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

ЗАТВЕРДЖУЮ
В.о. декана факультету комп'ютерних інформаційних технологій
_____Ігор ЯКИМЕНКО
«___» _____ 2023р.

ЗАТВЕРДЖУЮ
В.о. проректора з науково-педагогічної роботи
_____Віктор ОСТРОВЕРХОВ
«___» _____ 2023р.

РОБОЧА ПРОГРАМА

з дисципліни

«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

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. заняття (год.)	ІРС (год.)	Тренінг, КПІЗ (год.)	СРС (год.)	Разом (год.)	Іспит (сем.)
Денна	3	6	28	28	3	8	53	120	6

31.08.2023 рік

Тернопіль – 2023

Робоча програма складена 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 д.т.н., професор, завідувач кафедри кібербезпеки Яцків Василь Васильович, викладач кафедри кібербезпеки Давлетова Аліна Ярославівна

Робоча програма затверджена на засіданні кафедри кібербезпеки
протокол № 1 від 28.08.2023р.

Завідувач кафедри
кібербезпеки Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності кібербезпека та захист інформації, протокол №1 від 30.08.2023 р.

Голова групи забезпечення
спеціальності Василь ЯЦКІВ

Гарант освітньо-професійної
програми Ігор ЯКИМЕНКО

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни

Дисципліна «Управління інформаційною безпекою»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 4	Галузь знань 12 «Інформаційні технології»	Статус дисципліни - обов'язкова Мова навчання - українська
Кількість залікових модулів – 4	Спеціальність 125 «Кібербезпека»	Рік підготовки: 3 Семестр: 6
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції: 28 год. Лабораторні заняття: 28 год.
Загальна кількість годин – 120		Самостійна робота: 53 год. Тренінг: 8 год. Індивідуальна робота:3 год.
Тижневих годин – 8,5 з них аудиторних – 4		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни

2.1. Мета дисципліни

Метою вивчення дисципліни 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 щодо управління інформаційною безпекою в інформаційно-телекомунікаційних (автоматизованих) системах для реалізації встановленої політики безпеки.

2.2. Завдання вивчення дисципліни

Основними завданнями вивчення дисципліни є формування компетентностей та умінь щодо основних підходів захисту інформації, концептуальної моделі інформаційної безпеки, розроблення, впровадження та експлуатації систем управління інформації на об'єктах інформаційної діяльності, формування навичок аналізу систем забезпечення інформаційної безпеки з метою впровадження найкращих практик захисту інформації. Проведення лекційних занять забезпечує викладення основних термінів, положень і принципів інформаційної безпеки та механізмів її реалізації у відповідності з програмою та робочим планом та формуванні у студентів цілісної системи теоретичних знань з курсу «Управління інформаційною безпекою».

Проведення практичних занять забезпечує формування у студентів практичних навичок щодо управління інформаційною безпекою для забезпечення неперервності бізнес-процесів згідно встановленої політики інформаційної та/або кібербезпеки.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

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

Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою.

Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Управління інформаційною безпекою» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів «Основи кібербезпеки», «Кібернетична

безпека», «Комп'ютерні мережі», «Операційні системи», а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи студентів.

2.5. Результати навчання

Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

Вирішувати задачі управління процедурами ідентифікації, аутентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

3. Програма навчальної дисципліни

Змістовий модуль 1. Основні положення управління інформаційною безпекою.

Тема 1. Інформаційні ресурси, що підлягають захисту.

1. Основні поняття. 2. Сфери розповсюдження державної таємниці на інформацію. 3. Комерційна таємниця. 4. Персональні дані.

Література: 1-11

Тема 2. Загрози безпеці інформації.

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

Література: 1-11

Тема 3. Характеристики захищеності інформаційних ресурсів. Модель CIA.

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. Модель CIA. 5. Задачі забезпечення цілісності доступності, конфіденційності.

Література: 1-11

Тема 4. Політика інформаційної безпеки.

1. Класифікаційна політика у сфері інформації. 2. Механізми реалізації інформаційної безпеки. 3. Сертифікація: створення захищеної роботи. 4. Контроль якості інформації. 5. Методи забезпечення інформаційної безпеки. 6. Положення щодо політики безпеки. 7. Розробка політики безпеки. 8. Програма реалізації політики безпеки.

