НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Інститут комп'ютерних інформаційних технологій
Кафедра безпеки інформаційних технологій

УЗГОДЖЕНО
Директор ІІДС
_____ С. Філоненко
"____"_____2014 р.

ЗАТВЕРДЖУЮ
Проректор
з науково - педагогічної роботи
_____ А.Полухін
"_____"_____2014р.

Система менеджменту якості

РОБОЧА НАВЧАЛЬНА ПРОГРАМА

навчальної дисципліни

«Новітні технології захисту інформації»

(за кредитно-модульною системою)

Напрям:	6.040301	«Прикладна математика»
Спеціальність :	7.04030101	«Прикладна математика»
	8.04030101	«Прикладна математика»

Курс – 5

Семестр – 9

Лекції – 17
Практичні заняття – 17
Самостійна робота – 72
Індивідуальні заняття – 2
Усього (годин/кредитів ECTS) – 108/3

Диференційований залік – 9 семестр

Індекс Р14 - 7.04030101 / 12-4.1.2
Р14 - 8.04030101 / 12-4.1.2

Робоча навчальна програма дисципліни «Новітні технології захисту інформації» розроблена на основі робочих навчальних планів № РС-14-7.04030101/12, № РМ-14-8.04030101/12 підготовки фахівців освітньо-кваліфікаційних рівнів "Спеціаліст", "Магістр" за напрямом 6.040301 «Прикладна математика» спеціальності 7/8.04030101 «Прикладна математика», навчальної програми цієї дисципліни, індекс Н14-7.04030101/12-4.1.2, Н14-8.04030101/12-4.1.2, затвердженої ректором "____"_____2014 р., "Тимчасового Положення про організацію навчального процесу за кредитно-модульною системою (в умовах педагогічного експерименту)" та "Тимчасового Положення про рейтингову систему оцінювання", затверджених наказом ректора від 15.06.2004 №122/од, та наказу ректора від 12.04.2005 №81/од.

Робочу навчальну програму розробили:
доцент кафедри безпеки
інформаційних технологій _____ В. Ковтун
доцент кафедри безпеки
інформаційних технологій _____ В. Кінзерявий

Робоча навчальна програма обговорена та схвалена на засіданні кафедри безпеки інформаційних технологій, протокол № ___ від _____ 2014 р.

Завідувач кафедри_____ О. Корченко

Навчальна програма обговорена та схвалена випусковою кафедрою напряму 6.040301 «Прикладна математика» (спеціальність 7/8.04030101 «Прикладна математика») – кафедри прикладної математики, протокол № ___ від «___» _____2014 р.

Завідувач кафедри_____ П. Приставка

Робоча навчальна програма обговорена та схвалена на засіданні науково-методично-редакційної ради інституту комп'ютерних інформаційних технологій, протокол № ___ від "_____"_____ 2014 р.

Голова НМРР_____ Б. Масловський

Рівень документа – 3б
Плановий термін між ревізіями – 1 рік
Контрольний примірник

ЗМІСТ

ВСТУП

Однією з необхідних умов організації навчального процесу за кредитно–модульною системою є наявність робочої навчальної програми з дисципліни «Новітні технології захисту інформації», виконаної за модульно–рейтинговими засадами і доведеної до відома викладачів та студентів.

Рейтингова система оцінювання (РСО) є невід'ємною складовою робочої навчальної програми і передбачає визначення якості виконаної студентом усіх видів аудиторної та самостійної навчальної роботи та рівня набутих ним знань та умінь шляхом оцінювання в балах результатів цієї роботи під час поточного, модульного та семестрового контролю, з наступним переведенням оцінки за багатобальною шкалою в оцінки за національною шкалою та шкалою ECTS.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце навчальної дисципліни в системі професійної підготовки фахівця

Дисципліна «Новітні технології захисту інформації» є спеціальним курсом, що належить до циклу дисциплін вільного вибору студента.

Предметом вивчення дисципліни «Новітні технології захисту інформації» є методи, алгоритми та засоби криптографічного захисту інформації, методи, алгоритми та засоби криптоаналітичного відтворення захищеної інформації із застосуванням обчислювальної техніки.

