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

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

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«30» серпня 2024 р.

ЗАТВЕРДЖУЮ
Директор ННІНОТ
_____ Святослав ПИТЕЛЬ
«30» серпня 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни – "Інформаційна безпека"

Ступінь вищої освіти – бакалавр
Галузь знань – 01 Освіта/Педагогіка
Спеціальність – 015 Професійна освіта
Спеціалізація – 015.39 Цифрові технології
Освітньо–професійна програма – "Професійна освіта (Цифрові технології)"

Кафедра економічної кібернетики та інформатики

Форма навчання	Курс	Семестр	Лекції (год.)	Практ. (год.)	Тренінг (год.)	ІРС (год.)	СРС (год.)	Разом (год.)	Іспит (сем.)
ДФН	3	5	28	28	8	3	83	150	5
ЗФН	3	5	8	4			138	150	5

Тернопіль – ЗУНУ
2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 01 Освіта/Педагогіка спеціальності 015 Професійна освіта, затвердженої на засіданні Вченої ради Західноукраїнського національного університету (протокол № 9 від 15. 06. 2022 р.)

Робочу програму склала: канд. фіз.-мат. наук, доцент, доцент кафедри економічної кібернетики та інформатики Надія ХОМА

Робоча програма затверджена на засіданні кафедри економічної кібернетики та інформатики, протокол № 1 від 28 серпня 2024 р.

Завідувачка кафедри економічної
кібернетики та інформатики,
д-р екон. наук, професор Леся БУЯК

Розглянуто та схвалено групою забезпечення спеціальності 015 Професійна освіта, протокол № 1 від 30.08 2024 р.

Голова групи забезпечення спеціальності,
канд. педаг. наук, доцент Володимир ШАФРАНСЬКИЙ

Гарант ОП,
канд. екон. наук, доцент Оксана БАШУЦЬКА

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– 5	Галузь знань – 01 Освіта/Педагогіка	**Статус дисципліни:** блок обов'язкових дисциплін, цикл загальної підготовки **Мова навчання** – українська
Кількість залікових модулів – 5	Спеціальність: 015 Професійна освіта	Рік підготовки: *денна* – третій *заочна* – третій Семестр: *денна* – п'ятий *заочна* –п'ятий
Кількість змістових модулів – 3	Спеціалізація: 015.39 Цифрові технології	Лекції: *денна* – 28 год. *заочна* – 8 Практичні заняття: *денна* – 28 год. *заочна* – 4
Загальна кількість годин – 150	Освітньо-професійна програма – Професійна освіта (Цифрові технології)	Самостійна робота: *денна* – 83 год. *заочна* – 138 Тренінги: *денна* – 8 год. Індивідуальна робота: *денна* – 3 год.
Кількість годин на тиждень – 10, з них 4 год. аудиторних (лекції – 2 год., практичні заняття – 2 год.)	Ступінь вищої освіти – бакалавр	Вид підсумкового контролю – екзамен

2. Мета і завдання дисципліни «Інформаційна безпека»

2.1. Мета вивчення дисципліни

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

2.2. Завдання вивчення дисципліни

Завданнями вивчення курсу «Інформаційна безпека» є:

– знати основні закони, принципи та правила поводження з інформацією;

– виявляти реальні та потенційні загрози у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;

– засвоєння базових понять забезпечення захисту інформації;

– формування у студентів цілісної системи теоретичних знань з курсу «Інформаційна безпека»;

– формуваня практичних навичок щодо визначення джерел та наслідків впливу на інформацію та способи їх попередження та усунення.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни «Інформаційна безпека»:

– здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище;

– здатність аналізувати ефективність проєктних рішень, пов'язаних з підбором, експлуатацією, удосконаленням, модернізацією технологічного обладнання та устаткування галузі/сфери відповідно до спеціалізації;

– здатність використовувати відповідне програмне забезпечення для вирішення професійних завдань, відповідно до спеціалізації.

