(Ф 03.02 – 110)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Факультет комп'ютерних наук та технологій
Кафедра технічного захисту інформації

ЗАТВЕРДЖУЮ
Декан ФКНТ
_____ Андрій ФЕСЕНКО
«10» 03 2026 р.

КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ

РОБОЧА ПРОГРАМА

навчальної дисципліни

«Захист інформації»

Освітньо професійна програма: «Документознавство та інформаційна діяльність»
Галузь знань: 02 «Культура, мистецтво »
Спеціальність: 029 «Інформаційна бібліотечна, та архівна справа»

Форма здобуття освіти	Сем.	Усього (год. / кредитів ECTS)	ЛКЦ	ПР.З	Л.З	СРС	ДЗ / РГР / К.р	КР / КП	Форма сем. контролю
Денна	2д	135/4,5	36	36	-	63	-	-	Диф залік 2 с
Заочна	2,3	135/4,5	6	8		121	К.Р.-3с.		Диф залік 3 с

Індекс: № РБ-8-029-1/25-2.1.10
Рб-8-029-1з/23-2.1.10

Робочу програму навчальної дисципліни «Захист інформації» розроблено на основі освітньої-професійної програми «Документознавство та інформаційна діяльність», навчальних та робочих навчальних планів № НБ(РБ)-8-029-1/25, НБ(РБ)-8-029-1/25(з) підготовки здобувачів вищої освіти освітнього ступеня «Бакалавр» за спеціальністю 029 «,Інформаційна бібліотечна, та архівна справа» та відповідних нормативних документів.

Робочу програму розробив
доцент кафедри засобів захисту інформації,
к.т.н., доцент _____ Тетяна ЩЕРБАК

Робочу програму обговорено та схвалено на засіданні кафедри технічного захисту інформації, протокол № 1 від 25. 08 2025р.

Завідувач кафедри _____ Валерій КОЗЛОВСЬКИЙ

Робочу програму обговорено та схвалено на засіданні випускової кафедри освітньо-професійної програми «Документознавство та інформаційна діяльність», спеціальності 029 «Інформаційна бібліотечна ,а та архівна справа» - кафедри «Української мови » , протокол № 1 від 22 січня 2026 р.

Гарант освітньо-професійної програми
«Документознавство та інформаційна діяльність» _____ Ірина ТЮРМЕНКО

Завідувач кафедри _____ Анастасія СІБРУК

Робочу програму обговорено та схвалено на засіданні науково-методично-редакційної ради факультету комп'ютерних наук та технологій, протокол № 1 від «11 » лютого 2026 р.

Голова НМРР _____ Оксана ПОЛІЩУК

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

Вступ 4

1. Пояснювальна записка 4

1.1. Місце, мета, завдання навчальної дисципліни 4

1.2. Результати навчання, які дає можливість досягти навчальна дисципліна 4

1.3. Компетентності, які дає можливість здобути навчальна дисципліна 5

1.4. Міждисциплінарні зв`язки 6

2. Програма навчальної дисципліни 6

2.1. Зміст навчальної дисципліни 6

2.2. Модульне структурування та інтегровані вимоги до кожного модуля 7

2.3. Тематичний план 9

2.4. Завдання на контрольну (домашню) роботу 11

2.5. Перелік питань для підготовки до підсумкової контрольної роботи (ЗФН) 11

3. Навчально-методичні матеріали з дисципліни 12

3.1. Методи навчання 12

3.2. Рекомендована література (базова і допоміжна) 13

3.3. Інформаційні ресурси в Інтернет 14

4. Рейтингова система оцінювання набутих студентом знань та вмінь 14

ВСТУП

Робоча програма (РП) навчальної дисципліни «Захист інформації» розроблена на основі «Методичних рекомендацій до розроблення і оформлення робочої програми навчальної дисципліни, та відповідних нормативних документів.

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

1.1. Заплановані результати.

Місце даної дисципліни є теоретичною основою сукупності знань та вмінь, що формують профіль фахівця з кібербезпеки в області комплексного підходу до побудови систем захисту інформації.

Метою є вивчення теоретичних основ проблеми зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення конфіденційної інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформації. Вивчення методологічних, організаційних та наукових основ розробки засобів і систем збору та захисту інформації (ЗІ), забезпечення інформаційної безпеки процесів опрацювання, зберігання та поширення інформації в інформаційно-комунікаційних мережах з урахуванням сучасного стану та прогнозу розвитку методів, систем і засобів здійснення погроз з боку потенційних порушників.