Дисципліна «Новітні технології захисту інформації» повинна дати студентам знання і навички для вивчення і засвоєння подальших дисциплін, пов'язаних з захистом інформації та її обробкою, у значній мірі визначає рівень загальнонаукової підготовки спеціалістів і становить базову основу для вивчення принципів, методів, алгоритмів та обчислювальних технологій обробки інформації з обмеженим доступом із застосуванням електронно-обчислювальних машин (ЕОМ).

1.2. Мета виконання навчальної дисципліни

Основна мета дисципліни «Новітні технології захисту інформації» полягає в створенні як теоретичної, так і практичної бази для засвоєння та розвитку практичних навиків та умінь з захисту інформації, математичних методів та алгоритмів криптографічного перетворення даних із застосуванням ЕОМ у автоматизованих системах управління із заданим ступенем надійності та швидкодії.

1.3. Завдання вивчення навчальної дисципліни

Завдання вивчення дисципліни визначаються вимогами до підготовки спеціалістів та магістрів за спеціальністю 7/8.04030101 «Прикладна математика».

Головне завдання вивчення дисципліни полягає в висвітленні нових аспектів теорії інформації, теорії інформаційної безпеки та криптографічного перетворення даних, що виникають у зв'язку з можливостями застосування обчислювальної техніки, сучасних прикладних методів перетворення інформації із застосуванням комп'ютерних технологій, зокрема, криптографічні перетворення за допомогою ЕОМ із заданими властивостями, криптоаналітичної оцінки стійкості криптографічних перетворень, оцінка вразливості підсистем захисту інформації у автоматизованих систем до атак зловмисників, збір та первинна обробка інформації з виробленням оптимальних рішень та управляючих впливів.

Завдання вивчення навчальної дисципліни є:

- аналіз захищеності інформаційних ресурсів;
- створення криптографічних систем захисту інформації;
- реалізація захищеного електронного документообігу.

1.4. Інтегровані вимоги до знань та умінь з навчальної дисципліни

У результаті вивчення дисципліни студент повинен:

Знати:

- Основні теоретичні положення та визначення.
- Канали несанкціонованого отримання та руйнування інформації. Технічні канали витоку інформації. Класифікація, причини та джерела утворення. Методи та способи виявлення.
- Основи побудови криптосистем: безумовно стійкі, обчислювально-стійкі, доведено стійкі.
- Основні методи та алгоритми формування псевдовипадкових послідовностей та чисел із заданими характеристиками. Дослідження їх характеристик.
- Основи побудови симетричних криптосистем: блочні шифри, поточні шифри.
- Основи побудови криптосистем з відкритим ключем. Обчислення образу інформації (повідомлення) за допомогою геш-функції. Обмін ключами та вироблення спільного секрету. Формування та перевірка електронного цифрового підпису. Направлене блокове шифрування.
- Складно-обчислювальні задачі: Криптосистеми у полях та кільцях. Формування загальносистемних параметрів. Криптосистеми на еліптичних кривих. Формування загальносистемних параметрів. Криптосистеми на гіпереліптичних кривих. Формування загальносистемних параметрів.
- Методи криптоаналізу симетричних криптографічних алгоритмів (шифрів): блочних та поточних шифрів.
- Методи криптоаналізу геш-функцій.
- Методи криптоаналізу складно-обчислювальних задач, що покладені у основу криптографічних алгоритмів с відкритим ключем. Криптосистеми у полях та кільцях. Криптосистеми на еліптичних кривих. Криптосистеми на гіпереліптичних кривих.
- Сучасні криптографічні алгоритми. Блочні симетричні шифри: DES, ГОСТ 28147-89, AES. Поточні симетричні шифри: SNOW, у поточному режимі: DES, ГОСТ 28147-89, AES. Геш-функції: ГОСТ Р34.11-94, RIPEMD160, MD5. Електронний цифровий підпис: RSA, DSA, ECDSA, ДСТУ 4145-2002, ECGDSA, ECKDSA. Обмін ключами: ECKAS-DH1, ECKAS-DH2, ECKAS-MQV. Направленого шифрування: RSA, El-Gamal.
- Підходи до створення комплексної системи захисту інформації.