Література: 1-11

Тема 5. Соціотехнічна безпека.

1. Поняття соціотехнічної системи та її властивостей. 2. Структурно-логічна схема соціотехнічної системи. 3. Головні характеристики соціотехнічної системи. 4. Методи соціального інжинірингу. 5. Основні алгоритми соціотехнічних атак на інформаційні ресурси, етапи проведення. 6. Захист інформації від соціотехнічних атак. 7. Соціальний фактор у проблемі забезпечення інформаційної і кібербезпеки. 8. Соціальні мережі: особливості, основні поняття та визначення. 9. Моніторинг соціальних мереж. 10. Менеджмент персоналу у сфері інформаційної безпеки. 11. Стратегія захисту.

Література: 1-11

Змістовий модуль 2. Інформаційна безпека держави

Тема 6. Національна безпека.

1. Визначення національної безпеки. 2. Основні категорії теорії національної безпеки. 3. Принципи забезпечення національної безпеки. 4. Характеристики національної безпеки. 5. Фактори забезпечення національної безпеки. 6. Основні засоби забезпечення національної безпеки.

Література: 1-11

Тема 7. Кіберзлочинність.

1. Характеристики кіберзлочинності. 2. Стан кіберзлочинності в Україні. 3. Засоби протидії кіберзлочинності. 4. Класифікація кіберзлочинів. 5. Протидія кіберзлочинності в Україні. 6. Боротьба з кіберзлочинами. 7. Національні інтереси України в інформаційній сфері та шляхи їх забезпечення.

Література: 1-11

Тема 8. Інформаційне протиборство. Інформаційна війна.

1. Визначення поняття інформаційне протиборство, інформаційна війна, інформаційний тероризм, інформаційна злочинність. 2. Інформаційне протиборство як форма забезпечення інформаційної безпеки. 3. Концепція інформаційної війни. 4. Основні форми інформаційної війни на державному рівні. 5. Інформаційна зброя. 6. Засоби ураження комп'ютерних інформаційних систем.

Література: 1-11

Змістовий модуль 3. Організація управління інформаційною безпекою

Тема 9. Управління ризиками інформаційної безпеки

1. Оцінка ризиків інформаційної безпеки. 2. Рівняння ризику. 3. Рішення щодо управління ризиками. 4. Управління ризиками. 5. Схильність до ризику.

Тема 10. Аналіз ризиків

1. Методи аналізу ризиків. 2. Оцінка ризиків. 3. Види аналізу оцінки ризиків. 4.Документування оцінки ризиків. 5. Реєстр ризиків.

Література: 1-11

Тема 11. Реагування на інциденти інформаційної безпеки

1. Вирішення інцидентів і планування реагування на інциденти. 2. Аварійне відновлення. 3.Процес реагування. 4. Плани внутрішніх і зовнішніх комунікацій. 5. Ідентифікація інциденту.

Тема 12. Аналіз інцидентів інформаційної безпеки

1. Вплив і масштаб інцидентів. 2. Оцінка та аналіз інцидентів. 3. Стримування інциденту. 4.Пом'якшення та ліквідація інциденту. 5. Інструменти обробки інцидентів.

Література: 1-11

Тема 13. Управління наслідками інцидентів інформаційної безпеки

1. Зміцнення системи. 2. Ізоляція. 3. Honeypot. 4. Чорнийсписок. 5. Білий список. 6. DNS фільтрація. 7. Маршрутизація чорної діри. 8. Управління мобільними пристроями. 9. Безпечне видалення та утилізація. 10. Пристрої та інструменти, що використовуються для стримування та пом’якшення. 11. Важливість оновлення підписів пристроїв. 12. Додаткова тактика стримування та пом’якшення.

Література: 1-11

Тема 14. Розслідування інцидентів

1. Обов'язки експерта-криміналіста. 2. Моделі розслідувань. 3. Підготовка криміналістичного дослідження. 4. Обсяг дослідження. 5. Генерація та аналіз хронології. 6. Автентифікація доказів. 7. Ланцюжок зберігання. 8. Спілкування та взаємодія з третіми сторонами. 9. Forensic Toolkit. 10. Криміналістичний інструментарій. 11. Підготовка до криміналістичного дослідження. 12. Порядок мінливості. 13. Файлові системи. 14. Вирізання файлів і вилучення даних. 15. Збереження даних для криміналістики. 16. Безпечне зберігання речових доказів. 17. Криміналістичний аналіз скомпрометованих систем. 18. Динамічний аналіз.