2.4. Передумови для вивчення дисципліни

Базові знання зі шкільного курсу «Інформатика», наявність систематичних і грунтовних знань із курсу «Інформаційно–комунікаційні технології».

2.5. Програмні результати навчання:

– володіти інформацією чинних нормативно-правових документів, законодавства, галузевих стандартів професійної діяльності в установах, на виробництвах, організаціях галузі/сфери (відповідно до спеціалізації);

– розуміти особливості комунікації, взаємодії та співпраці в міжнародному культурному та професійному контекстах;

– володіти культурою мовлення, обирати оптимальну комунікаційну стратегію у спілкуванні з групами та окремими особами.

– аналізувати та оцінювати ризики, проблеми у професійній діяльності й обирати ефективні шляхи їх вирішення.

3. Програма навчальної дисципліни «Інформаційна безпека»

Змістовий модуль 1. Основи знань про інформаційну безпеку

Тема 1. Основи інформаційної безпеки

1. Поняття інформаційної безпеки.
2. Основні види безпеки.
3. Тріада (CIA): конфіденційність, цілісність, доступність.

Тема 2. Загрози інформаційній безпеці

1. Класифікація загроз.
2. Типи атак на інформаційні системи.

Тема 3. Безпека даних

1. Концепція захисту інформації.
2. Захист конфіденційності, цілісності та доступності даних.
3. Методи аутентифікації, авторизації та аудиту даних.
4. Види забезпечення безпеки інформації.

Тема 4. Політика безпеки інформації

1. Реалізація, підтримка політики безпеки.
2. Моделі політики безпеки.
3. Закони України про захист інформації.

Змістовий модуль 2. Криптографічний захист інформації

Тема 5. Симетричні системи

1. Криптографія і її основні поняття.
2. Симетричні криптосистеми
3. Класифікація симетричних криптоалгоритмів.
4. Блокові алгоритмі і режими шифрування.
5. Мережі Фейстеля.
6. Алгоритм симетричного шифрування DES.

Тема 6. Асиметричні системи

1. Концепція криптосистем з відкритим ключем.
2. Однонаправлені функції.
3. Криптосистема шифрування даних RSA.
4. Протокол Діффі — Геллмана.

Тема 7. Сучасні криптографічні протоколи

1. Аутентифікація. Електронний цифровий підпис.
2. Хеш-функція.
3. Інфраструктура відкритих ключів (PKI).

Змістовий модуль 3. Управління інформаційною безпекою

Тема 8. Соціальна інженерія та фішинг

1. Вивчення методів атак, які спрямовані на отримання конфіденційної інформації шляхом маніпулювання людьми.

Тема 9. Управління ризиками та відповідальність

1. Оцінка ризиків, стратегії управління ризиками, стандарти безпеки, законодавство та регулювання в галузі кібербезпеки.

Тема 10. Концепція побудувати віртуальних приватних мереж VPN

1. Визначення VPN.
2. Переваги і недоліки використання VPN з’єднання.
3. Рівні реалізації, структура, ласифікація VPN.
4. Визначення IPSec. Робота протоколу IPsec. Сфери застосування IPsec. Конфіденційність і шифрування. Асоціації IKE і IPSEC. П'ять кроків IPSEC.

4. Структура залікового кредиту дисципліни «Інформаційна безпека»

денна форма навчання

Тема	Кількість					
	Лекції	**Практичні заняття**	**Індивідуальна робота**	**Тренінги**	**Самостійна робота**	**Контрольні заходи**
Змістовий модуль 1. Основи знань про інформаційну безпеку						
Тема 1. Основи інформаційної безпеки	2	2	1	2	4	поточне опитування, завдання, тести
Тема 2. Загрози інформаційній безпеці	2	4			8	
Тема 3. Безпека даних	2	4			8	
Тема 4. Політика безпеки інформації	2	2			8	
Змістовий модуль 2. Криптографічний захист інформації						
Тема 5. Симетричні системи	4	2	1	4	12	поточне опитування, завдання, тести
Тема 6. Асиметричні системи	4	4			8	
Тема 7. Сучасні криптографічні протоколи	4	4			14	
Змістовий модуль 3. Управління інформаційною безпекою						
Тема 8. Соціальна інженерія та фішинг	2	2	1	2	8	поточне опитування, завдання, тести
Тема 9. Управління ризиками та відповідальність	4	2			7	
Тема 10. Концепція побудувати віртуальних приватних мереж VPN	2	2			6	
Всього	**28**	**28**	**3**	**8**	**83**	
Тема	**Кількість**					