Вміти:

- Аналізувати характеристики та класифікувати джерела інформації.
- Досліджувати псевдовипадкові послідовності з використанням пакету NIST STS.
- Використовувати сучасні криптографічні бібліотеки, що інтегровані до операційних систем: Crypto Service Provider у операційних системах сімейства Windows для симетричного шифрування (DES, AES), з відкритими ключем (RSA шифрування та ЕЦА, ЕЦП за DSA та ECDSA.
- Використовувати сучасні криптографічні бібліотеки Intel Performance Primitives Crypto Package для реалізації: симетричного шифрування AES, GOST 28147-89. Асиметричного шифрування RSA, El-Gamal. Електронного цифрового підпису ECDSA та DSTU 4145-2002.
- Формулювати вимоги до підсистеми захисту інформації систем обробки інформації з обмеженим доступом.

1.5. Інтегровані вимоги до знань і умінь з навчальних модулів

Навчальний матеріал дисципліни структурований за модульним принципом і складається з одного навчального модуля.

1.5.1. У результаті засвоєння навчального матеріалу навчального модуля №1 «Основні поняття та симетричні криптосистеми. Асиметричні криптосистеми та особливості побудови криптографічних систем захисту інформації» студент повинен:

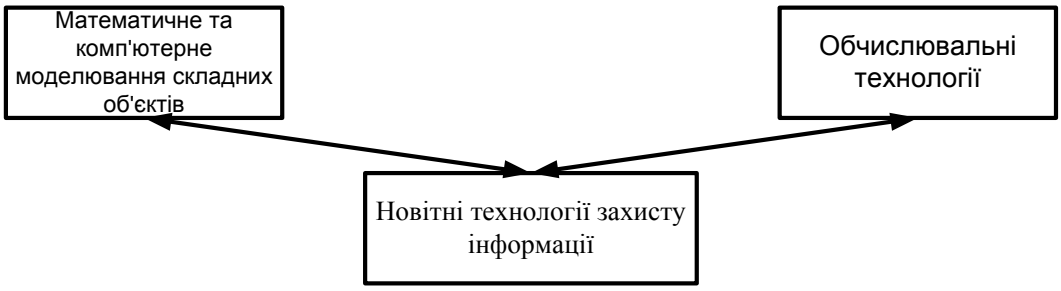
Знати:

- Основні теоретичні положення та визначення.
- Канали несанкціонованого отримання та руйнування інформації. Технічні канали витоку інформації. Класифікація, причини та джерела утворення. Методи та способи виявлення.
- Основи побудови криптосистем: безумовно стійкі, обчислювально-стійкі, доведено стійкі.
- Основні методи та алгоритми формування псевдовипадкових послідовностей та чисел із заданими характеристиками. Дослідження їх характеристик.
- Основи побудови симетричних криптосистем: блочні шифри, поточні шифри. Сучасні криптографічні алгоритми. Блочні симетричні шифри: DES, ГОСТ 28147-89, AES. Поточні симетричні шифри: SNOW, у поточному режимі: DES, ГОСТ 28147-89, AES.
- Методи криптоаналізу симетричних криптографічних алгоритмів: блочних та поточних шифрів.
- Основи побудови асиметричних криптосистем (з відкритим ключем): геш-функції, ЕЦП, обмін ключами, направлене шифрування.
- Основні асиметричні криптографічні алгоритм (з відкритим ключем). Геш-функції: ГОСТ Р34.11-94, RIPEMD160, MD5. Електронний цифровий підпис: RSA, DSA, ECDSA, ДСТУ 4145-2002, ECGDSA, ECKDSA. Обмін ключами: ECKAS-DH1, ECKAS-DH2, ECKAS-MQV. Направленого шифрування: RSA, El-Gamal.
- Методи криптоаналізу геш-функцій.
- Методи криптоаналізу складно-обчислювальних задач, що покладені у основу криптографічних алгоритмів с відкритим ключем. Криптосистеми у полях та кільцях. Криптосистеми на еліптичних кривих. Криптосистеми на гіпереліптичних кривих.
- Підходи до створення комплексної системи захисту інформації.