Література: 1-11

4. Структура залікового кредиту дисципліни

	Кількість годин					
	Лекції	Лаборат. заняття	СРС	ІРС	Тренінг, КПІЗ	Контрольні заходи
Змістовий модуль 1. Основні положення управління інформаційною безпекою.						
Тема 1. Інформаційні ресурси, що підлягають захисту.	2	2	3		2	Поточне опитування
Тема 2. Загрози безпеці інформації.	2	2	3	1		Поточне опитування
Тема 3. Характеристики захищеності інформаційних ресурсів. Модель CIA.	2	2	3		2	Поточне опитування

Тема 4. Політика інформаційної безпеки.	2	2	4	1		Поточне опитування
Тема 5. Соціотехнічна безпека.	2	2	4			Поточне опитування
Змістовий модуль 2. Інформаційна безпека держави						
Тема 6. Національна безпека.	2	2	4		2	Поточне опитування
Тема 7. Кіберзлочинність.	2	2	4			Поточне опитування
Тема 8. Інформаційне протиборство. Інформаційна війна.	2	2	4			Поточне опитування
Змістовий модуль 3. Організація управління інформаційною безпекою						
Тема 9. Управління ризиками інформаційної безпеки	2	2	4	1	2	Поточне опитування
Тема 10. Аналіз ризиків	2	2	4			Поточне опитування
Тема 11. Реагування на інциденти інформаційної безпеки	2	2	4			Поточне опитування
Тема 12. Аналіз інцидентів інформаційної безпеки	2	2	4			Поточне опитування
Тема 13. Стримування та пом'якшення наслідків інцидентів	2	2	4			Поточне опитування
Тема 14. Розслідування інцидентів	2	2	4			Поточне опитування
Разом	**28**	**28**	**53**	**3**	**8**	

5. Тематика лабораторних занять.

Лабораторне заняття №1

Тема: Інформаційні ресурси, що підлягають захисту.

Мета: Вивчення та дослідження інформаційних ресурсів, що підлягають захисту.

Питання для обговорення: 1. Основні поняття. 2. Сфери розповсюдження державної таємниці на інформацію. 3. Комерційна таємниця.4. Персональні дані.

Література: 1-10.

Лабораторне заняття № 2

Тема: Загрози безпеці інформації

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: 1-10.

Лабораторне заняття №3

Тема: Характеристики захищеності інформаційних ресурсів. Модель CIA.

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. Модель CIA. 5. Задачі забезпечення цілісності, доступності, конфіденційності та приватності.

Література: 1-10.

Лабораторне заняття №4

Тема: Політика інформаційної безпеки.

Мета: Вивчення та дослідження політика інформаційної безпеки.

Питання для обговорення: 1. Загальні положення щодо політики безпеки. 2. Розробка політики безпеки. 3. Програма реалізації політики безпеки. 4. Зміст основних документів політики безпеки. 5. Класифікаційна політика у сфері інформації. 6. Методи забезпечення інформаційної безпеки.

Література: 1-10.

Лабораторне заняття №5

Тема: Соціотехнічна безпека.

Мета: Вивчення та дослідження соціального аспекту інформаційної безпеки.

Питання для обговорення: 1. Структурно-логічна схема соціотехнічної системи. 2. Методи соціального інжинірингу. 3. Основні алгоритми соціотехнічних атак на інформаційні ресурси, етапи проведення. 4. Рекомендації щодо захисту від соціотехнічних атак. 5. Менеджмент персоналу у сфері інформаційної безпеки

Література: 1-10.

Лабораторне заняття № 6

Тема: Інформаційна програмна зброя

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

Питання для обговорення: Інформаційна зброя атаки. Інформаційна зброя забезпечення. Інформаційна алгоритмічна (математична) зброя. Інформаційна програмна зброя. інформаційна апаратна зброя. Засоби протидії.

Література: 1-10.

