

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідас ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 1

ЗАТВЕРДЖЕНО

Вченою радою факультету
інформаційно-комп'ютерних технологій
28 серпня 2024 р. протокол № 8
Голова Вченої ради
Тетяна ПІКІТЧУК



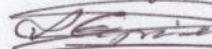
РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 25 «МЕРЕЖНА БЕЗПЕКА»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 123 «Комп'ютерна інженерія»
освітньо-професійна програма «Комп'ютерна інженерія»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерної інженерії та кібербезпеки

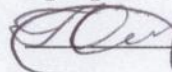
Схвалено на засіданні
кафедри комп'ютерної інженерії та
кібербезпеки

26 серпня 2024 р., протокол № 6

Завідувач кафедри

 Андрій ЄФІМЕНКО

Гарант освітньо-
професійної програми

 Олена ГОЛОВНЯ

Розробник: кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії та кібербезпеки Єфіменко Андрій Анатолійович

Житомир
2026-2027 н.р.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	<i>Екземпляр № 1</i>	<i>Арк 26 / 2</i>

Робоча програма навчальної дисципліни «Мережна безпека» для здобувачів вищої освіти освітнього ступеня «бакалавр» спеціальності 123 «Комп'ютерна інженерія» освітньо-професійна програма «Комп'ютерна інженерія» затверджена Вченою радою факультету інформаційно-комп'ютерних технологій від 28 серпня 2024 р., протокол № 8.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 3

1. Опис навчальної дисципліни

Найменування показників	Галузь знань, спеціальність, освітній ступінь	Характеристика навчальної дисципліни	
		денна форма навчання	
Кількість кредитів 9	Галузь знань 12 «Інформаційні технології»	Нормативна	
Модулів – 2	Спеціальність 123 «Комп'ютерна інженерія»	Рік підготовки:	
Змістових модулів – 4		3-й	
Загальна кількість годин – 270		Семестр	
		5-й	6-й
Тижневих годин для денної форми навчання: аудиторних – 6 (5-й семестр), 6 (6-й семестр) самостійної роботи – 2,4 (5-й семестр), 2,4 (6-й семестр)	Освітній ступінь «бакалавр»	Лекції	
		32 год.	32 год.
		Практичні	
		–	–
		Лабораторні	
		64 год.	64 год.
		Самостійна робота	
		39 год.	39 год.
		Вид контролю: 5 семестр – залік, 6 семестр – екзамен , курсний проект	

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 67% аудиторних занять, 33% самостійної та індивідуальної роботи;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 4

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є: дати студентам знання базових понять теорії, принципів побудови, стандартів, алгоритмів функціонування сучасних захищених комп'ютерних систем та мереж, знання базових підходів до побудови, технологій, протоколів, обладнання, програмного забезпечення в сфері захисту комп'ютерних систем та мереж.

Завданнями вивчення навчальної дисципліни є:

- розуміння основ організації і функціонування комп'ютерних систем та мереж, їх стандартів, протоколів та сервісів, що надаються;
- розуміння основних видів загроз інформації в комп'ютерних системах та мережах;
- розуміння основних методів і засобів реалізації віддалених мережевих атак на комп'ютерні системи та мережі;
- розуміння та оволодіння основними методами і засобами протидії віддаленим мережевим атакам на комп'ютерні системи та мережі;
- розуміння та оволодіння основними протоколами безпеки, програмними та апаратними засобами захисту інформації в комп'ютерних системах та мережах;
- розуміння організаційно-правових та нормативних основ захисту інформації в комп'ютерних системах та мережах;
- знання та розуміння основ побудови комплексної системи захисту для ресурсів комп'ютерних систем та мереж;
- розуміння основних тенденцій та закономірностей розвитку комп'ютерних систем та мереж і засобів їх реалізації;
- знання основних тенденції і закономірності розвитку засобів і методів захисту інформації в комп'ютерних системах та мережах.
- визначення і усунування основних загрози інформаційної безпеки для комп'ютерних систем та мереж;
- вміння будувати модель порушника інформаційної безпеки комп'ютерних систем та мереж;
- вміння виявляти і усувати вразливості в основних компонентах комп'ютерних систем та мереж;
- вміння виявляти, переривати та попереджувати віддалені мережеві атаки за їх характерними ознаками;
- вміння розробляти політику інформаційної безпеки для комп'ютерних систем та мереж;
- вміння проектувати і реалізовувати комплексну системи забезпечення інформаційної безпеки комп'ютерних систем та мереж;
- вміння тестувати і на основі результатів тестування робити обґрунтований вибір засобів захисту для комп'ютерних систем та мереж;

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 5

– вміння здійснювати моніторинг мережевої безпеки адмініструвати комп'ютерні системи та мережі.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених стандартом вищої освіти зі спеціальності 123 «Комп'ютерна інженерія» та освітньо-професійною програмою «Комп'ютерна інженерія»:

КЗ 1. Здатність до абстрактного мислення, аналізу і синтезу.

КЗ 2. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 3. Здатність застосовувати знання у практичних ситуаціях.

КЗ 7. Вміння виявляти, ставити та вирішувати проблеми.

КЗ 12. Здатність до розуміння предметної галузі та професійної діяльності.

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії.

КФ 2. Здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення.

КФ 4. Здатність забезпечувати захист інформації, що обробляється в комп'ютерних та кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки.

КФ 5. Здатність використовувати засоби і системи автоматизації проектування до розроблення компонентів комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем тощо.