Вміти:

- Аналізувати характеристики та класифікувати джерела інформації.
- Досліджувати псевдовипадкові послідовності з використанням пакету NIST STS.
- Використовувати сучасні криптографічні бібліотеки, що інтегровані до операційних систем: Crypto Service Provider у операційних системах сімейства Windows для симетричного шифрування (DES, AES).
- Використовувати сучасні криптографічні бібліотеки, що інтегровані до операційних систем: Crypto Service Provider у операційних системах сімейства Windows для симетричного шифрування (DES, AES), з відкритими ключем (RSA шифрування та ЕЦА, ЕЦП за DSA та ECDSA.
- Використовувати сучасні криптографічні бібліотеки Intel Performance Primitives Crypto Package для реалізації: симетричного шифрування AES, GOST 28147-89. Асиметричного шифрування RSA, El-Gamal. Електронного цифрового підпису ECDSA та DSTU 4145-2002.
- Формулювати вимоги до підсистеми захисту інформації систем обробки інформації з обмеженим доступом.

1.6. Міждисциплінарні зв'язки навчальної дисципліни



2. ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1 Тематичний план навчальної дисципліни

Таблиця 2.1

№ пор.	*Назва теми*	Обсяг навчальних занять, год.				
		Усього	Лекції	Прак.	СРС	ІЗ
9 семестр						
Модуль №1 «Основні поняття та симетричні криптосистеми. Асиметричні криптосистеми та особливості побудови криптографічних систем захисту інформації»						
1.1	Основні теоретичні положення та визначення. Канали несанкціонованого отримання та руйнування інформації.	12	2	2	8	
1.2	Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести. Криптографічно безпечні генератори псевдовипадкових послідовностей.	16	2	4	10	
1.3	Симетричні криптосистеми. Блочний шифр: ГОСТ 28-147-89, AES. Поточний шифр: SNOW.	22	4	4	14	
1.4	Криптоаналіз симетричних криптосистем.	9	2		6	1
1.5	Асиметричні криптосистеми (з відкритим ключем). Геш-функції. ЕЦП. Направлене шифрування. Обмін ключами.	20	2	4	14	
1.6	Криптоаналіз асиметричних криптосистем.	8	2		6	
1.7	Підходи до створення комплексної системи захисту інформації.	16	2	3	10	1
1.8	Модульна контрольна робота №1	5	1		4	
	Всього за модулем №1	**108**	**17**	**17**	**72**	**2**
	Всього за 9 семестр	**108**	**17**	**17**	**72**	**2**
	Всього за дисципліною	**108**	**17**	**17**	**72**	**2**

2.2. Проектування дидактичного процесу за видами навчальних занять

2.2.1. Лекційні заняття, їх тематика і обсяг

Таблиця 2.2

№ пор	*Назва теми*	Обсяг нав. занять, год.	
		Лекції	СРС
9 семестр			
Модуль №1 «Основні поняття та симетричні криптосистеми. Асиметричні криптосистеми та особливості побудови криптографічних систем захисту інформації»			
1.1	Основні теоретичні положення та визначення. Канали несанкціонованого отримання та руйнування інформації.	2	6
1.2	Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести. Криптографічно безпечні генератори псевдовипадкових послідовностей.	2	6
1.3	Симетричні криптосистеми. Блочний шифр: ГОСТ 28-147-89, AES.	2	5
	Симетричні криптосистеми. Поточний шифр: SNOW.	2	5
1.4	Криптоаналіз симетричних криптосистем.	2	6
1.5	Асиметричні криптосистеми (з відкритим ключем). Геш-функції. ЕЦП. Направлене шифрування. Обмін ключами.	2	10
1.6	Криптоаналіз асиметричних криптосистем.	2	6
1.7	Підходи до створення комплексної системи захисту інформації.	2	6
1.8	Модульна контрольна робота №1	1	4
	Всього за модулем №1	**17**	**54**
	Всього за 9 семестр	**17**	**54**
	Всього за дисципліною	**17**	**54**