Лабораторне заняття № 7

Тема: Оцінка та управління ризиками інформаційної безпеки

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

Питання для обговорення: 1. Оцінка ризиків інформаційної безпеки:Актив, загроза, загроза, вразливість, експлойт. 2. Рівняння ризику. 3 Рішення щодо управління ризиками.
4. Управління ризиками. 5. Схильність до ризику. 5 Методи аналізу ризиків. 5 Оцінка ризиків.
6 Види аналізу оцінки ризиків. 7. Документування оцінки ризиків. 8 Реєстр ризиків

Література: 1-10.

Лабораторне заняття №8

Тема: Система розробки та управління інформаційною безпекою.

Мета: Вивчення та дослідження принципів роботи системи розробки та управління політикою інформаційної безпеки.

Питання для обговорення: 1. Стандарт управління політикою інформаційної безпеки.
2. Загальні положення з управління інформаційною безпекою. 3. Фізична безпека й безпека навколишнього середовища. 4. Адміністрування комп'ютерних систем і обчислювальних мереж.
5. Управління доступом до систем. 6. Розробка та супроводження інформаційних систем.
7. Планування безперебійної роботи підприємства та аудит безпеки.

Література: 1-10.

Лабораторне заняття №9

Тема: Розслідування інцидентів інформаційної безпеки.

Мета: Вивчення та дослідження методів та засобів розслідування інцидентів інформаційної безпеки.

Питання для обговорення: 1. Обов'язки експерта-криміналіста. 2. Оцінювання області розслідування. 3. Моделі розслідувань. 4. Збір, дослідження, аналіз та відображення доказів.
5. Автентифікація доказів. 6. Криміналістичний інструментарій. 7. Ланцюжок зберігання.
8. Кіберправо.

Література: 1-10.

Лабораторне заняття № 10

Тема: Управління інформаційною безпекою організації. Електронний документообіг.

Мета: Вивчення та дослідження управління інформаційною безпекою організації. Створення цифрового підпису за допомогою формування пар відкритих та закритих ключів.

Питання для обговорення: 1. Сучасна криптографія. 2. Шифрування / дешифрування.
3. Алгоритми шифрування: симетричні, асиметричні. 3. Електронний документообіг. 4. Захист інформації, що міститься в документах. 5. Електронно-цифровий підпис.

Література: 1-10.

6. Комплексне практичне індивідуальне завдання (КПІЗ) з дисципліни

Індивідуальне завдання з курсу «Управління інформаційною безпекою» виконується самостійно студентом на основі сформованого завдання. КПІЗ охоплює основні теми курсу. Виконання КПІЗ є одним із обов'язкових складових модулів залікового кредиту. Метою виконання

КПІЗ є оволодіння навичками оцінювання ступеня ризику при вирішенні конкретних задач кібербезпеки. 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. Технічні канали 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. Зміст основних 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.

7. Самостійна робота та дуальна освіта

№ п/п	Тематика
1	Складові забезпечення інформаційної безпеки.
2	Проблеми та шляхи їх вирішення у забезпеченні інформаційної безпеки.
3	Загрози інформації та вибір функціонального класу послуг захисту.
4	Особливості реалізації комплексних систем захисту інформації.
5	Структура та функції державної системи забезпечення інформаційної безпеки.
6	Ліцензування в галузі забезпечення інформаційно-психологічної безпеки.
7	Сертифікація засобів і методів неусвідомленого інформаційного впливу
8	Експертиза з метою забезпечення інформаційно-психологічної безпеки
9	Контроль за забезпеченням інформаційно-психологічної безпеки.
10	Критерії оцінки рівня інформаційної безпеки за національними та міжнародними стандартами.
11	Оцінка рівня інформаційної безпеки інформаційних ресурсів.
12	Критерії оцінки рівня інформаційної безпеки за національними стандартами.
13	Критерії оцінки рівня інформаційної безпеки за міжнародними стандартами.
14	Нормативні документи з оцінювання захищеності інформаційних ресурсів.
15	Системи менеджменту інформаційної безпеки.
16	Система управління інформаційною безпекою.
17	Функції технологічного управління інформаційною безпекою.

8. Тренінг з дисципліни.

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.

3.Практична частина реалізується шляхом виконання завдань з певних проблемних питань теми тренінгу.

