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

ЗАТВЕРДЖУЮ
Декан факультету комп'ютерних інформаційних технологій
_____ Ігор ЯКИМЕНКО
«_29_» _08_____ 20_25_р.

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної роботи
_____ Віктор ОСТРОВЕРХОВ
«_29_» _08_____ 20_25_р.

РОБОЧА ПРОГРАМА

з дисципліни

«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

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

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лабор. заняття (год.)	ІРС (год.)	Тренінг, (год.)	СРС (год.)	Разом (год.)	Залік / екзамен (семестр)
Денна	3	6	30	30	4	8	48	120	Екзамен (6)

29.08.2025

Тернопіль – 2025

Робоча програма складена на основі освітньо-професійної програми «Кібербезпека» першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека та захист інформації галузі знань 12 Інформаційні технології, затвердженої Вченою радою ЗУНУ,
протокол №10 від 23.06.2023р.

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 26.08.2025р.

Завідувач кафедри
кібербезпеки  Василь ЯЦКІВ

Гарант освітньо-професійної
програми  Михайло КАСЯНЧУК

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 – 5	Спеціальність 125 «Кібербезпека та захист інформації»	Рік підготовки: 3 Семестр: 6
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції: 30 год. Лабораторні заняття: 30 год.
Загальна кількість годин – 120		Самостійна робота: 48 год. Тренінг: 8 год. Індивідуальна робота:4 год.
Тижневих годин – 8 з них аудиторних – 4		Вид підсумкового контролю – екзамен

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 здобувачами 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 здобувачів цілісної системи теоретичних знань з курсу «Управління інформаційною безпекою».

Проведення практичних занять забезпечує формування у здобувачів 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 застосовувати знання у практичних ситуаціях.

Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі 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», «Програмування», «Архітектура комп'ютерів та систем», «Комп'ютерні мережі», «Операційні системи», «Кібернетична безпека», «Оцінка та управління ризиками», а також цілеспрямованої роботи на лекційних та лабораторних заняттях, самостійної роботи.

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, автентифікації, 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).

Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

Вирішувати задачі захисту потоків даних в інформаційних, інформаційно телекомунікаційних (автоматизованих) системах.

Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

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.

Тема 2. Загрози безпеці інформації.

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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Тема 15. Система управління інформаційною безпекою.

1. Проблематика впровадження СУІБ у державних установах. 2. Нормативно-правові аспекти у сфері інформаційної безпеки. 3. Структура системи кіберзахисту. 4. Алгоритм організації СУІБ. 5. Взаємозв'язки між ключовими компонентами та етапами процесу впровадження СУІБ. 6. Життєвий цикл СУІБ. 7. План-графік впровадження СУІБ. 8. Практичні рекомендації щодо реалізації СУІБ.

4. Структура залікового кредиту дисципліни

	Кількість годин					
	Лекції	Лаборат. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Основні положення управління інформаційною безпекою.						
Тема 1. Інформаційні ресурси, що підлягають захисту.	2	2	3	1	2	Поточне опитування
Тема 2. Загрози безпеці інформації.	2	2	3			
Тема 3. Характеристики захищеності інформаційних ресурсів. Модель CIA.	2	2	3			
Тема 4. Політика інформаційної безпеки.	2	2	4			
Тема 5. Соціотехнічна безпека.	2	2	3			
Змістовий модуль 2. Інформаційна безпека держави						
Тема 6. Національна безпека.	2	2	3	1	2	Поточне опитування
Тема 7. Кіберзлочинність.	2	2	3			
Тема 8. Інформаційне протиборство.	2	2	3			

Інформаційна війна.						
Змістовий модуль 3. Організація управління інформаційною безпекою						
Тема 10. Аналіз ризиків	2	2	4	2	4	Поточне опитування
Тема 9. Управління ризиками інформаційної безпеки	2	2	3			
Тема 12. Аналіз інцидентів інформаційної безпеки	2	2	3			
Тема 11. Реагування на інциденти інформаційної безпеки	2	2	3			
Тема 13. Стримування та пом'якшення наслідків інцидентів	2	2	3			
Тема 14. Розслідування інцидентів	2	2	3			
Тема 15. Система управління інформаційною безпекою	2	2	4			
Разом	**30**	**30**	**48**	**4**	**8**	

5. Тематика лабораторних робіт.

