(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра засобів захисту інформації

УЗГОДЖЕНО
Декан
_____ К. Нестеренко
«03» 06 2021 р.

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
_____ А. Полухін
«03» 06 2021 р.

Система менеджменту якості

РОБОЧА ПРОГРАМА

навчальної дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності»

Освітньо-професійна програма: «Системи технічного захисту інформації, автоматизація її обробки»
Галузь знань: 12 «Інформаційні технології»
Спеціальність: 125 «Кібербезпека»

Форма навчання	Сем.	Усього (год. / кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна	3	120/4	17	-	34	69	3 (1)	-	Екзамен
Заочна	3, 4	120/4	8	-	4	108	4	-	

Індекс: НБ-4-125-4/21 - 2.1.13
Індекс: НБ-4-125-4з/21 - 2.1.13

СМЯ НАУ РП 09.01.10-01-2021

Робочу програму навчальної дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» розроблено на основі освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», навчальних та робочих навчальних планів № НБ-4-125-4/21, № РБ-4-125-4/21 та № НБ-4-125-4з/21, № РБ-4-125-4з/21 підготовки здобувачів вищої освіти освітнього ступеня «Бакалавр» за спеціальністю 125 «Кібербезпека» та відповідних нормативних документів.

Робочу програму розробив:

Професор кафедри засобів захисту інформації
доцент _____ Лазаренко С.В.

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Системи технічного захисту інформації, автоматизація її обробки», спеціальності 125 «Кібербезпека» – кафедри засобів захисту інформації (випускова), протокол № 10 від «11» 05 2021 р.

Гарант освітньо-професійної програми _____ Темніков В.О.

Завідувач кафедри _____ Козловський В.В.

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради Факультету кібербезпеки, комп'ютерної та програмної інженерії, протокол № 5 від «12» Травня 2021 р.

Голова НМРР _____ Куклінський М.В.

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

ЗМІСТ

ВСТУП

Робоча програма (РП) навчальної дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» розроблена на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни денної та заочної форм навчання», затверджених наказом ректора розпорядженням від 29.04.2021 № 249/од, та відповідних нормативних документів.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Місце, мета, завдання навчальної дисципліни.

Навчальна дисципліна «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» відноситься до циклу професійної підготовки обов'язкової компоненти та є теоретичною і практичною основою сукупності знань та вмінь, що формують профіль фахівця в галузі інформаційної/кібернетичної безпеки.

Метою навчальної дисципліни є засвоєння порядку виявлення та блокування каналів несанкціонованого розповсюдження інформації; вивчення принципів побудови та порядку застосування пошукових систем та комплексів; організація та порядок проведення пошукових заходів з виявлення закладних пристроїв.

Завданнями вивчення навчальної дисципліни є:

- вивчення каналів витоку інформації та підстав їх утворення;
- вивчення систем та комплексів виявлення каналів витоку інформації;
- засвоєння порядку проведення обстеження об'єктів інформаційної діяльності (ОІД), з метою виявлення закладних пристроїв;
- оволодіння організаційними заходами щодо захисту інформації на ОІД.

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна.

За результатами вивчення навчальної дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» студенти повинні:

Знати:

- призначення, класифікацію та принципи побудови пошукових систем та комплексів;
- поняття, класифікацію та підстави утворення каналів витоку інформації;
- порядок використання пошукових систем, комплексів та засобів (засобів виявлення закладних пристроїв, відеокамер тощо);

- порядок проведення обстеження ОІД, з метою виявлення закладних пристроїв.

Вміти:

- самостійно проводити обстеження ОІД, з метою виявлення закладних пристроїв;
- самостійно застосовувати пошукові засоби та комплекси;
- здійснювати оцінку захищеності інформації, що циркулює на ОІД;
- забезпечувати гарантований захист інформації;
- вести технічну документацію, оформляти результати обстеження ОІД), (виявлення та блокування каналів витоку інформації, виявлення закладних пристроїв).

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

За результатами вивчення навчальної дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» студенти повинні здобути наступні програмні компетентності:

Інтегральну

- здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки та/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов;

Загальні

- здатність застосовувати знання у практичних ситуаціях;
- знання та розуміння предметної області та розуміння професії;
- вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;
- здатність до пошуку, оброблення та аналізу інформації;
- здатність використовувати технічні засоби захисту та охорони інформаційних ресурсів і баз даних обмеженого доступу;
- здатність організовувати функціонування системи організаційно-службових і спеціальних (охоронних) заходів із забезпечення інформаційної та/або кібербезпеки установ, підприємств, організацій;
- 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.