КФ 6. Здатність проектувати, впроваджувати та обслуговувати комп'ютерні системи та мережі різного виду та призначення.

КФ 8. Готовність брати участь у роботах з впровадження комп'ютерних систем та мереж, введення їх до експлуатації на об'єктах різного призначення.

КФ 9. Здатність системно адмініструвати, використовувати, адаптувати та експлуатувати наявні інформаційні технології та системи.

КФ 10. Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації.

КФ 12. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних та кіберфізичних систем, мереж та їхніх компонентів шляхом використання аналітичних методів і методів моделювання.

КФ 14. Здатність проектувати системи та їхні компоненти з урахуванням усіх аспектів їх життєвого циклу та поставленої задачі, включаючи створення, налаштування, експлуатацію, технічне обслуговування та утилізацію.

КФ 15. Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 6

КФ 17. Здатність забезпечувати проектування та розроблення програмних і технічних засобів комп'ютерних систем та мереж.

КФ 18. Здатність організовувати збір, оброблення та зберігання даних у базах та сховищах даних, передачу та захист інформації в комп'ютерних системах та мережах.

КФ 19. Здатність застосовувати сучасні інформаційні технології, технології комп'ютерної інженерії, методи та засоби забезпечення кібербезпеки та захисту інформації під час виконання функціональних завдань та обов'язків.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 123 «Комп'ютерна інженерія» та освітньо-професійною програмою «Комп'ютерна інженерія»:

РН 1. Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.

РН 2. Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.

РН 3. Знати новітні технології в галузі комп'ютерної інженерії.

РН 4. Знати та розуміти вплив технічних рішень в суспільному, економічному, соціальному і екологічному контексті.

РН 6. Вміти застосовувати знання для ідентифікації, формулювання і розв'язування технічних задач спеціальності, використовуючи методи, що є найбільш придатними для досягнення поставлених цілей.

РН 7. Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.

РН 9. Вміти застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення технічних задач спеціальності.

РН 11. Вміти здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії.

РН 13. Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.

РН 14. Вміти поєднувати теорію і практику, а також приймати рішення та виробляти стратегію діяльності для вирішення завдань спеціальності з урахуванням загальнолюдських цінностей, суспільних, державних та виробничих інтересів.

РН 15. Вміти виконувати експериментальні дослідження за професійною тематикою.

РН 16. Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення.

РН 19. Здатність адаптуватись до нових ситуацій, обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	<i>Екземпляр № 1</i>	<i>Арк 26 / 7</i>

РН 20. Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.

РН 21. Якісно виконувати роботу та досягати поставленої мети з дотриманням вимог професійної етики.

РН 23. Використовувати знання з фундаментальних природничих, математичних та загально-інженерних дисциплін для вирішення типових завдань проєктування, побудови та адміністрування комп'ютерних систем та мереж.

РН 24. Використовувати навички розроблення алгоритмів та програмування мовами низького та високого рівнів, навички проєктування, розроблення, адміністрування і захисту баз даних та інформаційних ресурсів (зокрема веб-ресурсів).

РН 25. Обґрунтовувати застосування методів, способів та технологій збору, зберігання, оброблення, передавання та захисту даних у комп'ютерних системах та мережах.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 8

3. Програма навчальної дисципліни

Модуль 1

Змістовий модуль 1. СТАНДАРТИЗАЦІЯ І МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА

ТЕМА 1. ОСНОВНІ ЕЛЕМЕНТИ ТА СТАНДАРТИ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Мета, завдання та порядок вивчення дисципліни. Інформаційно-методичне забезпечення дисципліни: основна та додаткова література, перелік рекомендованих інформаційних джерел у мережі Інтернет.

Основні елементи відкритих інформаційно-комунікаційних систем. Основні поняття і визначення. Концепція відкритих інформаційно-комунікаційних систем. Роль стандартів в технології відкритих інформаційно-комунікаційних систем. Основні групи стандартів і організації по стандартизації.

ТЕМА 2. МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Сумісність відкритих інформаційно-комунікаційних систем. Переносимість і здатність до взаємодії. Базова модель інформаційної системи. Системний підхід до опису функціональності на базі модельного представлення інформаційних систем. Розширення базової моделі інформаційної системи для взаємодіючих систем. Переносимість. Способи реалізації переносимості. Класифікація сервісів платформи додатків по критеріях переносимості. Здатність до взаємодії. Способи реалізації здатності до взаємодії. Класифікація сервісів платформи додатків по критеріях здатності до взаємодії. Основні моделі відкритих систем. Модель OSI. Модель POSIX.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 9

ТЕМА 3. ІНТРАНЕТ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Поняття інтранета. Структура інтранета. Еталонна модель інтранета. Етапи створення інтранета. Види інтранета. Стандарти створення інтранета. Інтранет як частина середовища відкритих систем. Інтранет і екстранет.

ТЕМА 4. ПОРТАЛ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Портал і інтранет. Класифікація порталів. Логічна структура і компоненти порталу. Схема порталу. Базові сервіси порталу.

Змістовий модуль 2. ВРАЗЛИВОСТІ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ НА ПРИКЛАДІ ІНТРАНЕТА. АТАКИ НА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ СИСТЕМИ

ТЕМА 5. ЗАГРОЗИ ТА ВРАЗЛИВОСТІ РЕСУРСІВ ІНТРАНЕТА

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Загрози ресурсам інтранета і причини їх реалізації. Уразливість архітектури клієнт-сервер. Конфігурація системи. Уразливість операційних систем. Уразливість серверів. Уразливість робочих станцій. Уразливість каналів зв'язку.