2.2.2. Практичні заняття, їх тематика і обсяг

Таблиця 2.3

№ пор.	*Назва теми*	Обсяг навчальних занять (год.)	
		Прак.	СРС
1	2	3	4
9 семестр			
Модуль №1 «Основні поняття та симетричні криптосистеми. Асиметричні криптосистеми та особливості побудови криптографічних систем захисту інформації»			
1.1	Основні теоретичні положення та визначення. Канали несанкціонованого отримання та руйнування інформації.	2	2
1.2	Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести. Криптографічно безпечні генератори псевдовипадкових послідовностей. Розробка програмного забезпечення.	2	2
1.3	Генератори випадкових та псевдовипадкових послідовностей. Статистичні тести. Криптографічно безпечні генератори псевдовипадкових послідовностей. Дослідження властивостей.	2	2
1.4	Симетричні криптосистеми. Блочний шифр: ГОСТ 28-147-89, AES. Поточний шифр: SNOW. Розробка програмного забезпечення.	2	2

1	*2*	*3*	*4*
1.5	Симетричні криптосистеми. Блочний шифр: ГОСТ 28-147-89, AES. Поточний шифр: SNOW. Дослідження властивостей.	2	2
1.6	Асиметричні криптосистеми (з відкритим ключем). Геш-функції.	2	2
1.7	ЕЦП. Направлене шифрування. Обмін ключами.	2	2
1.8	Підходи до створення комплексної системи захисту інформації.	2	2
1.9	Підходи до створення комплексної системи захисту інформації.	1	2
	Всього за модулем №1	**17**	**18**
	Всього за 9 семестр	**17**	**18**
	Всього за дисципліною	**17**	**18**

2.2.3. Самостійна робота студента, її зміст та обсяг

Таблиця 2.4

№	Зміст самостійної роботи студента	Обсяг, год.
9 семестр		
1	Опрацювання лекційного матеріалу	50
2	Підготовка до практичних занять	18
3	Підготовка до модульної контрольної роботи №1	4
	Всього за 9 семестр	**72**
	Всього за дисципліною	**72**

2.2.4. Індивідуальні заняття

№	Зміст	Обсяг, год.
9 семестр		
1	Криптоаналіз симетричних криптосистем	1
2	Підходи до створення комплексної системи захисту інформації	1

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Список рекомендованих джерел

Основні рекомендовані джерела

3.1.1. В.А. Хорошко, А.А. Чекотков. Методы и средства защиты информации. –Юниор, 2003. 479 с.

3.1.2. Столингс В. Криптография и защита сетей: принципы и практика. 3-е издание. –М: Издательский дом «Вильямс», 2001. –672 с.

3.1.3. К. Шеннон. Теория связи в секретных системах // Работы по теории информации и кибернетике. М., ИЛ, 1963. -с. 333-369.

3.1.4. Intel Performance Primitives. User manual. URL: http://www.intel.com

3.1.5. В.В. Домарев. Безопасность информационных технологий. Методология создания систем защиты. — К.: ООО “ДС”, 2001. 688 с.

3.1.6. В.В. Домарев. Защита информации и безопасность компьютерных систем. К.: Издательство ДиаСофт, 1999. 480 с.

Додаткові рекомендовані джерела:

3.1.7. H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography// Kenneth H. Rosen Ed. 2006. 843 p.

3.1.8. О.В. Казарин. Теория и практика защиты программ. М.: МГУЛ, 2003. 450 с.

3.1.9. Microsoft Software Development Network. URL: http://www.msdn.com

3.2. Перелік наочних та інших навчально-методичних посібників, методичних матеріалів до технічних засобів навчання

№ пор.	Назва	Шифр тем за тематичним планом	Кількість
1.	Конспек лекцій	1.1. – 1.7.	Електронна версія
2.	Методичні вказівки з виконання практичних занять	1.1 – 1.9	1 прим. з кожної практичного заняття та їх електронні версії

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. Основні терміни, поняття, означення

4.1.1. ***Семестровий екзамен*** - це форма підсумкового контролю засвоєння студентом теоретичного та практичного матеріалу з окремої навчальної дисципліни за семестр. Складання екзамену здійснюється під час екзаменаційної сесії в комісії, яку очолює завідувач кафедри, відповідно до затвердженого в установленому порядку розкладу.