заочна форма навчання

	Лекції	**Практичні заняття**	**Самостійна робота**
Змістовий модуль 1. Основи знань про інформаційну безпеку			
Тема 1. Основи інформаційної безпеки	2	1	8
Тема 2. Загрози інформаційній безпеці			10
Тема 3. Безпека даних			12
Тема 4. Політика безпеки інформації			10

Змістовий модуль 2. Криптографічний захист інформації			
Тема 5. Симетричні системи	4	2	22
Тема 6. Асиметричні системи			20
Тема 7. Сучасні криптографічні протоколи			20
Змістовий модуль 3. Управління інформаційною безпекою			
Тема 8. Соціальна інженерія та фішинг	2	1	12
Тема 9. Управління ризиками та відповідальність			16
Тема 10. Концепція побудувати віртуальних приватних мереж VPN			8
Всього	**8**	**4**	**138**

5. Тематика практичних занять з дисципліни «Інформаційа безпека»

Денна форма

Змістовий модуль 1. Основи знань про інформаційу безпеку

Практичне заняття № 1

Тема: Основи інформаційної безпеки
Мета: Вивчення та дослідження інформаційної безпеки.
Питання для обговорення:
1. Поняття інформаційної безпеки.
2. Основні види безпеки.
3. Тріада (CIA): конфіденційність, цілісність, доступність.

Література: 1-12

Практичне заняття № 2-3

Тема: Загрози інформаційній безпеці.
Мета: Вивчення та дослідження загроз безпеці інформації.
Питання для обговорення:
1. Класифікація загроз.
2. Типи атак на інформаційні системи.
3. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів.
4. Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

Література: 1-12

Практичне заняття № 4

Тема: Безпека даних.
Мета: Вивчення та дослідження проблем інформаційної безпеки.
Питання для обговорення:
1. Концепція захисту інформації.
2. Захист конфіденційності, цілісності та доступності даних.
3. Методи аутентифікації, авторизації та аудиту даних.
4. Види забезпечення безпеки інформації.
5. Критерії оцінки інформаційної безпеки та аспекти захисту інформації

Література: 1-12

Практичне заняття № 5

Тема: Політика безпеки інформації.
Мета: Вивчення та дослідження політики інформаційної безпеки.
Питання для обговорення:
1. Реалізація, підтримка політики безпеки.

2. Моделі політики безпеки.
3. Закони України про захист інформації.

Література: 1-12

Практичне заняття № 6

Тема: Встановлення віртуальної машини на ПК

Мета: Навчитись встановлювати віртуальну машину.

1. Встановлення та початкове налагодження Virtual Box.
2. Створення віртуальної машини.
3. Додаткові налаштування віртуальної машини.
4. Підготовка віртуальної машини до встановлення операційної системи

Література: 1-12

Практичне заняття № 7

Тем: Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування повідомлення.

Мета: Розглянути базові поняття теорії чисел, отримання практичних навичок шифрування і дешифрування повідомлень за допомогою відкритого та закритого ключа криптосистеми RSA з використанням теорії чисел.

Питання для обговорення:

1. Основні поняття криптографії, способи шифрування файлів, папок, повідомлень; криптографічні методи захисту інформації, основні засоби здійснення криптографічного захисту інформації
2. Використання теорії чисел для захисту інформації.
3. Криптосистема шифрування даних RSA.

Література: 1-12

Практичне заняття № 8-9

Тема: Засоби аутентифікації користувачів і аналізу безпеки системи.

Мета: Вивчення та дослідження засобів аутентифікації користувачів і аналіз безпеки системи. Навчитися налаштовувати елементи керувати безпекою під час управління обліковим записом.