ТЕМА 6. СЛАБКОСТІ СИСТЕМНИХ УТИЛІТ, КОМАНД, МЕРЕЖЕВИХ СЕРВІСІВ, ТЕХНОЛОГІЙ ПРОГРАМУВАННЯ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Слабкості системних утиліт, команд і мережевих сервісів. Telnet. FTP. NFS. DNS. NIS. World Wide Web. Команди видаленого виконання. Sendmail і електронна пошта. Інші утиліти. Слабкості сучасних технологій програмування. Помилки в програмному забезпеченні. Мережеві віруси.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 10

ТЕМА 7. ВІДДАЛЕНІ АТАКИ НА КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Віддалені атаки на відкриті системи. Аналіз мережевого трафіку. Підміна довіреного об'єкту або суб'єкта. Помилковий об'єкт. "Відмова в обслуговуванні". Віддалений контроль над станцією в мережі.

ТЕМА 8. ТИПОВІ СЦЕНАРІЇ І РІВНІ АТАК

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Типові сценарії і рівні атак. Етапи реалізації атак. Рівні атак. Класичні і сучасні методи, використовувані нападниками для проникнення у відкриті системи. Перехоплення даних і виявлення прослуховуючих додатків Моніторинг в графічних інтерфейсах. Підміна системних утиліт. Атаки з використанням мережевих протоколів. Приклади деяких атак.

Модуль 2

Змістовий модуль 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ. АУТЕНТИФІКАЦІЯ СУБ'ЄКТІВ І ОБ'ЄКТІВ ВЗАЄМОДІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ. МІЖМЕРЕЖЕВІ ЕКРАНИ. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖ

ТЕМА 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Чотирьохрівнева модель відкритої системи. Специфіка захисту ресурсів відкритих систем на прикладі інтранета. Вибір мережевої топології інтранета при підключенні до інших зовнішніх мереж. Фізична ізоляція. Ізоляція протоколу. Виділені канали і маршрутизатори. Принципи створення захищених засобів зв'язку об'єктів у відкритих системах. Стандарти ISO 7498-2. Стандарт ISO 17799. Стандарт ISO 15408. Вимоги до захищених каналів зв'язку у відкритих системах.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 11

Політика безпеки для відкритих систем. Визначення політики безпеки. Причини вироблення політики безпеки. Основні вимоги до політики безпеки. Етапи вироблення політики безпеки. Зміст політики безпеки. Реалізація політики безпеки. Аудит за проведенням політики безпеки.

ТЕМА 10. СЕРВІСИ БЕЗПЕКИ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Ідентифікація/аутентифікація. Розмежування доступу. Протоколювання і аудит. Екранування. Тунелювання. Шифрування. Контроль цілісності. Контроль захищеності. Виявлення відмов і оперативне відновлення. Управління. Засоби забезпечення інформаційної безпеки у відкритих системах. Створення комплексної системи забезпечення безпеки відкритих систем. Управління безпекою відкритих систем. Організаційно-правові методи захисту відкритих систем. Деякі рекомендації по забезпеченню інформаційної безпеки відкритих систем. Що робити у разі злому системи. Як простежити за роботою користувачів. Короткі рекомендації адміністраторам інформаційної безпеки

ТЕМА 11. МЕРЕЖЕВА АУТЕНТИФІКАЦІЯ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Мережева аутентифікація – «перший рубіж» захисту відкритої системи. Уніфікація даних про суб'єктів і об'єкти. Єдина система аутентифікації. Єдина система авторизації. Єдина система персоналізації. Єдина система делегованого управління даними про суб'єктів і об'єкти. Єдина система аудиту доступу.

ТЕМА 12. ПІДСИСТЕМА АУТЕНТИФІКАЦІЇ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Аутентифікація в клієнт-серверних системах. Типові моделі аутентифікації. Методи аутентифікації. Протоколи аутентифікації. Сервери аутентифікації. Ринок засобів аутентифікації.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 12

ТЕМА 13. БУДОВА ТА ФУНКЦІЇ, КЛАСИФІКАЦІЯ МІЖМЕРЕЖЕВИХ ЕКРАНІВ.

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Основні компоненти міжмережевого екрану. Функції міжмережевих екранів. Профілі захисту для міжмережевих екранів. Типи міжмережевих екранів. Екрануючі концентратори. Пакетні фільтри. Шлюзи сеансового рівня. Шлюзи прикладного рівня. Міжмережеві екрани експертного рівня. Персональні міжмережеві екрани.

ТЕМА 14. ТИПОВІ СХЕМИ ПІДКЛЮЧЕННЯ МІЖ МЕРЕЖЕВИХ ЕКРАНІВ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Схеми підключення міжмережевих екранів. Слабкості міжмережевих екранів. Вибір реалізацій міжмережевих екранів. Приклади між мережевих екранів.

ТЕМА 15. ЗАХИСТ НА КАНАЛЬНОМУ РІВНІ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Проколи РРТР. Протокол L2ТР. Протокол L2F.

ТЕМА 16. ЗАХИСТ НА МЕРЕЖЕВОМУ ТА СЕАНСОВОМУ РІВНЯХ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Архітектура засобів безпеки IPSec. Захист даних, що передаються за допомогою протоколів АН та ESP. Протокол управління криптоключами ІКЕ. Особливості реалізації засобів IPSec. Захист на сеансовому рівні – протоколи SSL, TLS, SOCKS.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 13

ТЕМА 17. ЗАХИСТ БЕЗПРОВІДНИХ МЕРЕЖ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Загальні відомості про особливості організації захисту безпроводних мереж. Протоколи захисту безпроводних мереж.