З метою забезпечення об'єктивності оцінок та прозорості контролю набутих студентами знань та вмінь, семестровий контроль здійснюються в університеті в письмовій формі або з використанням комп'ютерних інформаційних технологій. Ця норма не розповсюджується на дисципліни, викладення навчального матеріалу з яких потребує від студента переважно усних відповідей. Перелік дисциплін з усною (комбінованою) формою семестрового контролю встановлюється окремо за кожним напрямом (спеціальністю) підготовки фахівців з дозволу проректора з навчальної роботи.

4.1.2. ***Семестровий диференційований залік*** - це форма підсумкового контролю, що полягає в оцінці засвоєння студентом навчального матеріалу з певної дисципліни на підставі результатів виконання ним усіх видів запланованої навчальної роботи протягом семестру: аудиторної роботи під час лекційних, практичних, семінарських, лабораторних занять тощо та самостійної роботи при виконанні індивідуальних завдань (розрахунково-графічних робіт, рефератів тощо).

Семестровий диференційований залік не передбачає обов'язкову присутність студента і виставляється за умови, що студент виконав усі попередні види навчальної роботи, визначені робочою навчальною програмою дисципліни, та отримав позитивні (за національною шкалою) підсумкові модульні рейтингові оцінки за кожен з модулів. При цьому викладач для уточнення окремих позицій має право провести зі студентом додаткову контрольну роботу, співбесіду, експрес-контроль тощо.

4.1.3. ***Кредитно-модульна система –*** це модель організації навчального процесу, яка ґрунтується на поєднанні двох складових: модульної технології навчання та кредитів (залікових одиниць) і охоплює зміст, форми та засоби навчального процесу, форми контролю якості знань та вмінь і навчальної діяльності студента в процесі аудиторної та самостійної роботи. Кредитно-модульна система має за мету поставити студента перед необхідністю регулярної навчальної роботи протягом усього семестру з розрахунком на майбутній професійний успіх.

4.1.4. ***Навчальний модуль*** - це логічно завершена, відносно самостійна, цілісна частина навчального курсу, сукупність теоретичних та практичних завдань відповідного змісту та

структури з розробленою системою навчально-методичного та індивідуально-технологічного забезпечення, необхідним компонентом якого є відповідні форми рейтингового контролю.

4.1.5. ***Кредит (залікова одиниця)*** - це уніфікована одиниця виміру виконаної студентом аудиторної та самостійної навчальної роботи (навчального навантаження), що відповідає 36 годинам робочого часу.

4.1.6. ***Рейтинг (рейтингова оцінка)*** - це кількісна оцінка досягнень студента за багатобальною шкалою в процесі виконання ним заздалегідь визначеної сукупності навчальних завдань.

4.1.7. ***Рейтингова система оцінювання*** - це система визначення якості виконаної студентом усіх видів аудиторної та самостійної навчальної роботи та рівня набутих ним знань та вмінь шляхом оцінювання в балах результатів цієї роботи під час поточного, модульного (проміжного) та семестрового (підсумкового) контролю, з наступним переведенням оцінки в балах у оцінки за традиційною національною шкалою та шкалою ECTS.

РСО передбачає використання поточної, контрольної, підсумкової, підсумкової семестрової модульних рейтингових оцінок, а також екзаменаційної та підсумкової семестрових рейтингових оцінок.

4.1.7.1. ***Поточна модульна рейтингова оцінка*** складається з балів, які студент отримує за певну навчальну діяльність протягом засвоєння даного модуля - виконання та захист індивідуальних завдань (розрахунково-графічних робіт, рефератів тощо), лабораторних робіт, виступи на семінарських та практичних заняттях тощо.

4.1.7.2. ***Контрольна модульна рейтингова оцінка*** визначається (в балах та за національною шкалою) за результатами виконання модульної контрольної роботи з даного модуля.

4.1.7.3. ***Підсумкова модульна рейтингова оцінка*** визначається (в балах та за національною шкалою) як сума поточної та контрольної модульних рейтингових оцінок з даного модуля.

4.1.7.4. ***Підсумкова семестрова модульна рейтингова оцінка*** визначається (в балах та за національною шкалою) як сума підсумкових модульних рейтингових оцінок, отриманих за засвоєння всіх модулів.