Фахові

- 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;
- здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки;

- здатність до використання програмних, апаратних та програмно-апаратних комплексів засобів захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних (автоматизованих) системах;

- здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки;

- здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки;

- здатність виявляти та блокувати канали витоку інформації, методи несанкціонованого доступу до інформації, джерел і способів дестабілізуючого впливу на інформацію, здійснювати пошук закладних пристроїв;

- здатність використовувати теоретичні знання та практичні навички з підготовки технічної документації.

1.4. Міждисциплінарні зв'язки

Навчальна дисципліна «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» базується на знаннях таких дисциплін: «Фізика», «Інформаційні технології», «Основи кібербезпеки» та є базою для вивчення наступних дисциплін: «Авіаційна безпека та кібербезпека авіаційних інформаційних систем», «Управління інформаційною безпекою», «Системи технічного захисту інформації», «Комлексні системи захисту інформації», «Методи та засоби технічного захисту інформації».

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни.

Навчальний матеріал дисципліни структурований за модульним принципом і складається з двох навчальних модулів, а саме:

– навчального **модуля № 1 «Канали несанкціонованого отримання інформації»**

– навчального **модуля № 2 «Засоби захисту інформації на об'єктах інформаційної діяльності».**

Кожен з модулів є логічно завершеною, відносно самостійною, цілісною частиною навчальної дисципліни, засвоєння якої передбачає проведення модульної контрольної роботи та аналіз результатів її виконання.

2.2. Модульне структурування та інтегровані вимоги до кожного модуля.

Модуль № 1 «Канали несанкціонованого отримання інформації».

Інтегровані вимоги модуля № 1:

знати

- нормативно-правове забезпечення інформаційної/кібернетичної безпеки;
- заходи із забезпечення інформаційної/кібернетичної безпеки;
- класифікацію та підстави утворення каналів витоку інформації;
- класифікацію та принципи функціонування засобів несанкціонованого отримання інформації.

вміти

- визначати режимні території (зони) на ОІД;
- аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам;

Тема 1. Інформаційна/кібербезпека та її складові елементи.

Поняття інформаційної/кібербезпеки та її складових елементів. Нормативно-правове забезпечення інформаційної/кібернетичної безпеки. Організаційні заходи щодо захисту інформації. Завдання, які вирішуються системами та комплексами (приладами) інформаційної/кібербезпеки.

Тема 2. Канали несанкціонованого отримання інформації.

Підстави утворення каналів витоку інформації. Загальна характеристика та класифікація каналів витоку інформації (легальні, напівлегальні, нелегальні). Особливості природних та штучних каналів витоку інформації. Поняття технічних каналів витоку інформації.

Тема 3. Технічні канали витоку інформації.

Поняття та ознаки радіотехнічного каналу витоку інформації. Поняття та ознаки електричного каналу витоку інформації. Поняття та ознаки візуально-оптичного каналу витоку інформації. Поняття та ознаки матеріально-речовинного каналу витоку інформації. Поняття та ознаки акустичного каналу витоку інформації.

Тема 4. Засоби перехоплення (з'єму) інформації.

Поняття та загальна характеристика засобів перехоплення (з'єму) інформації. Класифікація засобів перехоплення (з'єму) інформації. Ознаки застосування засобів перехоплення (з'єму) інформації. Особливості побудови та функціонування закладних пристроїв.

Модуль № 2 «Засоби захисту інформації на об'єктах інформаційної діяльності».

Інтегровані вимоги модуля № 2:

знати

- організаційні заходи із забезпечення ТЗІ на ОІД;
- призначення, класифікацію та принципи побудови пошукових систем та комплексів;
- особливості використання пошукових систем та комплексів.

вміти

- відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем та комплексів ТЗІ після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження;
- використовувати пошукові системи та комплекси;
- оцінювати захищеність інформації, що циркулює на ОІД;
- вести технічну документацію (оформляти результати пошукових заходів).

Тема 1. Класифікація систем і пристроїв виявлення закладних пристроїв.

Загальна характеристика методів та засобів пошуку каналів витоку інформації та закладних пристроїв. Призначення та порядок проведення візуального огляду ОІД. Особливості використання металодетекторів при виявленні закладних пристроїв.