ТЕМА 18. СПЕЦИФІКА ТА ПРОТОКОЛИ ПОБУДОВИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Визначення віртуальних приватних обчислювальних мереж. Цілі і завдання побудови VPN. Специфіка побудови VPN. Тунелювання у VPN. Схема VPN. Політики безпеки для VPN. Стандартні протоколи побудови VPN. Рівні захищених каналів. Захист даних на каналному рівні. Захист даних між каналним і мережевим рівнями. Захист даних на мережевому рівні. Захист на сеансовому рівні. Порівняння функціональних можливостей протоколів.

ТЕМА 19. ВАРІАНТИ ПОБУДОВИ VPN

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

VPN на базі мережевої операційної системи. VPN на базі маршрутизаторів. VPN на базі міжмережесих екранів. VPN на базі спеціалізованого програмного забезпечення. VPN на базі апаратних засобів. Види VPN залежно від вирішуваних завдань. Intranet VPN. Client/server VPN. Extranet VPN. Remote Access VPN. Топології VPN. VPN-консорціум про VPN. Рекомендації фахівців з вибору рішень для побудови VPN. Проблеми і уразливості сучасних VPN.

ТЕМА 20. ВІРТУАЛЬНІ ЛОКАЛЬНІ ОБЧИСЛЮВАЛЬНІ МЕРЕЖІ.

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Призначення і технології VLAN. Види VLAN. Переваги технології VLAN. Протоколи побудови VLAN

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 14

Змістовий модуль 4. СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ

ТЕМА 21. АУДИТ І МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

**(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8,
КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3,
РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20,
РН 21, РН 23, РН 24, РН 25)**

Аудит і моніторинг інформаційної безпеки у відкритих системах. Місце і завдання систем аналізу захищеності в захисті відкритих систем. Класифікації систем аналізу захищеності.

ТЕМА 22. МЕРЕЖЕВІ СКАНЕРИ

**(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8,
КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3,
РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20,
РН 21, РН 23, РН 24, РН 25)**

Мережеві сканери. Розміщення агентів мережевих сканерів. Принципи роботи мережевих сканерів. Етапи роботи мережевих сканерів. Порівняння поширених мережевих сканерів. Системні сканери. Сканери безпеки для додатків. Критерії вибору сканерів безпеки .

ТЕМА 23. ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

**(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8,
КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3,
РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20,
РН 21, РН 23, РН 24, РН 25)**

Методи відбиття вторгнень. Запобігання вторгненням. Переривання вторгнення. Заборона вторгнення. Відхилення вторгнення. Виявлення вторгнень. Усунення наслідків вторгнення. Основи побудови систем виявлення вторгнень. Структура систем виявлення вторгнень. Класифікація систем виявлення вторгнень. Ефективність систем виявлення вторгнень. Системне виявлення вторгнень. Принципи роботи системних систем виявлення вторгнення. Переваги і недоліки систем виявлення вторгнення. Мережеве виявлення вторгнень. Принципи роботи мережевих систем виявлення вторгнення. Розміщення мережевих систем виявлення вторгнення. Переваги і недоліки мережевих систем виявлення вторгнення. Поведінкове виявлення вторгнень. Інтелектуальне виявлення вторгнень. Комплексне виявлення вторгнень. Вибір системи виявлення вторгнень. Визначення вимог. Оцінка продукту. Розгортання системи

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 15

виявлення вторгнень. Практика виявлення вторгнень. Обмеженість систем виявлення вторгнень.

ТЕМА 24. СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Системи запобігання вторгненням. Реагування на вторгнення в інтранет, виявлені системами виявлення вторгнень. Етапи реагування. Реагування на виявлення вірусів і черв'яків. Реагування після атаки злоумисників. Збереження доказів вторгнення. Принципи і етапи збору доказів. Інструментальні засоби збору доказів. Стандарти в області виявлення вторгнень.

ТЕМА 25. ЗАХИСТ СИСТЕМ ЕЛЕКТРОННОЇ ПОШТИ

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Інші засоби забезпечення безпеки у відкритих системах. Захист від спаму в електронній пошті. Визначення спаму. Методи детектування спаму. Архітектура захищеної від спаму електронної пошти. Правові аспекти боротьби із спамом. Приклади засобів захисту від спаму.

ТЕМА 26. БАГАТОФУНКЦІОНАЛЬНІ ПРИСТРОЇ ЗАХИСТУ ВІД МЕРЕЖЕВИХ АТАК

(КЗ 1, КЗ 2, КЗ 3, КЗ 7, КЗ 12, КФ 1, КФ 2, КФ 4, КФ 5, КФ 6, КФ 8, КФ 9, КФ 10, КФ 12, КФ 14, КФ 15, КФ 17, КФ 18, КФ 19, РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25)

Багатофункціональні пристрої захисту від мережеских атак. Системи аналізу і управління ризиками. Системи забезпечення інформаційної безпеки на рівні підприємства.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 16