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

Тематика тренінгу: Застосування методів, засобів та алгоритмів для управління інформаційною безпекою.

№	Вид роботи	Порядок проведення тренінгу
1	Аналіз потреб та загроз у сфері інформаційної безпеки	− Проведення аналізу існуючих інформаційних активів та ризиків безпеки. − Визначення потенційних загроз для інформаційної безпеки. - Оцінка вразливостей інформаційних систем.
2	Розробка політик і процедур інформаційної безпеки	− Створення політик безпеки даних і інформаційних систем. − Визначення стандартів та правил доступу до інформації. - Розробка процедур для управління інцидентами безпеки.
3	Впровадження технічних заходів інформаційної безпеки	− Встановлення програмного забезпечення для захисту від вірусів та зловмисного програмного забезпечення. − Проведення навчання для співробітників з питань інформаційної безпеки. − Шифрування даних та резервне копіювання.
4	Моніторинг інформаційної безпеки	− Налаштування системи моніторингу подій безпеки − Проведення аудиту системи інформаційної безпеки − Оновлення політик та процедур відповідно до змінних умов та загроз.

9. Методи навчання.

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

10. Засоби оцінювання та методи демонстрування результатів навчання.

У процесі вивчення дисципліни «Управління інформаційною безпекою» використовуються наступні методи оцінювання та методи демонстрування результатів навчання:

– поточне тестування та опитування;

– підсумкове тестування за кожним змістовним модулем;

– оцінювання виконання лабораторних робіт;

– ректорська контрольна робота;

– комплексне практичне індивідуальне заняття (КПІЗ).

– екзамен.

11. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Управління інформаційною безпекою» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту:

Семестр 6 – іспит

Заліковий модуль 1	**Заліковий модуль 2 (ректорська контрольна робота)**	**Заліковий модуль 3 (підсумкова оцінка за КПІЗ)**	**Заліковий модуль 4 (письмовий екзамен)**
20 %	20 %	20 %	40 %

1. Усне опитування на заняттях (8 тем по 2 бали) - max 16 балів. 2. Письмова робота - max 60 балів. 3. Практичне завдання (6 практичних завдань по 4 балів)- max 24 бали.	1. Усне опитування на заняттях (6 тем по 4 балів) - max 24 балів. 2. Письмова робота - max 52 бали. 3. Практичне завдання (4 практичні завдання по 6 балів) - max 24 бали.	1. Підготовка КПІЗ - max 40 балів. 2. Захист КПІЗ -max 40 балів. 3. Участь у тренінгах - max 20 балів	1. Теоретичні питання: 2 питання по 30 балів - max 60 балів. 2. Практичне завдання - max 40 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)

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

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1-14
2	Персональні комп'ютери	1-14
3	Наявність доступу до мережі Інтернет	1-14
4	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-14
5	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-14
6	Спеціалізовані програмні продукти (CrowdTangle, Botometer, Botsentinel, Hoaxy, DoesFollow, TinEye, InVid, Social Bearning, Social Blade, Digital Security)	1-14

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Шумейко О.О. Інформаційна безпека. Дніпровський державний технічний університет, 2019. - 155 с.
2. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
3. Мужанова Т.М. Інформаційна безпека держави. Київ: Державний університет телекомунікацій, 2019. - 131 с.
4. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
5. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p.
6. Alassouli Hidaia. Common Windows, Linux and Web Server Systems Hacking Techniques. Independently published, 2021. - 181 p.
7. Barnum Todd. The Cybersecurity Manager's Guide: The Art of Building Your Security Program. O'Reilly Media, Inc., 2021. - 168 p.
8. Daimi K., Peoples C. Advances in Cybersecurity Management. Springer, 2021.- 497 p.
9. Alexandrou Alex. Cybercrime and Information Technology: The Computer Network Infrastructure and Computer Security, Cybersecurity Laws, Internet of Things (IoT), and Mobile Devices. CRC Press, 2022. - 455 p.
10. Goyal D., Balamurugan S., Senthilnathan K., Annapoorani I., Israr M. (Eds.) Cyber-Physical Systems and Industry 4.0: Practical Applications and Security Management. Apple Academic Press Inc., CRC Press, 2022. - 290 p.