Завданнями вивчення навчальної дисципліни є:

- засвоєння основних теорій інформації й сучасних захищених інформації;
- формування загальних вимог до захисту інформації;
- оволодіння сучасним методами обробки, перетворення та захисту інформації в комп'ютерних системах;
- оволодіння навичками основи криптології та крипто аналізу;
- засвоєння методів й алгоритмів експлуатації програмних систем збору, закриття, відновлення і автентифікації інформації;
- ознайомлення з порядком сучасних способів боротьби з несанкціонованим блокуванням, копіюванням, зміною та збором інформації;
- засвоєння порядку програминих засобів забезпечення інформаційної безпеки;
- оволодіння навичками практичного вирішення завдання захисту програм та даних.

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

За результатами вивчення навчальної дисципліни «Захист інформації» студенти набувають таких знань та вмінь:

ПРН 4. Застосовувати у професійній діяльності технології інформаційного менеджменту, створення і підтримки функціонування електронних бібліотек та архівів, баз даних, методологію вивчення та задоволення культурних та інформаційних потреб користувачів.

ПРН 5. Узагальнювати, аналізувати і синтезувати інформацію в діяльності, пов'язаній з її пошуком, накопиченням, зберіганням та використанням.
ПРН 7. Забезпечувати ефективність функціонування документно-комунікаційних систем.
ПРН 8. Використовувати знання технічних характеристик, конструкційних особливостей, призначення і правил експлуатації комп'ютерної техніки та офісного обладнання для вирішення технічних завдань спеціальності.
ПРН 12. Застосовувати сучасні методики і технології автоматизованого опрацювання інформації, формування та використання електронних інформаційних ресурсів та сервісів.

1.3. Компетентності, які дає можливість здобути навчальна дисципліна.

У результаті вивчення даної навчальної дисципліни студенти повинні набути такі **компетентності**:

ІК. Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі інформаційної, бібліотечної та архівної справи, та соціальних комунікацій або у процесі навчання щодо передбачення застосування положень і методів інформаційної, бібліотечної та архівної справи і характеризується комплексністю та неповною визначеністю умов

Загальні

ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
ЗК 3. Здатність знати та розуміти предметну
область та професійну діяльність.
ЗК 7. Здатність до пошуку, опрацювання та аналізу інформації з різних джерел.

Фахові

ФК 3. Здатність використовувати сучасні прикладні комп'ютерні технології, програмне забезпечення, мережеві та мобільні технології для вирішення професійних завдань.
ФК 11. Здатність використовувати автоматизовані інформаційно-пошукові системи, організовувати електронні бібліотеки та архіви.
ФК 12. Здатність створювати, наповнювати та забезпечувати функціонування вебсайтів та вебспільнот у мережі «Інтернет». .
ФК 14. Здатність до подальшого навчання з високим рівнем автономності, постійного підвищення рівня інформаційної культури.

Міждисциплінарні зв'язки

Навчальна дисципліна «Захист інформації» є базою для вивчення наступних дисциплін: «Інформаційна аналітична діяльність», «Бібліотекознавство», «Управління проєктами в інформаційній сфері».

2. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

2.1. Зміст навчальної дисципліни

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

- навчального **модуля № 1 «Безпека і захист даних»**;
- навчального **модуля № 2 «Засоби криптографічного захисту»**.

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 «Безпека і захист даних».

Інтегровані вимоги модуля №1:

Знати:

основи вітчизняного та міжнародного законодавства в сфері побудови систем захисту інформації;

методика визначення складу інформації, що захищається;

каналів несанкційованого доступу до інформації;;

моделі загроз та порушника.

Вміти:

самостійно управляти ризиками на вимогу основних законодавчім актам;

самостійно будувати кадрове забезпечення комплексної системами захисту інформації;

самостійно оцінити ризики, канали витоку комплексної системи захисту інформації:

Тема 1. Теоретичні основи інформаційної безпеки

Вступ до захисту інформації Цілі підтримки безпеки. Атаки. Послуги і механізми. Методи Характеристика інформаційної безпеки Умови безпеки інформації Державна політика та система технічного захисту інформації в Україні. Нормативно-правова база України у сфері технічного захисту інформації Структура системи захисту інформації

Тема 2. Інформаційна система персональних даних.

Нормативні документи захисту даних. Конфіденційність персональних даних Захист персональної інформації Європейська система захисту персональних даних

Тема 3. **Інформація, як основне джерело захисту.**

Методика визначення складу інформації, що захищається. Класифікація інформації за видами таємниці і ступенями конфіденційності. Визначення об'єктів

захисту. Сховища носіїв інформації, як об'єкт захисту. Методи оцінки захищеності підприємства.