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі	Кількість годин			
	Всього	Лекції	Лабораторні	Самостійна робота
2	3	4	5	6
Модуль 1				
Змістовий модуль 1. СТАНДАРТИЗАЦІЯ І МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА				
ТЕМА 1. ОСНОВНІ ЕЛЕМЕНТИ ТА СТАНДАРТИ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ	15	4	8	3
ТЕМА 2. МОДЕЛЬНЕ ПРЕДСТАВЛЕННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ. ІНТРАНЕТ ЯК ВІДКРИТА СИСТЕМА	14	4	8	2
ТЕМА 3. ІНТРАНЕТ	14	4	8	2
ТЕМА 4. ПОРТАЛ	14	4	7	3
Модульний контроль 1	1	-	1	-
Разом за змістовний модуль 1	58	16	32	10
Змістовий модуль 2. ВРАЗЛИВОСТІ ВІДК КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ НА ПРИКЛАДІ ІНТРАНЕТА. АТАКИ НА КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ				
ТЕМА 5. ЗАГРОЗИ ТА ВРАЗЛИВОСТІ РЕСУРСІВ ІНТРАНЕТА	14	4	8	2
ТЕМА 6. СЛАБКОСТІ СИСТЕМНИХ УТИЛІТ, КОМАНД, МЕРЕЖЕВИХ СЕРВІСІВ, ТЕХНОЛОГІЙ ПРОГРАМУВАННЯ	14	4	8	2
ТЕМА 7. ВІДДАЛЕНІ АТАКИ НА КОМП'ЮТЕРНІ СИСТЕМИ ТА МЕРЕЖІ	14	4	8	2
ТЕМА 8. ТИПОВІ СЦЕНАРІЇ І РІВНІ АТАК	14	4	7	3
Модульний контроль 2	1	-	1	-
Разом за змістовний модуль 2	57	16	32	9
Разом модуль 1	115	32	64	19
Модуль 2				
Змістовий модуль 3. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ. АУТЕНТИФІКАЦІЯ СУБ'ЄКТІВ І ОБ'ЄКТІВ ВЗАЄМОДІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ. МІЖМЕРЕЖЕВІ ЕКРАНИ. ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖ				
ТЕМА 9. ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ	6	1	4	1
ТЕМА 10. СЕРВІСИ БЕЗПЕКИ	7	1	4	2
ТЕМА 11. МЕРЕЖЕВА АУТЕНТИФІКАЦІЯ	7	1	4	2
ТЕМА 12. ПІДСИСТЕМА АУТЕНТИФІКАЦІЇ	7	1	4	2
ТЕМА 13. БУДОВА ТА ФУНКЦІЇ, КЛАСИФІКАЦІЯ	8	2	2	2

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 17

МІЖМЕРЕЖЕВИХ ЕКРАНІВ.				
ТЕМА 14. ТИПОВІ СХЕМИ ПІДКЛЮЧЕННЯ МІЖ МЕРЕЖЕВИХ ЕКРАНІВ	8	2	4	2
ТЕМА 15. ЗАХИСТ НА КАНАЛЬНОМУ РІВНІ	6	2	2	2
ТЕМА 16. ЗАХИСТ НА МЕРЕЖЕВОМУ ТА СЕАНСОВОМУ РІВНЯХ	6	2	2	2
ТЕМА 17. ЗАХИСТ БЕЗПРОВІДНИХ МЕРЕЖ	6	2	2	2
ТЕМА 18. СПЕЦИФІКА ТА ПРОТОКОЛИ ПОБУДОВИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ	6	2	2	2
ТЕМА 19. ВАРІАНТИ ПОБУДОВИ VPN	6	2	2	2
ТЕМА 20. ВІРТУАЛЬНІ ЛОКАЛЬНІ ОБЧИСЛЮВАЛЬНІ МЕРЕЖІ.	6	2	2	2
Модульний контроль 3	1	-	1	-
Разом за змістовний модуль 3	82	20	39	23
Змістовий модуль 4. СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ				
ТЕМА 21. АУДИТ І МОНИТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У КОМП'ЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ	7	2	4	1
ТЕМА 22. МЕРЕЖЕВІ СКАНЕРИ	7	2	4	1
ТЕМА 23. ОСНОВИ ПОБУДОВИ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ	7	2	4	1
ТЕМА 24. СИСТЕМИ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ	7	2	4	1
ТЕМА 25. ЗАХИСТ СИСТЕМ ЕЛЕКТРОННОЇ ПОШТИ	7	2	4	1
ТЕМА 26. БАГАТОФУНКЦІОНАЛЬНІ ПРИСТРОЇ ЗАХИСТУ ВІД МЕРЕЖЕВИХ АТАК	7	2	4	1
Модульний контроль 4	1	-	1	-
Разом за змістовний модуль 4	43	12	25	6
Разом модуль 2	125	32	64	29
КУРСОВИЙ ПРОЕКТ	30	-	-	30
ВСЬОГО	270	64	128	78