Лабораторна робота №1

Тема: Аналіз вразливостей мережі та управління безпекою

Мета роботи: Ознайомитися з основами аналізу мережевих вразливостей, навчитися використовувати інструменти сканування мережі та аналізу трафіку для виявлення потенційних загроз.

Питання для обговорення: 1. Загрози, що можуть бути пов'язані з відкритими портами у мережі. 2. Можливості Wireshark для виявлення вразливості у трафіку. 3. Методи захисту, що застосовуються для запобігання несанкціонованому скануванню мережі. 4. Відмінності шифрованого та незашифрованого трафіку. 5. Шляхи обмеження можливості сканування мережі.

Лабораторна робота № 2

Тема: Виявлення фішингових атак та захист.

Мета роботи: Ознайомитися з методами фішингових атак, навчитися виявляти підозрілі електронні листи та перевіряти безпечність посилань за допомогою доступних інструментів.

Питання для обговорення: 1. Засоби, що допомагають в тестуванні фішингових атак. 2. Ознаки, що можуть свідчити про фішинговий лист. 3. Можливості VirusTotal для перевірки безпечності посилань і файлів. 4. Шляхи зниження ризику фішингових атак для користувачів. 5. Способи захисту поштової скриньки від фішингових листів.

Лабораторна робота №3

Тема: Аналіз вразливостей веб-ресурсів.

Мета роботи: Ознайомитися з основами сканування веб-ресурсів на наявність вразливостей, навчитися використовувати інструмент для виявлення потенційних загроз.

Питання для обговорення: 1. Загрози, що можуть виникнути через відсутність заголовків безпеки. 2. Шляхи запобігання атакам через SQL ін'єкції та XSS на веб-серверах. 3. Налаштування для захисту веб-сервера від загроз, виявлених за допомогою Nikto. 4. Використання Nikto для перевірки на застарілі версії ПЗ та їх потенційні уразливості.

Лабораторна робота №4

Тема: Налаштування міжмережевого екрану та контроль мережевого трафіку.

Мета роботи: Навчитися налаштовувати міжмережевий екран, керувати мережевими правилами та аналізувати потоки трафіку для підвищення безпеки мережі.

Питання для обговорення: 1. Основні функції міжмережевого екрану. 2. Типи міжмережевих екранів. 3. Відмінності між становою фільтрацією та безстановою 4. Засоби та шляхи перевірики роботи міжмережевого екрану 5. Методи обходу міжмережевих екранів, що можуть використовуватися зловмисниками.

Лабораторна робота №5

Тема: Управління безпекою облікових записів.

Мета роботи: Ознайомитися з принципами створення та впровадження політик безпеки облікових записів, дослідити методи аналізу стійкості паролів, навчитися використовувати

інструменти для перевірки їхньої вразливості та оцінити ефективність різних підходів до управління безпекою паролів у сучасних інформаційних системах

Питання для обговорення: 1. Основні вимоги, що висуваються сучасними політиками безпеки паролів. 2. Алгоритми хешування паролів їх характеристики. 3. Основні методи атак на паролі та їх ефективність. 4. Відмінності brute force, атаки зі словником та гібридних атак. 5. Інструменти, що використовуються для злому хешів. 6. Заходи для підвищення безпеки облікових записів та паролів.

Лабораторна робота № 6

Тема: Методи хешування паролів та використання солі для підвищення їх стійкості й безпечного зберігання.