Тема 2. Індикатори (детектори) електромагнітного поля.

Поняття, призначення та класифікація індикаторів (детекторів) електромагнітного поля. Порядок використання індикаторів поля під час пошуку радіозакладних пристроїв. Поняття, призначення та класифікація засобів пошуку скритно встановлених відеокамер (проводових/радіо). Порядок використання засобів виявлення скритно встановлених відеокамер.

Тема 3. Спеціальні радіоприймальні пристрої виявлення закладних пристроїв.

Загальна характеристика спеціальних радіоприймальних пристроїв виявлення закладних пристроїв. Принципи побудови спеціальних приймачів виявлення закладних пристроїв. Основні види панорамних приймачів та їх характеристики.

Тема 4. Програмно-апаратні комплекси виявлення закладних пристроїв.

Загальна класифікація і принципи побудови програмно-апаратного комплексів виявлення закладних пристроїв. Основні характеристики і принцип роботи OSC-5000. Основні характеристики і принцип роботи СРМ-700. Основні характеристики і принцип роботи ST-031. Основні характеристики і принцип роботи DigiScan EX. Основні характеристики і принцип роботи комплексів АРК.

Тема 5. Використання нелінійних радіолокаторів для виявлення закладних пристроїв.

Принципи побудови та роботи нелінійних радіолокаторів. Класифікація і загальна характеристика нелінійних радіолокаторів. Характеристика основних типів нелінійних радіолокаторів. Порядок використання нелінійних радіолокаторів.

2.3. Тематичний план.

№ пор	Назва теми (тематичного розділу)	Обсяг навчальних занять (год.)							
		Денна форма навчання				Заочна форма навчання			
		Усього	Лекції	Лаб./прак. заняття	СРС	Усього	Лекції	Лаб./прак. заняття	СРС
		3 семестр				3, 4 семестр			
Модуль № 1 «Канали несанкціонованого отримання інформації»									
1.1	Тема 1. Інформаційна/кібербезпека та її складові елементи.	10	2	2	6	-	-	-	-
1.2	Тема 2. Канали несанкціонованого отримання інформації.	12	2	2 2	6	29	2	2	25
1.3	Тема 3. Технічні канали витоку інформації.	12	2	2 2	6	-	-	-	-
1.4	Тема 4. Засоби перехоплення (з'єму) інформації.	10	2	2	6	27	2	-	25
1.5	Модульна контрольна робота № 1	4	-	1	3	-	-	-	-
Усього за модулем № 1		**48**	**8**	**13**	**27**	**56**	**4**	**2**	**50**
Модуль № 2 «Засоби захисту інформації на об'єктах інформаційної діяльності»									
2.1	Тема 1. Класифікація систем і пристроїв виявлення закладних пристроїв.	12	2	2 2	6	29	2	2	25
2.2	Тема 2. Індикатори (детектори) електромагнітного поля.	12	2	2 2	6	-	-	-	-
2.3	Тема 3. Спеціальні радіоприймальні пристрої виявлення закладних пристроїв.	12	2	2 2	6	-	-	-	-
2.4	Тема 4. Програмно-апаратні комплекси виявлення закладних пристроїв.	12	2	2 2	6	27	2	-	25
2.5	Тема 5. Використання нелінійних радіолокаторів для виявлення закладних пристроїв.	11	1	2 2	6	-	-	-	-
2.6	Модульна контрольна робота № 2	5	-	1	4	-	-	-	-
2.7	Домашнє завдання	8	-	-	8	-	-	-	-
2.8	Контрольна робота (домашня)	-	-	-	-	8	-	-	8
Усього за модулем № 2		**72**	**9**	**21**	**42**	**64**	**4**	**2**	**58**
Усього за навчальною дисципліною		**120**	**17**	**34**	**69**	**120**	**8**	**4**	**108**

2.4. Домашнє завдання, контрольна робота (домашня).

Домашнє завдання, контрольна робота (домашня) з дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» виконується самостійно кожним студентом і є важливим етапом у засвоєнні навчального матеріалу.

Домашнє завдання, контрольна робота (домашня) охоплює всі основні теми дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» та виконується з метою закріплення та поглиблення теоретичних

знань та вмінь студентів в області організації робіт з виявлення закладних пристроїв та блокування каналів витоку інформації.