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 18

5. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
		денна форма
1.	Лабораторна робота № 1. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ БАЗОВИХ ЗАСОБІВ ЗАХИСТУ МЕРЕЖНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ CISCO IOS ТА МЕРЕЖНОГО ОБЛАДНАННЯ CISCO	8
2.	Лабораторна робота № 2. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ КАНАЛЬНОГО РІВНЯ MAC-FLOODING ТА MAC-SPOOFING У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	8
3.	Лабораторна робота № 3. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ НА ПРОТОКОЛ STP/PVST+ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	8
4.	Лабораторна робота № 4. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ТЕХНОЛОЇ VLAN НА ОСНОВІ ГРУПУВАННЯ ПОРТІВ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	8
5.	Лабораторна робота № 5. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ НА ОСНОВІ ГРУПУВАННЯ ПОРТІВ ТА ТРАНКОВИХ ПРОТОКОЛІВ У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	8
6.	Лабораторна робота № 6. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ЛОКАЛЬНИХ МЕРЕЖ типу Private VLAN У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	8
7.	Лабораторна робота № 7. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ VTP У МЕРЕЖІ НА БАЗІ КОМУТАТОРІВ CISCO	8
8.	Лабораторна робота № 8. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ НА ПРОТОКОЛ ARP	4
9.	Лабораторна робота № 9. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ПРОТИДІЇ АТАКАМ НА СЕРВІСИ ПРОТОКОЛУ DNSR	4
10.	Лабораторна робота № 10. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
11.	Лабораторна робота № 11. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ АУТЕНТИФІКАЦІЇ ПРОТОКОЛІВ КАНАЛЬНОГО РІВНЯ	4
12.	Лабораторна робота № 12. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАСОБІВ ПРОТОКОЛУ PPPoE У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
13.	Лабораторна робота № 13. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ АУТЕНТИФІКАЦІЇ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ	4
14.	Лабораторна робота № 14. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ АУТЕНТИФІКАЦІЇ НА ОСНОВІ МОДЕЛІ AAA ТА ПРОТОКОЛІВ RADIUS ТА TACACS+ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 19

15.	Лабораторна робота № 15. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ТУНЕЛЮВАННЯ GRE У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
16.	Лабораторна робота № 16. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАСОБІВ ПРОТОКОЛУ RPTP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
17.	Лабораторна робота № 17. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ЗАСОБІВ ПРОТОКОЛУ L2TP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO	4
18.	Лабораторна робота № 18. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ МІЖМЕРЕЖНИХ ЕКРАНІВ НА БАЗІ СТАНДАРТНИХ СПИСКІВ ДОСТУПУ	4
19.	Лабораторна робота № 19. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ МІЖМЕРЕЖНИХ ЕКРАНІВ НА БАЗІ РОЗШИРЕНИХ СПИСКІВ ДОСТУПУ	4
20.	Лабораторна робота № 20. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ОСНОВНИХ ЗАСОБІВ ЗАХИСТУ АПАРАТНОГО МІЖМЕРЕЖНОГО ЕКРАНУ CISCO ASA 5505	4
21.	Лабораторна робота № 21. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ДОДАТКОВИХ ЗАСОБІВ ЗАХИСТУ АПАРАТНОГО МІЖМЕРЕЖНОГО ЕКРАНУ CISCO ASA 5505	4
22.	Лабораторна робота № 22. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ ТИПУ SITE-TO-SITE	4
23.	Лабораторна робота № 23. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ ТИПУ DMVPN	4
24.	Лабораторна робота № 24. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ СИСТЕМ IDS/IPS	4
	Разом	124

6. Завдання для самостійної роботи

Відпрацювання матеріалу навчального курсу Cisco Network Security (проходження онлайн навчання, виконання тестових контрольних робіт, виконання тестових проміжних оцінювань).

Відпрацювання самостійного завдання у вигляді індивідуального курсового проєкту.

7. Індивідуальні завдання

Виконання індивідуальних завдань передбачено у вигляді курсового проєкту.

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 20

8. Методи навчання

Під час викладання навчальної дисципліни використовуються методи навчання, що сприяють досягненню відповідних програмних результатів:

Результат навчання	Методи навчання
РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25	МН01 – вербальні (лекція, пояснення, розповідь, бесіда, інструктаж); МН02 – наочні (спостереження, ілюстрація, демонстрація); МН03 – практичні (різні види вправ та завдань, виконання розрахунків тощо); МН04 – пояснювально-ілюстративний (передбачає надання готової інформації викладачем та її засвоєння студентами); МН05 – репродуктивний, в основу якого покладено виконання різного роду завдань за зразком; МН06 – метод проблемного викладу; МН07 – частково-пошуковий (евристичний); МН08 – дискусійний метод; МН09 – метод активного навчання (проведення ділових ігор, ігрового проектування); МН10 – ситуаційний метод, розв'язування кейсових завдань.

9. Методи контролю

Передбачено заходи поточного та підсумкового контролю. Під час проведення заходів контролю перевірка досягнення програмних результатів навчання здійснюється з використанням наступних методів:

Результат навчання	Методи контролю
РН 1, РН 2, РН 3, РН 4, РН 6, РН 7, РН 9, РН 11, РН 13, РН 14, РН 15, РН 16, РН 19, РН 20, РН 21, РН 23, РН 24, РН 25	оцінювання роботи під час аудиторних занять; виконання практичних завдань; поточне тестування; перевірка завдань модульної контрольної роботи; захист індивідуального завдання (за наявності); залік/екзамен (3-й семестр – залік, 4-й семестр – екзамен).

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 21

10. Оцінювання результатів навчання здобувачів вищої освіти

Оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни здійснюється відповідно до Положення про оцінювання результатів навчання здобувачів вищої освіти у Державному університеті «Житомирська політехніка» та розподілу балів, що наведений нижче.

Система оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни включає поточний, модульний та підсумковий контроль у всіх семестрах вивчення навчальної дисципліни.

Поточний контроль проводиться для оцінювання рівня засвоєння знань, формування умінь і навичок здобувачів вищої освіти впродовж вивчення ними матеріалу модуля (змістових модулів) навчальної дисципліни. Поточний контроль здійснюється під час проведення навчальних занять.