Мета роботи: Ознайомитися з різними методами хешування паролів, дослідити вплив використання солі на їх стійкість, а також проаналізувати сучасні алгоритми хешування безпечного зберігання паролів.

Питання для обговорення: 1. Алгоритми хешування, що вважаються стійкими до криптографічних атак. 2. Вплив параметрів хешування на безпечне зберігання паролів. 3. Роль солі у хешуванні паролів та її переваги. 4. Критерії оцінки стійкості паролів.

Лабораторна робота № 7

Тема: Забезпечення цілісності та конфіденційності даних під час передавання.

Мета роботи: Ознайомитися з методами забезпечення цілісності та конфіденційності даних під час передавання, навчитися використовувати криптографічні інструменти для шифрування, дешифрування та цифрового підпису файлів.

Питання для обговорення: 1. Відмінності між шифруванням і хешуванням. 2. Цифровий підпис, процес створення та перевірки. 3. Механізми управління ключами.

Лабораторна робота №8

Тема: Тестування на проникнення.

Мета роботи: Ознайомитися з основами тестування на проникнення для оцінки рівня захищеності інформаційних систем, навчитися використовувати інструменти для проведення тестів на проникнення, виявлення вразливостей та розробки рекомендацій для підвищення безпеки.

Питання для обговорення: 1. Етапи тестування на проникнення. 2. Виявлення відкритих портів, аналіз трафіку. 3. Пошук вразливостей. 4. Використання експлойта. 5. Пост-експлуатаційний аналіз..

Лабораторна робота №9

Тема: Розпізнавання і протидія атакам типу DDoS.

Мета роботи: Ознайомитися з методами виявлення та протидії атакам типу DDoS (Distributed Denial of Service), які спрямовані на блокування доступу до ресурсів в Інтернеті шляхом перевантаження серверів запитами.

Питання для обговорення: 1. Основні ознаки DDoS-атаки. 2. Типи DDoS-атак. 3. Реагування на підозрілі запити, блокування IP-адрес 4. Виявлення аномального трафіку. 5. Основні заходи захисту веб-сервера від DDoS-атак.

Лабораторна робота № 10

Тема: Впровадження та управління політиками безпеки в Linux.

Мета роботи: Ознайомитися з методами керування доступом і налаштування аудиту в Linux, навчитися застосовувати механізми контролю доступу, аудиту та моніторингу дій користувачів.

Питання для обговорення: 1. Основні механізми контролю доступу в Linux. 2. Налаштувати ACL для розширеного контролю доступу до файлів та каталогів. 3. Основні можливості системи аудиту 4. Журнали подій. 5. Методи заборони доступу до системи через SSH. 5. Обмеження використання USB-накопичувачів.

Лабораторна робота № 11

Тема: Впровадження та управління політиками безпеки в Windows.

Мета роботи: Ознайомитися з методами упарвління доступом та налаштуванням політик безпеки в Windows, навчитися застосовувати механізми контролю доступу, обмеження прав користувачів та аудиту дій у системі.

Питання для обговорення: 1. Способи налаштування локальних політик безпеки в ОС Windows. 2. Методи обмеження доступу до файлів та каталогів в Windows, і їх реалізацыя 3.

Розширене налаштування прав доступу користувачів. 4. Обмеження підключення до системи через SSH у Windows. 5. Обмеження використання USB-накопичувачів. 6. Основні можливості системи аудиту, перегляд журнал подій.

Лабораторна робота № 12

Тема: Системи виявлення та запобігання вторгнень

Мета роботи: Ознайомитися з принципами роботи систем виявлення та запобігання вторгнень (IDS/IPS), навчитися налаштовувати та аналізувати їх роботу для підвищення рівня безпеки мережі.

Питання для обговорення: 1. Відмінності між IDS та IPS. 2. Методи, що використовують IDS/IPS для виявлення атак. 3. Шляхи підвищення ефективості правил виявлення атак у Snort та Suricata. 4. Аналіз журналів IDS/IPS для виявлення потенційних загроз. 5. Недоліки IDS/IPS систем.