Питання для виконання домашнього завдання доводяться викладачем до студента індивідуально і виконуються відповідно до розроблених провідним викладачем методичних матеріалів, затверджених протоколом кафедри розробника.

Завдання для виконання контрольної роботи (домашньої) розробляються автором робочої програми. Навчальні матеріали затверджуються протоколом засідання випускової кафедри, доводяться до відома студента індивідуально і виконуються відповідно до методичних рекомендацій.

Час, потрібний для виконання домашнього завдання, контрольної роботи (домашньої) – до 8 годин самостійної роботи.

2.5. Перелік питань для підготовки до екзамену.

Перелік питань та зміст завдань, для підготовки до екзамену, розробляються провідним викладачем кафедри відповідно до робочої програми, затверджується на засіданні кафедри та доноситься до відома студентів.

3. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.1. Методи навчання

При вивченні навчальної дисципліни «Виявлення закладних пристроїв на об'єктах інформаційної діяльності» використовуються навчальні технології, що застосовуються для активізації навчально-пізнавальної діяльності студентів, а саме: робота в малих групах, семінар-дискусія, мозкова атака, кейс, презентація, рольова гра, дидактична гра тощо.

Використання технології *дистанційного навчання* реалізуються за допомогою комп'ютерної техніки, шляхом проведення занять з використанням чат-технологій, дистанційних занять, конференцій, семінарів, ділових ігор, лабораторних робіт, практикумів й інших форм навчальних занять, які проводяться за допомогою засобів телекомунікацій з використанням веб-технологій.

Також, використовується *проблемно-орієнтоване навчання* (яке передбачає формулювання та вирішення проблеми під час лекцій, розв`язання ситуативних задач на семінарах, практичних заняттях, дослідження проблеми під час самостійної роботи студентів) та *практико-орієнтоване навчання* (здійснюється через різні види практик на підприємствах, установах та організаціях різних форм власності).

3.2. Рекомендована література (базова і допоміжна)

Базова література

3.2.1. Закон України "Про інформацію".

3.2.2. Закон України "Про державну таємницю".

3.2.3. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

3.2.4. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

3.2.5. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. НД ТЗІ 3.7-003-05 [Електронний ресурс] / Нормативна база Держспецзв'язку // 2015 - Режим доступу:http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

3.2.6. НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

3.2.7. НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

3.2.8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

3.2.9. Самохвалов Ю.Я., Темніков В.О., Хорошко В.О. Організаційно-технічне забезпечення захисту інформації. Навчальний посібник.- Київ: НАУ, 2012.- 207 с.

3.2.10. Методы и средства защиты информации Хорошко В.А., Чекатков А.А. – К.: ЮНИОР, 2003.

3.2.11. Большая энциклопедия промышленного шпионажа Каторин Ю.Ф., Куренков Е.В., Лысов А.В., Остапенко А.Н..- СПб.: Полигон, 2000.

3.2.12. Максименко Г.А., Хорошко В.О. Методи виявлення, обробки та ідентифікації сигналів радіозакладних приладів. - К.: ООО „Поліграф Консалтинг", 2004.-317 ст.

3.2.13. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО „ТИД „ДС", 2002. – 688 с.

Допоміжна література

3.2.14. Домарев В.В. Безопасность информационных технологий. Системный подход. К.: ООО „ТИД „ДС", 2014. – 992 с.

3.2.15. Системы и устройства информационной безопасности. Учебное пособие / под ред. проф. В.А. Хорошко/ Соавторы: А.П. Провозин, О.В. Рыбальский, В.А.Хорошко, Д.В. Чирков/- К. ДУИКТ, 2007.

3.2.16. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. –178 с.

3.3. Інформаційні ресурси в Інтернет

3.3.1. http://www.czo.gov.ua/index.php?page=docs&id=41.

3.3.2. http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=97BBACF714A05BF6459C5F476282F024?art_id=39738&cat_id=38835.

3.3.3. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article;jsessionid=BA075F688F4E729D7C88A20E1C636EA4?art_id=40393&cat_id=38835.

3.3.4. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

3.3.5. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40396&cat_id=38835.

3.3.6. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835.

3.3.7. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40381&cat_id=38835.

3.3.8. http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40374&cat_id=38835.

3.3.9. http://tzi.com.ua/rubzh-rso-versya-20.html.

3.3.10. http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art id=46074.

3.3.11. https://metod.onat.edu.ua.