4.1.7.5. ***Екзаменаційна рейтингова оцінка*** визначається (в балах та за національною шкалою) за результатами виконання екзаменаційних завдань.

4.1.7.6. ***Залікова рейтингова оцінка*** визначається (в балах та за національною шкалою) за результатами виконання всіх видів навчальної роботи протягом семестру.

4.1.7.7. ***Підсумкова семестрова рейтингова оцінка*** визначається як сума підсумкової семестрової модульної та екзаменаційної (залікової - у випадку диференційованого заліку) рейтингових оцінок (в балах, за національною шкалою та за шкалою ECTS).

Підсумкова рейтингова оцінка з дисципліни, яка викладається протягом декількох семестрів, визначається як середньозважена оцінка з підсумкових семестрових рейтингових оцінок у балах з наступним її переведенням у оцінки за національною шкалою та шкалою ECTS. Зазначена підсумкова рейтингова оцінка з дисципліни заноситься до додатку до диплому фахівця.

4.2. Порядок рейтингового оцінювання набутих студентом знань та вмінь

4.2.1. Оцінювання окремих видів виконаної студентом навчальної роботи та набутих знань та умінь здійснюється в балах відповідно до табл. 4.1.

Таблиця 4.1.

9 семестр		
Модуль №1		Max кількість балів
Вид навчальної роботи	Max кількість балів	
Виконання та захист поточних практичних завдань на практичних заняттях №1.1 – 1.9 (5х9)	45	
Опитування по матеріалам лекцій на практичних заняттях (13б х 1)	13	
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше 35 бала		
Виконання модульної контрольної роботи №1	30	
Усього за модулем №1	**88**	
Диференційований залік		**12**
Усього за 9 семестр		**100**

4.2.2. Виконаний вид навчальної роботи зараховується студенту, якщо він отримав за нього позитивну оцінку за національною шкалою відповідно до табл. 4.2.

4.2.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить поточну модульну рейтингову оцінку, яка заноситься до відомості модульного контролю.

4.2.4. Якщо студент успішно та своєчасно виконав передбачені в даному модулі всі види навчальної роботи (з позитивними за національною шкалою оцінками), то від допускається до модульного контролю з цього модуля.

Таблиця 4.2

Відповідність рейтингових оцінок за окремі види навчальної роботи у балах оцінкам за національною шкалою

Оцінка в балах			Оцінка за національною шкалою
Виконання та захист практичних завдань	Опитування по матеріалам лекцій на практичних заняттях	Виконання та захист модульної контрольної роботи	
5	12-13	27-30-	Відмінно
4	10-11	22-26	Добре
3	9-8	18-21	Задовільно
менше 3	менше 9	менше 18	Незадовільно

4.2.5. Модульний контроль здійснюється в комісії, яку очолює завідувач кафедри, шляхом виконання студентом модульної контрольної роботи тривалістю до двох академічних годин.

4.2.6. Сума поточної та контрольної модульної рейтингових оцінок становить підсумкову модульну рейтингову оцінку, яка виражається в балах та за національною шкалою відповідно до табл. 4.3.

4.2.7. Модуль зараховується студенту, якщо він під час модульного контролю отримав позитивну (за національною шкалою) контрольну модульну рейтингову оцінку (табл. 4.2) та позитивну підсумкову модульну рейтингову оцінку (табл. 4.3).

Таблиця 4.3

Відповідність підсумкових модульних рейтингових оцінок у балах оцінкам за національною шкалою

Модуль 1	Оцінка за національною шкалою
79-88	Відмінно
66-78	Добре
53-65	Задовільно
< 53	Незадовільно

4.2.8. У випадку відсутності студента на модульному контролі з будь-яких причин (через не допуск, хворобу тощо), проти його прізвища у колонці «Контрольна модульна рейтингова оцінка» відомості модульного контролю робиться запис «Не з'явився», а у колонці «Підсумкова модульна рейтингова оцінка» – «Не атестований».

При цьому студент вважається таким, що не має академічної заборгованості, якщо він має допуск до модульного контролю і не з'явився на нього з поважних причин, підтверджених документально. У протилежних випадках студент вважається таким, що має академічну заборгованість.