Лабораторна робота № 13

Тема: Оцінка ризиків інформаційної безпеки

Мета роботи: Ознайомитися з методами оцінки ризиків для організаційних систем інформаційної безпеки, навчитися застосовувати методи оцінки ризиків, такі як OCTAVE, NIST SP 800-30 або ISO/IEC 27005, для ідентифікації, оцінки та управління інформаційними ризиками.

Питання для обговорення: 1. Методи оцінки ризиків, їх основні характеристики та відмінності. 2. Етапи процесу оцінки ризиків в організації. 3. Оцінка наслідків вразливостей у процесі аналізу ризиків.

Лабораторна робота № 14

Тема: Моніторинг безпеки з використанням SIEM-систем

Мета роботи: Ознайомитися з системами моніторингу безпеки в реальному часі (SIEM), їх налаштуванням та використанням для збору, аналізу і кореляції логів подій безпеки.

Питання для обговорення: 1. Налаштувати SIEM-системи для збору даних. 2. Інструменти кореляції подій безпеки. 3. Можливості SIEM-системи у виявленні аномалій та загроз.

6. Організація та проведення тренінгу з курсу.

Порядок проведення тренінгу:

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

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

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 та засобів для управління інформаційною безпекою.

Мета тренінгу: забезпечення здобувачів теоретичними знаннями та практичними навичками щодо аналізу загроз та застосування методів захисту інформаційних ресурсів для ефективного управління інформаційною безпекою.

Завдання тренінгу: презентація результатів, що можуть включати огляд виявлених загроз та ризиків; опис обраних методів чи засобів захисту та особливостей їх реалізації; оцінку ефективності розглянутих рішень у сфері управління інформаційною безпекою на основі конкретних сценаріїв, тощо. Здобувачі обирають одну із запропонованих тем або формулюють власну тему дослідження у межах проблематики управління інформаційною безпекою. для підготовки короткої доповіді з подальшим обговоренням у групі.

Орієнтована тематика:

1. Складові системи управління інформаційною безпекою – основні елементи та їх взаємозв’язок.
2. Найпоширеніші загрози інформаційній безпеці – класифікація та приклади.
3. Політики безпеки та організаційні процедури – роль у захисті інформаційних ресурсів.
4. Методи контролю доступу до інформації – переваги та обмеження.
5. Комплексні системи захисту інформації – принципи побудови та приклади застосування.
6. Державні стандарти та нормативи у сфері інформаційної безпеки – вплив на організаційні рішення.

7. Ліцензування та сертифікація засобів інформаційної безпеки – основні положення та значення.
8. Технічні канали витоку інформації – виявлення та способи контролю.
9. Моделі порушника та оцінка ризиків – аналіз потенційних загроз та вразливостей.
10. Оцінка рівня інформаційної безпеки інформаційних ресурсів організації – методи та критерії.
11. Порівняння національних і міжнародних стандартів управління інформаційною безпекою – ключові відмінності.
12. Технологічне управління безпекою інформації – основні функції та практичне застосування.
13. Приклади успішного впровадження систем менеджменту інформаційної безпеки – кейси та уроки.
14. Контроль і моніторинг ефективності системи захисту інформації – інструменти та методики.
15. Проблеми та шляхи вдосконалення інформаційної безпеки у сучасних організаціях – обговорення актуальних викликів.

7. Самостійна робота

Виконання самостійної роботи є одним із обов'язкових складових модулів залікового кредиту. Вона спрямована на розвиток умінь аналізувати теоретичний матеріал, опрацьовувати навчальну та наукову літературу, робити висновки та узагальнення, а також представляти власні результати у вигляді презентації.

Метою виконання є оволодіння навичками управління інформаційною безпекою, включаючи аналіз загроз та застосування відповідних методів захисту інформаційних ресурсів при вирішенні задач кібербезпеки.