Питання для обговорення:

1. Розмежування доступу до інформації.
2. Ідентифікація, аудентифікація, авторизація.
3. Системи аудиту та моніторингу.

Література: 1-12

Практичне заняття № 10-11

Тема: Використання цифрових підписів.

Мета: Зрозумітит концепцію цифрового підпису.

Питання для обговорення:

1. Електронний підпис: види та використання.
2. Онлайн інфмтрументи для електронного підпису.

Література: 1-12

Практичне заняття № 12

Тема: Відновлення даних з різних носіїв інформації.

Мета: Вивчення та дослідження засобів відновлення даних з різних носіїв інформації.

Питання для обговорення:

1. Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації
2. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних

Література: 1-12

Практичне заняття № 13

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.

2. Стратегії управління ризиками.
3. Стандарти безпеки, законодавство та регулювання в галузі кібербезпеки.

Література: 1-12

Практичне заняття № 14

Тема: Засоби управління, збереження, доступу до паролів та правила роботи з ними.

Мета: Вивчення та дослідження засобів управління, збереження, доступу до паролів та правила роботи з ними.

Питання для обговорення:

1. Управління паролями.
2. Засоби збереження та доступу до паролів.
3. Правила роботи з паролями.

Література: 1-12

Заочна форма

Змістовий модуль 1. Основи знань про інформаційу безпеку

Практичне заняття № 1

Тема: Основи інформаційної безпеки

Мета: Вивчення та дослідження інформаційної безпеки.

Питання для обговорення:

1. Поняття інформаційної безпеки.
2. Основні види безпеки.
3. Тріада (CIA): конфіденційність, цілісність, доступність.

Література: 1-12

Тема: Загрози інформаційній безпеці.

Мета: Вивчення та дослідження загроз безпеці інформації.

Питання для обговорення:

1. Класифікація загроз.
2. Типи атак на інформаційні системи.
3. Шкідливе програмне забезпечення. Основні типи та загальний огляд комп'ютерних вірусів.
4. Поняття антивірусної програми. Огляд найпоширеніших антивірусних програм та їх класифікація.

Література: 1-12

Тема: Безпека даних.

Мета: Вивчення та дослідження проблем інформаційної безпеки.

Питання для обговорення:

1. Концепція захисту інформації.
2. Захист конфіденційності, цілісності та доступності даних.
3. Методи аутентифікації, авторизації та аудиту даних.
4. Види забезпечення безпеки інформації.
5. Критерії оцінки інформаційної безпеки та аспекти захисту інформації

Література: 1-12

Тема: Політика безпеки інформації.

Мета: Вивчення та дослідження політики інформаційної безпеки.

Питання для обговорення:

1. Реалізація, підтримка політики безпеки.
2. Моделі політики безпеки.
3. Закони України про захист інформації.

Література: 1-12

Тема: Встановлення віртуальної машини на ПК

Мета: Навчитись встановлювати віртуальну машину.

1. Встановлення та початкове налагодження Virtual Box.
2. Створення віртуальної машини.
3. Додаткові налаштування віртуальної машини.
4. Підготовка віртуальної машини до встановлення операційної системи

Література: 1-12

Тема: Відновлення даних з різних носіїв інформації.

Мета: Вивчення та дослідження засобів відновлення даних з різних носіїв інформації.

Питання для обговорення:

1. Поняття захисту інформації та інформаційної безпеки. Критерії оцінки інформаційної безпеки. Аспекти захисту інформації
2. Засоби резервного копіювання та відновлення даних. Пристрої відновлення даних

Література: 1-12

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.
2. Стратегії управління ризиками.
3. Стандарти безпеки, законодавство та регулювання в галузі кібербезпеки.

Література: 1-12

Тема: Засоби управління, збереження, доступу до паролів та правила роботи з ними.

Мета: Вивчення та дослідження засобів управління, збереження, доступу до паролів та правила роботи з ними.