3.3.12. http://www.nau.edu.ua

3.3.13. http://www.kzzi.nau.edu.ua

3.3.14. https://www.coursera.org/learn/r-programming/

3.3.15. http://prometheus.org.ua/dataanalysis/

Відповідне інформаційне та навчально-методичне забезпечення розташоване на освітніх платформах Google Classroom, Moodle (Modular Object-Oriented Dynamic Learning Environment).

Електронний репозитарій наукової бібліотеки НАУ: http://er.nau.edu.ua.

Всі ресурси науково-технічної бібліотеки доступні через сайт університету: http://www.lib.nau.edu.ua.

4. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

4.1. Методи контролю та схема нарахування балів.

Оцінювання окремих видів виконаної студентом навчальної роботи здійснюється в балах відповідно до табл. 4.1.

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

Таблиця 4.1

Вид навчальної роботи	Max кількість балів	
	Денна форма навчання	Заочна форма навчання
	3 семестр	4 семестр
Модуль № 1 «Канали несанкціонованого отримання інформації»		
Виконання та захист лабораторних робіт	15	20
Для допуску до виконання модульної контрольної роботи № 1 студент має набрати не менше	*9*	-
Виконання модульної контрольної роботи № 1	15	-
Усього за модулем № 1	**30**	**20**
Модуль № 2 «Засоби захисту інформації на об'єктах інформаційної діяльності»		
Виконання та захист лабораторних робіт	20	20
Виконання домашнього завдання	15	-
Виконання контрольної роботи (домашньої)	-	20
Для допуску до виконання модульної контрольної роботи № 2 студент має набрати не менше	*12*	-
Виконання модульної контрольної роботи № 2	15	-
Усього за модулем № 2	**50**	**40**
Усього за модулями № 1, № 2	**80**	**60**
Семестровий екзамен	**20**	**40**
Усього за дисципліною	**100**	

4.2. Виконані види навчальної роботи зараховуються студенту, якщо він отримав за них позитивну рейтингову оцінку (табл. 4.2).

Таблиця 4.2

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

Рейтингова оцінка в балах					Оцінка за національною шкалою
Виконання та захист лабораторної роботи		Виконання контрольної роботи (домашньої)	Виконання домашнього завдання	Виконання модульної роботи	
14 - 15	18 - 20	18 - 20	14 - 15	14 - 15	Відмінно
12 - 13	15 - 17	15 - 17	12 - 13	12 - 13	Добре
9 - 11	12 - 14	12 - 14	9 - 11	9 - 11	Задовільно
менше 9	менше 12	менше 12	менше 9	менше 9	Незадовільно

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

4.4. Сума підсумкової семестрової модульної та екзаменаційної рейтингових оцінок, у балах становить підсумкову семестрову рейтингову оцінку (табл. 4.3, 4.4), яка перераховується в оцінки за національною шкалою та шкалою ECTS (табл. 4.5).

Таблиця 4.3

Відповідність підсумкової семестрової модульної рейтингової оцінки в балах оцінкам за національною шкалою

Оцінка в балах		Оцінка за національною шкалою
72 - 80	54 - 60	Відмінно
60 - 71	45 - 53	Добре
48 - 59	36 - 44	Задовільно
менше 48	менше 44	Незадовільно

Таблиця 4.4

Відповідність екзаменаційної рейтингової оцінки в балах оцінці за національною шкалою

Оцінка в балах		Оцінка за національною шкалою
18 - 20	36 - 40	Відмінно
15 - 17	30 - 35	Добре
12 - 14	24 - 29	Задовільно
менше 12	менше 24	Незадовільно

Таблиця 4.5

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)

4.5. Підсумкова семестрова рейтингова оцінка в балах, за національною шкалою та шкалою ECTS заноситься до заліково-екзаменаційної відомості, навчальної картки та залікової книжки студента, наприклад, так: ***92/Відм./A, 87/Добре/B, 79/Добре/C, 68/Задов./D, 65/Задов./E*** тощо.

4.6. Підсумкова рейтингова оцінка з дисципліни дорівнює підсумковій семестровій рейтинговій оцінці. Зазначена підсумкова рейтингова оцінка з дисципліни заноситься до Додатку до диплома.

(Ф 03.02 – 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

№ прим.	Куди передано (підрозділ)	Дата видачі	П.І.Б. отримувача	Підпис отримувача	Примітки
1	03.02	03.06.21	Федоренко К.А.		

(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				