Модульний контроль проводиться з метою оцінювання результатів навчання здобувачів вищої освіти за модуль (змістові модулі) навчальної дисципліни. Модульний контроль проводиться під час навчального заняття після завершення вивчення матеріалу модуля (змістових модулів) навчальної дисципліни. Модульний контроль здійснюється у формі комп'ютерного тестування та виконання індивідуальних практичних завдань.

Підсумковий контроль проводиться для підсумкового оцінювання результатів навчання здобувачів вищої освіти з навчальної дисципліни. Підсумковий контроль у формі заліку проводиться у першому семестрі, у формі екзамену – у другому семестрі вивчення навчальної дисципліни. Процедура складання заліку та екзамену визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Розподіл балів з навчальної дисципліни

Види робіт здобувача вищої освіти	Кількість балів за семестр
	денна форма
Семестр 5	
Виконання завдань поточного контролю	60
Виконання завдань модульного контролю	40
Підсумкова семестрова оцінка	100
Семестр 6	
Виконання завдань поточного контролю	60
Виконання завдань модульного контролю	40
Підсумкова семестрова оцінка	100
Курсовий проєкт	100

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 22

Розподіл балів за виконання завдань поточного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр
	денна форма
Семестр 5	
Виконання завдань під час навчальних занять	60
Виконання та захист індивідуальних самостійних завдань	0
Виконання науково-дослідної роботи та інших видів робіт (додаткові – заохочувальні бали): 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт: - активна участь в опитуваннях, обговореннях, дискусіях під час лекцій протягом семестру - вчасна здача лабораторної роботи (до наступного лабораторного заняття) - сумлінна робота на лабораторних заняттях протягом семестру (здано всі лабораторні роботи, звіти виконано якісно)	до 20
Разом за виконання завдань поточного контролю	60
Семестр 6	
Виконання завдань під час навчальних занять	60
Виконання та захист індивідуальних самостійних завдань	0
Виконання науково-дослідної роботи та інших видів робіт (додаткові – заохочувальні бали): 1. Участь у студентських предметних олімпіадах, Всеукраїнському конкурсі студентських наукових робіт, грантах, науково-дослідних проектах 2. Підготовка наукових статей, тез доповідей наукових конференцій 3. Інші види робіт: - активна участь в опитуваннях, обговореннях, дискусіях під час лекцій протягом семестру - вчасна здача лабораторної роботи (до наступного лабораторного заняття) - сумлінна робота на лабораторних заняттях протягом семестру (здано всі лабораторні роботи, звіти виконано якісно)	до 20
Разом за виконання завдань поточного контролю	60

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 23

Розподіл балів за виконання завдань під час навчальних занять

Види робіт здобувача вищої освіти ¹	Кількість балів за семестр
	денна форма
Семестр 5	
Виконання та захист лабораторних робіт	24
Виконання поточних тестів	24
Участь у лекційних заняттях	4
Проходження матеріалів курсів на платформі Netacad	8
Разом за виконання завдань під час навчальних занять	60
Семестр 6	
Виконання та захист лабораторних робіт	24
Виконання поточних тестів	24
Участь у лекційних заняттях	4
Проходження матеріалів курсів на платформі Netacad	8
Разом за виконання завдань під час навчальних занять	60

З метою застосування цілих чисел для оцінювання активностей здобувачів вищої освіти під час навчальних занять протягом семестру використовується 100-бальна шкала оцінювання кожного окремо виду робіт. Розрахунок набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр проводиться за формулою:

$$P_{НЗ} = (P_{ЛР100} \times VK_{ЛР} + P_{ПТ100} \times VK_{ПТ} + P_{ЛЕК100} \times VK_{ЛЕК} + P_{Netacad100} \times VK_{Netacad}) \times K_{НЗ},$$

де $P_{НЗ}$ – кількість набраних здобувачем вищої освіти балів за виконання завдань під час навчальних занять за семестр;

$P_{ЛР100}$, $P_{ПТ100}$, $P_{ЛЕК100}$, $P_{Netacad100}$ – кількість набраних здобувачем вищої освіти балів за семестр відповідно за виконання та захист лабораторних робіт, виконання поточних тестів, участь у лекційних заняттях, проходження курсів на платформі Netacad (кожний окремо вид робіт на навчальних заняттях оцінюється за 100-бальною шкалою);

$VK_{ЛР}$, $VK_{ПТ}$, $VK_{ЛЕК}$, $VK_{Netacad}$ – вагові коефіцієнти відповідно за виконання та захист лабораторних робіт, виконання поточних тестів, участь у лекційних заняттях, проходження курсів на платформі Netacad. Значення вагових коефіцієнтів розраховуються шляхом ділення кількості балів, які встановлені за виконання окремого виду робіт під час навчальних занять, на сумарну кількість балів за виконання цих робіт (дані для розрахунку вагових коефіцієнтів наведено в табл. «Розподіл балів за виконання завдань під час навчальних занять»);

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 24

$K_{НЗ}$ – коригувальний коефіцієнт, який визначається шляхом ділення кількості балів, що встановлені за виконання завдань під час навчальних занять, на 100 балів.

Розподіл балів за виконання завдань модульного контролю

Види робіт здобувача вищої освіти	Кількість балів за семестр
	денна форма
Семестр 5	
Виконання завдань модульного контролю 1	20
Виконання завдань модульного контролю 2	20
Разом за виконання завдань модульного контролю	40
Семестр 6	
Виконання завдань модульного контролю 3	20
Виконання завдань модульного контролю 4	20
Разом за виконання завдань модульного контролю	40

Якщо здобувач вищої освіти виконав завдання модульного контролю і з урахуванням отриманих балів за поточний контроль набрав у сумі 60 балів або більше за семестр, він може погодити дану оцінку в електронному кабінеті і вона стане семестровою оцінкою за вивчення навчальної дисципліни.