Завдання:

1. Обрати тему із запропонованого переліку (або узгодити власну тему у межах курсу).
2. Опрацювати навчальні та наукові джерела з обраної теми.
3. Підготувати презентацію, яка повинна містити:
   - короткий теоретичний огляд теми;
   - приклади практичної реалізації чи застосування;
   - висновки та узагальнення.
4. Представити результати у формі доповіді з подальшим обговоренням.

Орієнтовна тематика:

1. Основні положення щодо організації системи захисту інформації.
2. Система захисту інформації у контексті системного мислення та системного підходу.
3. Державна таємниця і конфіденційна інформація, що є власністю держави.
4. Недержавна конфіденційна і відкрита інформація, що потребує захисту.
5. Дослідження структури і умов функціонування інформаційної системи установи.
6. Виявлення загроз безпеки інформаційним ресурсам, які підлягають захисту.
7. Технічні канали витоку інформації та НСД в комп'ютерних системах.
8. Джерела загроз і модель порушника.
9. Проведення оцінки вразливості і ризиків для інформаційних ресурсів.
10. Оцінка ефективності методів захисту інформації від технічних витоків.
11. Захист інформації в комп'ютерних системах від несанкціонованого доступу.
12. Критерій і особливості проектування оптимальної системи захисту інформації.
13. Технічне завдання на розробку СЗІ. План захисту інформації.
14. Аналіз якості та ефективності реалізованої системи захисту інформації.
15. Контроль функціонування і управління системою захисту.
16. Структура та вимоги забезпечення інформаційної безпеки.

8. Методи навчання.

У освітньому 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 «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;

– оцінювання тренінгів;

– оцінювання результатів самостійної роботи;

– підсумковий екзамен.

10. Політика оцінювання.

Політика щодо дедлайнів і перескладання. Для всіх видів навчальних завдань і контрольних заходів встановлюються чіткі дедлайни. Роботи, здані із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (-10 балів). Перескладання проводиться у встановленому порядку.

Політика щодо академічної доброчесності. Здобувач зобов'язаний виконувати усі роботи та завдання самостійно. Під час контрольного заходу він може користуватися лише дозволеними допоміжними матеріалами або засобами; йому забороняється в будь-якій формі обмінюватися інформацією з іншими здобувачами, а також використовувати, розповсюджувати або збирати варіанти чужих робіт чи контрольних завдань.

Політика щодо відвідування. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись у дистанційній формі за погодженням із керівником курсу та з дозволу дирекції факультету.

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:

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
Середнє арифметичне оцінок, отриманих за поточне опитування та підсумкове модульне тестування за темами №1-7.	Середнє арифметичне за виконання та захист лабораторних робіт №1-7.	Середнє арифметичне оцінок, отриманих за поточне опитування та підсумкове модульне тестування за темами №8-15.	Середнє арифметичне за виконання та за захист лабораторних робіт №8-14.	Середнє арифметичне з оцінок за виконання та презентацію одного завдання тренінгу.	Середнє арифметичне за виконання та презентацію одного завдання самостійної роботи.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Виконання лабораторних робіт:

90–100 балів – робота виконана самостійно, без помилок, усі етапи задокументовано, правильне використання інструментів.

75–89 балів – виконання із незначними помилками, що не вплинули на результат; часткова потреба в підказках.

60–74 бали – виконання із суттєвими помилками; поверхневе розуміння завдань.

1–59 балів – робота не виконана або результат неправильний; відсутність навичок.

Поточне опитування:

90–100 балів – повне володіння матеріалом, аргументовані й логічні відповіді, глибоке розкриття змісту.

75–89 балів – загалом повне володіння матеріалом, але окремі відповіді поверхневі або з незначними неточностями.

65–74 бали – знання основного змісту без достатньої глибини та аргументації, суттєві неточності.

60–64 бали – фрагментарне володіння матеріалом, недостатнє розкриття питань.