Питання для обговорення:

1. Управління паролями.
2. Засоби збереження та доступу до паролів.
3. Правила роботи з паролями.

Література: 1-12

Практичне заняття № 2

Тем: Криптографічний вид захисту інформації. Поняття шифрування файлів, папок, повідомлень. Засоби здійснення шифрування повідомлення.

Мета: Розглянути базові поняття теорії чисел, отримання практичних навичок шифрування і дешифрування повідомлень за допомогою відкритого та закритого ключа криптосистеми RSA з використанням теорії чисел.

Питання для обговорення:

1. Основні поняття криптографії, способи шифрування файлів, папок, повідомлень; криптографічні методи захисту інформації, основні засоби здійснення криптографічного захисту інформації
2. Використання теорії чисел для захисту інформації.
3. Криптосистема шифрування даних RSA.

Література: 1-12

Тема: Засоби аутентифікації користувачів і аналізу безпеки системи.

Мета: Вивчення та дослідження засобів аутентифікації користувачів і аналіз безпеки системи. Навчитися налаштовувати елементи керувати безпекою під час управління обліковим записом.

Питання для обговорення:

1. Розмежування доступу до інформації.
2. Ідентифікація, аудентифікація, авторизація.
3. Системи аудиту та моніторингу.

Література: 1-12

Тема: Використання цифрових підписів.
Мета: Зрозумітит концепцію цифрового підпису.
Питання для обговорення:
1. Електронний підпис: види та використання.
2. Онлайн інфмтрументи для електронного підпису.

Література: 1-12

6. Тренінг з дисципліни

Мета тренінгу з дисципліни «Інформаційа безпека» – оволодіння новими навиками візуалізації інформації. Успішне проходження тренінгу сприяє посиленню практичної спрямованості у підготовці фахівців за ступенем вищої освіти «бакалавр».

Проведення тренінгу дозволяє: забезпечити практичне засвоєння теоретичних знань, отриманих у процесі вивчення дисципліни «Інформаційна безпека»; виробити у студентів навички візуального представлення інформації.

Організація і порядок проведення тренінгу

1. Вступна частина. Актуалізація теми тренінгового заняття та структуризація процесу його проведення. Ознайомлення студентів з метою тренінгу, його завданнями, процедурою проведення, очікуваними результатами. Представлення програми тренінгу.

2. Організаційна частина. Встановлення правил проведення тренінгу, визначення завдань та розподіл ролей. Забезпечення учасників тренінгу інструкціями.

3. Практична частина. Виконання тренінгових завдань із використанням базових та інноваційних методів проведення тренінгу за визначеною темою. Підготовка презентаційних матеріалів за результатами виконання тренінгового завдання.

4. Підведення підсумків. Обговорення результатів виконаних завдань, підведення підсумків, оцінка результативності роботи та досягнення поставлених цілей тренінгу. Результати роботи представляються у звіті (файл .docx).

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 т азагроз.

Оцінюються виконані завдання max в 100 балів.

7. Самостійна робота студентів

Самостійна робота студентів має на меті формування пізнавальної активності студентів, засвоєння ними основних умінь та навичок роботи з навчальними матеріалами, поглиблення та розширення вже набутих знань, підвищення рівня організованості студентів тощо.

У процесі самостійної роботи студенти мають оволодіти вміннями та навичками:

- організації самостійної навчальної діяльності;
- самостійної роботи в бібліотеці з каталогами;
- праці з навчальною, навчально-методичною, науковою, науково-популярною літературою;
- роботи з довідковою літературою;
- обробки зібраної інформації з використанням технічних засобів і програм;
- послуговування інтернет-ресурсами.

Для набуття умінь самостійного мислення і самоконтролю у студентів особливе значення має виконання індивідуального завдання з дисципліни «Інформаційна безпека», яке виконується самостійно кожним студентом згідно методичних рекомендацій та інструкцій. Воно охоплює основні теми дисципліни та має на меті засвоєння теоретичного матеріалу, оволодіння навиками застосування набутих теоретичних знань щодо захисту інформаційної безпеки, і є одним із обов'язкових складових модулів залікового кредиту з дисципліни.