Якщо здобувач вищої освіти під час вивчення навчальної дисципліни за семестр набрав 60 балів або більше і бажає покращити свій результат успішності, він проходить процедуру підсумкового контролю у формі: заліку – у першому семестрі, екзамену – у другому семестрі. На залік з навчальної дисципліни, яка вивчається впродовж двох семестрів, виносяться ключові питання з першого семестру вивчення навчальної дисципліни. На екзамен з навчальної дисципліни, яка вивчається впродовж двох семестрів, виносяться ключові питання з усієї навчальної дисципліни. За складання заліку або екзамену здобувач вищої освіти може набрати 40 балів. Набрані бали за виконання завдань підсумкового контролю, а також бали за поточний контроль сумуються і формується семестрова оцінка з навчальної дисципліни. Бали, які здобувач вищої освіти набрав за виконання завдань модульного контролю, при цьому не враховуються під час розрахунку семестрової оцінки з навчальної дисципліни.

Здобувач вищої освіти допускається до процедури підсумкового контролю у формі заліку або екзамену, якщо протягом семестру за виконання завдань поточного контролю набрав 20 балів або більше.

Якщо здобувач вищої освіти протягом семестру за результатами поточного контролю набрав 15–19 балів, він отримує право за власною заявою повторно опанувати окремі теми (змістові модулі) навчальної дисципліни понад обсяги, встановлені навчальним планом освітньої програми. Повторне вивчення окремих тем (змістових модулів) навчальної дисципліни понад обсяги,

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ OK25 - 2024
	Екземпляр № 1	Арк 26 / 25

встановлені навчальним планом освітньої програми, здійснюється у вільний від занять здобувача вищої освіти час.

Якщо здобувач вищої освіти протягом семестру за результатами поточного контролю набрав від 0 до 14 балів (включно), він вважається таким, що не виконав вимоги робочої програми навчальної дисципліни та має академічну заборгованість. Здобувач вищої освіти отримує право за власною заявою повторно опанувати навчальний матеріал дисципліни за даний семестр у наступному семестрі понад обсяги, встановлені навчальним планом освітньої програми.

Процедура надання додаткових освітніх послуг здобувачу вищої освіти з метою повторного вивчення навчального матеріалу дисципліни понад обсяги, встановлені навчальним планом освітньої програми, визначена у Положенні про надання додаткових освітніх послуг здобувачам вищої освіти в Державному університеті «Житомирська політехніка».

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках окремих тем навчальної дисципліни, здійснюється викладачем за зверненням здобувача вищої освіти та представленням документів, які підтверджують результати навчання (сертифікати, свідоцтва, скріншоти тощо). Рішення про визнання та оцінка за відповідну частину освітнього компонента приймається викладачем за результатами співбесіди зі здобувачем вищої освіти.

Визнання результатів навчання, набутих у неформальній та/або інформальній освіті в рамках цілого освітнього компонента, здійснюється за процедурою, яка визначена у Положенні про організацію освітнього процесу у Державному університеті «Житомирська політехніка».

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

Житомирська політехніка	МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА» Система управління якістю відповідає ДСТУ ISO 9001:2015	Ф-22.05-05.01/ 123.00.1//Б/ ОК25 - 2024
	Екземпляр № 1	Арк 26 / 26

11. Рекомендована література

Основна література

1. Barker, Keith. CCNA Security 640-554. Official Cert Guide / Keith Barker, Scott Morris.– Cisco Press, 2013. – 740 p.
2. Conlan J., Patrik. Cisco Network Professional. Advanced Internetworking Guide. / Patrik J. Conlan. – Wiley Publishing, 2009. – 854 p.
3. Paquet, Catherine. Implementing Cisco IOS Network Security (IINS) / Catherine Paquet. – Cisco Press, 2009. – 600 p.
4. Santos, Omar. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p.
5. Vyncke, Eric. LAN Switch Security: What Hackers Know about Your Switches / Eric Vyncke, Christopher Paggen. – Cisco Press, 2007. – 340 p.
6. Watkins, Michael. CCNA Security. Official Exam Certification Guide / Michael Watkins, Kevin Wallace. – Cisco Press, 2008. – 638 p.
7. Wilkins, Sean. CCNP Security. SECURE 642-637. Official Cert Guide / Sean Wilkins, Franklin H. Smith III. – Cisco Press, 2011. – 738 p.
8. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч. 2 / підг. А. А. Єфіменко. – Житомир: ЖВІ, 2017. – 176 с.
9. Єфіменко А.А. Захист інформації в інформаційно-комунікаційних системах: методичні рекомендації для виконання лабораторних робіт. Ч. 1 / підг. А. А. Єфіменко. – Житомир: ЖДТУ, 2018. – 112 с.

Допоміжна література

10. Грайворонський М. В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.
11. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

12. Інформаційні ресурси мережі Інтернет

1. Навчальний курс Network Security [Електронний ресурс] – Режим доступу: www.netacad.com.
2. Навчальний курс CCNA Security [Електронний ресурс] – Режим доступу: www.netacad.com.
3. Навчальний курс CCNAv7: Enterprise Networking, Security, and Automation [Електронний ресурс] – Режим доступу: www.netacad.com.
4. Навчальний курс CCNP: Core Networking. [Електронний ресурс] – Режим доступу: www.netacad.com.