Питання подальшого проходження студентом модульного контролю у цих випадках вирішується в установленому порядку.

4.2.9. У випадку отримання незадовільної контрольної модульної рейтингової оцінки студент повинен повторно пройти модульний контроль в установленому порядку.

4.2.10. При повторному проходженні модульного контролю максимальна величина контрольної модульної рейтингової оцінки в балах, яку може отримати студент, дорівнює 26 (оцінці «Добре» за національною шкалою), тобто зменшується на чотири бали у порівнянні з наведеною в табл. 4.2.

4.2.11. Перескладання позитивної підсумкової модульної рейтингової оцінки з метою її підвищення не дозволяється.

4.2.12. Сума підсумкових модульних рейтингових оцінок у балах становить підсумкову семестрову модульну рейтингову оцінку, яка переховується в оцінку за національною шкалою (табл. 4.4).

4.2.13. Підсумкова семестрова рейтингова оцінка в семестрі дорівнює сумі підсумкової семестрової модульної рейтингової оцінки та залікової рейтингової оцінки, встановленої для кожної категорії підсумкових семестрових модульних рейтингових оцінок (***для "Відмінно" – 12 балів, для "Добре" – 10 балів, для "Задовільно" – 8 балів***) (табл. 4.5).

Таблиця 4.4

Відповідність підсумкових семестрових модульних рейтингової оцінки в балах оцінці за національною шкалою

Оцінка в балах	Оцінка за національною шкалою
79-88	Відмінно
66-78	Добре
53-65	Задовільно
менше 53	Незадовільно

Таблиця 4.5

Відповідність залікової рейтингової оцінки в балах оцінці за національною шкалою

Оцінка в балах	Оцінка за національною шкалою
12	Відмінно
10	Добре
8	Задовільно
-	

4.2.14. Сума підсумкової семестрової модульної та залікової рейтингової оцінки у балах становить підсумкову семестрову рейтингову оцінку, яка перераховується в оцінки за національною шкалою та шкалою ECTS

Таблиця 4.6

Відповідність підсумкової семестрової рейтингової оцінки в балах оцінці за національною шкалою та шкалою ECTS

Оцінка в балах	Оцінка за національною шкалою	Оцінка за шкалою ECTS	
		Оцінка	Пояснення
90-100	**Відмінно**	**A**	**Відмінно** (відмінне виконання лише з незначною кількістю помилок)
82 – 89	**Добре**	**B**	**Дуже добре** (вище середнього рівня з кількома помилками)
75 – 81		**C**	**Добре** (в загальному вірне виконання з певною кількістю суттєвих помилок)
67 – 74	**Задовільно**	**D**	**Задовільно** (непогано, але зі значною кількістю недоліків)
60 – 66		**E**	**Достатньо** (виконання задовольняє мінімальним критеріям)
35 – 59	**Незадовільно**	**FX**	**Незадовільно** (з можливістю повторного складання)
1 – 34		**F**	**Незадовільно** (з обов'язковим повторним курсом)

4.2.15. Повторне проходження семестрового контролю при отриманій раніше позитивній семестровій рейтинговій оцінці з метою підвищення підсумкової семестрової рейтингової оцінки не дозволяється.

4.2.16. Підсумкова семестрова рейтингова оцінка в балах, за національною шкалою та за шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента.

4.2.17. Підсумкова семестрова рейтингова оцінка заноситься до залікової книжки та навчальної картки студента, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E тощо***.

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки

(Ф 03.02 – 02)

АРКУШ ОЗНАЙОМЛЕННЯ З ДОКУМЕНТОМ

№ пор.	Прізвище ім'я по-батькові	Підпис ознайомленої особи	Дата ознайом-лення	Примітки

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ пор.	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	№ листа (сторінки)				Підпис особи, яка внесла зміну	Дата внесення зміни	Дата введення зміни
	Зміненого	Заміненого	Нового	Анульо-ваного			

(Ф 03.02 – 32)

УЗГОДЖЕННЯ ЗМІН

	Підпис	Ініціали, прізвище	Посада	Дата
Розробник				
Узгоджено				
Узгоджено				
Узгоджено				