Завдання:

Написання реферату на тему (max 100 балів):

1. Державна таємниця
2. Матеріальні носії секретної інформації
3. Система захисту державної таємниці
4. Допуск до державної таємниці
5. Гриф секретності
6. Ступінь секретності
7. Інформаційна безпека держав.
8. Поняття інформаційної безпеки держави, суспільства та особи
9. Загрози інформаційної безпеки
10. Система забезпечення інформаційної безпеки України.
11. Державна політика в інформаційній сфері та забезпечення інформаційної безпеки
12. Державна політика інформаційної безпеки як інструмент забезпечення інформаційної безпеки держави
13. Безпека інформації, інформаційних ресурсів та інформаційної інфраструктури
14. Національні інформаційні ресурси.
15. Система національних інформаційних ресурсів
16. Поняття та основні задачі інформаційної безпеки
17. Загрози інформаційної безпеки
18. Системи забезпечення інформаційної безпеки
19. Основні сервіси безепеки
20. Особливості сучасних інформаційних систем з погляду безпеки
21. Фізичні засоби захисту
22. Інформаційна безпека в електронному урядуванні
23. Інформаційні виборчі технології
24. Огляд міжнародних стандартів у галузі інформаційна безпека
25. Основні положення теорії захисту інформації
26. Сутність та види атак на комп'ютерну мережу
27. Реалізація системи захисту інформації в комп'ютерних системах і мережах
28. Інформаційне та правове забезпечення електронних видань і цифрової передачі даних в Україні

29. Міжнародна інформаційна безпека
30. Технологія реалізації атак на комп'ютерну систему та мережу
31. Законодавча база в галузі захисту інформації
32. Основні поняття і аналіз загроз інформаційної безпеки
33. Проблеми інформаційної безпеки мереж
34. Політики безпеки
35. Стандарти інформаційної безпеки
36. Принципи криптографічного захисту інформації
37. Криптографічні алгоритми
38. Технології аутентифікації
39. Забезпечення безпеки операційних систем
40. Технології міжмережевих екранів
41. Основи технології віртуальних захищених мереж VPN
42. Захист на канальному і сеансовому рівнях
43. Захист на мережевому рівні – протокол IPSEC
44. Інфраструктура захисту на прикладному рівні
45. Аналіз захищеності і виявлення атак
46. Захист від вірусів
47. Методи управління засобами мережевої безпеки

Роботу «Інформаційна безпека» слід оформляти у відповідності до вимог, розроблених і затверджених кафедрою. Обсяг – 12-15 друкованих сторінок. Остаточно оформлений реферат підлягає доповіді в режимі співбесіди з викладачем. Для визначення рівня та якості засвоєння теоретичного і фактичного матеріалу приймаються такі вимоги: 1) зміст реферату, його відповідність темі, повнота розкриття теми, логіка і послідовність написання тексту, самостійність думок, міркувань, суджень; 2) використання, крім рекомендованої літератури, періодичних видань та інформації з мережі Internet; 3) відповідність оформлення реферату вимогам нормативних документів; 4) змістовність, логічність, лаконічність відповіді та відповідей на запитання, володіння матеріалом обраної теми. Оцінюється реферат max в 100 балів..

8. Методи навчання

У навчальному процесі застосовуються: лекції, практичні та індивідуальні заняття, консультації, самостійна робота, метод опитування, тестування.

9. Засоби оцінювання та методи демонстрування результатів навчання

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

- стандартизовані тести;
- поточне опитування, виконання лабораторних робіт та їх захист;
- оцінювання результатів модульної контрольної роботи;
- залікове модульне тестування;
- презентації результатів виконаних завдань;
- оцінювання результатів самостійної роботи;
- екзамен.

10. Політика оцінювання

Політика щодо дедлайнів і перескладання. Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності. Використання друкованих і електронних джерел інформації під час контрольних заходів та екзаменів заборонено.

Політика щодо відвідування. Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівником курсу з дозволу дирекції факультету.

