ліра-К, 2021. 412 с.
4. Лизанчук В. В. Інформаційна безпека України: теорія і практика : підручник / Львів. нац. ун-т ім. Івана Франка, Львів. шк. журналістики. Львів : ЛНУ ім. Івана Франка, 2017. 725 с.
5. Панченко О. А. Інформаційна безпека в епоху турбулентності: державно-управлінський аспект : монографія. Київ : КВІЦ, 2020. 331 с.
6. Рижук О. М. Інформаційна безпека України в умовах глобалізаційних викликів та гібридної війни : монографія / за ред. Бебика В. М. ; Відкр. міжнар. ун-т розвитку людини "Україна". Київ : Університет "Україна", 2019. 177 с.

### Допоміжна література

1. Виговська О., Белоусова Н. Інформаційна складова національної безпеки України : кол. монографія / Ін-т міжнар. відносин, Київ. нац. ун-т ім. Тараса Шевченка, Київ. ун-т ім. Бориса Грінченка. Київ: Київ. ун-т ім. Б. Грінченка, 2017. 166 с.
2. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою: навч. посібник / Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с.
3. Кавун С.В., Носов В.В, Манжай О.В. Інформаційна безпека. Навчальний посібник / Харків: Вид. ХНЕУ, 2008. 352 с.
4. Міжнародна інформаційна безпека: теорія і практика : підруч. для студентів ВНЗ, які навчаються за напрямом підгот. "Міжнародні відносини" та "Міжнародна інформація" / Є. Макаренко [та ін.] ; Київ. нац. ун-т ім. Тараса Шевченка, [Ін-т міжнар. відносин]. Київ : Центр вільної преси, 2016. 417 с.
5. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
6. Николаєнко Н. О., Комарчук О. О. Засоби масової комунікації як детермінанти гібридної війни : монографія / Нац. ун-т кораблебудування ім. адмірала Макарова. Миколаїв : НУК, 2021. 217 с.