1–59 балів – відсутність знань, нездатність розкрити зміст теоретичних питань.

Тренінг, самостійна робота:

90–100 балів – повне володіння матеріалом, аргументоване застосування знань, правильне виконання завдань, наявність елементів власного дослідження, творчий підхід.

75–89 балів – здебільшого правильне виконання, незначні помилки, достатньо аргументоване використання матеріалу, частково присутні елементи власного дослідження.

65–74 бали – розв'язання завдань з помилками, недостатня аргументація, поверхневе опрацювання теми, обмежена самостійність.

60–64 бали – часткове або фрагментарне виконання завдань, відсутність повного обґрунтування, мінімальний авторський внесок.

1–59 балів – завдання практично не виконано, повністю неправильне розв'язання, відсутність дослідницького або творчого підходу.

Підсумкове модульне тестування:

90–100 балів – правильно виконано 90–100% завдань тесту.

75–89 балів – правильно виконано 75–89% завдань тесту.

60–74 бали – правильно виконано 60–74% завдань тесту.

1–59 балів – правильно виконано менше 60% завдань тесту.

Екзамен – підсумковий контроль, який проводиться з метою оцінювання засвоєння здобувачем вищої освіти теоретичного та практичного матеріалу. Екзаменаційне завдання складається з двох блоків:

Відповіді на теоретичні питання (максимум 60 балів):

25–30 балів – повне володіння матеріалом, аргументована та всебічна відповідь, демонстрація глибокого розуміння;

15–24 бали – достатнє володіння матеріалом, відповідь здебільшого правильна, допускаються незначні неточності;

0–14 балів – фрагментарне або неправильне викладення матеріалу, суттєві недоліки в аргументації.

Практичне завдання (тестове, максимум 40 балів):

30–40 балів – всі завдання виконані правильно, повне розуміння практичного матеріалу;

15–29 балів – завдання виконані частково правильно, допускаються незначні або суттєві помилки;

0–14 балів – завдання виконано неправильно або не виконано взагалі.

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	1-15
2	Персональні комп'ютери	1-15
3	Наявність доступу до мережі Інтернет	1-15
4	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1-15
5	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1-15

6	Спеціалізовані програмні продукти та інструментів (Nmap, Wireshark, Gophish, VirusTotal, Nikto, John the Ripper, Hashcat, OpenSSL, GPG, Metasploit, Fail2ban)	1-15

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Опорний конспект лекцій з дисципліни “Управління інформаційною безпекою” для здобувачів освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні спеціальності 125 «Кібербезпека» / Укл.: Давлетова А.Я., Драпак В.І., Возняк С.І. – Тернопіль 2022. – 76с.
2. Яцків В.В., Івасьєв С.В., Давлетова А.Я., Тимошенко Л.М. Методологія впровадження системи управління інформаційною безпекою на основі багаторівневої моделі кіберзахисту згідно з вимогами законодавства україни.- Інформатика та математичні методи в моделюванні Том 15, № 1, 2025, 137-149.
3. Шумейко О.О. Інформаційна безпека. Дніпровський державний технічний університет, 2019. - 155 с.
4. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.
5. Мужанова Т.М. Інформаційна безпека держави. Київ: Державний університет телекомунікацій, 2019. - 131 с.
6. Bender David. Bender on Privacy and Data Protection. LexisNexis, 2020. - 2940 p.
7. Schreider Tari. Building an Effective Security Program. 2nd Edition. - Rothstein Associates Inc., 2020. - 406 p.
8. Alassouli Hidaia. Common Windows, Linux and Web Server Systems Hacking Techniques. Independently published, 2021. - 181 p.
9. Barnum Todd. The Cybersecurity Manager's Guide: The Art of Building Your Security Program. O’Reilly Media, Inc., 2021. - 168 p.
10. Daimi K., Peoples C. Advances in Cybersecurity Management. Springer, 2021.- 497 p.
11. 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.
12. 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.