11. Критерії, форми поточного та підсумкового контролю

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

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульна контрольна робота	Поточне оцінювання	Модульна контрольна робота	Тренінги	Самостійна робота	Екзамен
Оцінка визначається як середнє арифметичне з оцінок, отриманих на практичних заняттях (теми 1-5)	Письмова робота по темах 1-5	Оцінка визначається як середнє арифметичне з оцінок, отриманих на практичних заняттях (теми 6-10)	Письмова робота по темах 6-10	Оцінка визначається як середнє арифметичне з оцінок, отриманих на тренінгу	Оцінка визначається як середнє арифметичне з оцінок, отриманих за написання реферату, виступ та захист	1. Тестові завдання (2 тестів по 2 бали) – max 40 балів 2. Практичні завдання (2) – max 60 балів.

Шкала оцінювання:

За шкалою ЗУНУ	**За національною шкалою**	**За шкалою ECTS**
90–100	відмінно	A (відмінно)
85-89	добре	B (дуже добре)
75–84		C (добре)
65–74	задовільно	D (задовільно)
60-64		E (достатньо)
35–59	незадовільно	FX (незадовільно з можливістю повторного складання)
1–34		F (незадовільно з обов'язковим повторним курсом)

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

№	Найменування	Номер теми
1.	Мультимедійний проєктор	1 – 10
2.	Проєкційний екран	1 – 10
3.	Комунікаційне програмне забезпечення (Internet Explorer, Google Chrome, Firefox)	1 – 10
4.	Наявність доступу до мережі Інтернет	1 – 10
5.	Персональні комп'ютери	1 – 10
6.	Комунікаційне програмне забезпечення (Zoom), сервіс Google Meet для проведення занять у режимі он-лайн (за необхідності)	1 – 10
7.	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 – 10

8.	Програмне забезпечення: ОС Windows	1 – 10
9.	Віртуальні машини Інструменти для викриття зловмисних інформаційцних впливів у мережі	1 – 10

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Закон України «Про основні засади забезпечення кібербезпеки України» зі змінами. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403, зі змінами від 28.07.2022 року. Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19#Text
2. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.
3. Вишняков В.М. Захист інформації в комп'ютерних системах: навч. посіб. Київ: КНУБА, 2022. 120 с.
4. Інформаційна безпека. Яковенко Є., Журавель І., Горбатий І., Бондарєв А. Видавництво Львівська політехніка, 2019. 580 с.
5. Костюченко А.О., Горошко Ю.В. Віртуалізація операційних систем: навчально-методичний посібник. Ч.: ФОП Баликіна С.М., 2021. 56 с.
6. Методичні вказівки до виконання лабораторних робіт з курсу “Основи кібербезпеки” для студентів спеціальностей “Кібербезпека” / Укл.: Яцків В. В. Тернопіль: Економічна думка, 2018. 44 с.
7. Методичні вказівки до лабораторних робіт з дисципліни “Програмно-апаратне забезпечення та захист мобільних пристроїв” укл. Лаптєв О.А., Гришанович Т. О., Жолоб Я. В., Жигаревич О. К. [Електронний ресурс]; ВНУ імені Лесі Українки. Електронні текстові данні (1 файл: 859 КБ). Луцк. 2022. 99 с.
8. Управління інформаційною безпекою: конспект лекцій [Електронний ресурс] : навч. посіб. для студ. спец. 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. – Електронні текстові дані (1 файл: 1114 Кбайт). Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.
9. AlFardan, N. (2023). Cyber threat hunting. Manning, 2023. 442 p.
10. Adedoyin, F. F., & Christiansen, B. (2023). Effective cybersecurity operations for Enterprise-Wide systems. Information Science Reference. 2023. 344 p.
11. Alexandrou, A. (2021). Cybercrime and internet technology: Theory and Practice. CRC Press, 2022. 455p.
12. Dr. Hidaia Mahmood Alassouli. (2021). Common Windows, Linux and Web Server Systems Hacking Techniques, 2021. 171 p.