Тема 4. Канали та методи несанкційованого доступу до інформації.

Методика виявлення каналів несанкційованого доступу до інформації. Ділова розвідка, як канал несанкційованого доступу до інформації. Легальні, напівлегальні та нелегальні способи отримання інформації.

Тема 5. Модель загроз.

Оцінка загроз безпеки інформації. Джерела, явища, фактори і умови дестабілізованого впливу на інформацію. Види і способи дестабілізованого впливу на інформацію з боку людей. Види і способи дестабілізованого впливу на інформацію з боку технічних засобів, технологічних процесів і природних явищ. Порядок розроблення та оформлення моделі загроз.

Тема 6. Модель потенційного порушника.

Джерела, явища, фактори і умови дестабілізованого впливу на інформацію. Оцінка загроз безпеки інформації. Види і способи дестабілізованого впливу на інформацію з боку порушника. Порядок розроблення та оформлення моделі порушника

Тема 7 Апаратні засоби захисту інформації

Основи апаратного захисту Класифікація технічних засобів зняття інформації Основні групи технічних засобів ведення розвідки Радіо-мікрофони Основні методи прослуховування телефонних ліній Телефонні радіо-транслятори. Системи прослуховування повідомлень, переданих по стільникових, пейджингових каналах і по факсу.Використання телефонної лінії для прослуховування приміщень. Спеціальні пристрої прослуховування Системи і пристрої відеоконтролю Пристрої дистанційного управління, відео-детектор руху.Системи та засоби виявлення, пошуку та знешкоджування технічних засобів зняття інформації. Основні стаціонарні засоби захисту інформації. Пошукове устаткування

Тема 8. Програмні засоби, що містять небезпеку

Перехоплювачі паролів першого роду. Перехоплювачі паролів другого роду. Перехоплювачі паролів третього роду. Принципа роботи троянских программ . Принципи роботи утиліт скритного адміністрування Комп'ютерні віруси і механізми боротьби з ними Класифікація комп'ютерних вірусів. Методи і засоби боротьби з вірусами. Пакетні фільтри

Модуль № 2 «Засоби криптографічного захисту».

Інтегровані вимоги модуля №2:

Знати:

розроблення політики безпеки ОІД,ІТС
вимоги до сучасних криптосистем
основи криптоаналізу;
шифри із симетричним ключем, шифри потоку і блокові шифри;
реагування на інциденти в глобальній мережі.

Вміти :
самостійно розробляти політику інформації;
самостійно оцінювати надійність розробленої політики інформації за допомогою методів шифрування;

Тема 9. Розроблення політики безпеки.

Сутність та призначення політики безпеки ОІД, ІТС, підприємства. Порядок розробки політики безпеки ОІД. Порядок розробки політики безпеки ІТС. Розробка політики безпеки підприємства. Вибір варіанту КСЗІ та порядок оформлення політики безпеки.

Тема 10. . Криптографічний захист інформації

Основи криптоаналізу. Стеганографія Історія криптографії. Класифікація та вимоги до сучасних криптосистем

Тема 11. . Традиційні шифри із симетричним ключем.

Шифри із симетричним ключем. Шифр підстановки Шифри із симетричним ключем. Шифр перестановки. Шифри потоку і блокові шифри. Алгебраїчні структури Криптографія із симетричними ключами.

Тема 12. Сучасні блокові шифри

. Сучасні шифри потоку і блокові шифри. Стандарт шифрування даних (DES). Аналіз DES. Багатократне застосування. Загальний опис криптоалгоритму стандарту шифрування AESC. Симетричні криптосистеми. Шифр Калина.

Тема 13 Режими роботи симетричних криптоалгоритмів

Математичні основи асиметричної криптографії. Криптосистеми RSA та Ель-Гамаля. Поняття електронного цифрового підпису. Електронний цифровий підпис DSA та ECDSA. Криптографічні функції хешування

Тема 14. Безпека в комп'ютерних мережах

Використання міжмережевих екранів. Політика безпеки під час роботи в мережі

Тема 15. . Захист інформації в глобальних мережах.

Загальні принципи побудови глобальних комп'ютерних мереж. Політика безпеки при роботі в глобальній мережі. Погрози при роботі з глобальними мережами. Реагування на інциденти в глобальній мережі.

2.3. Тематичний план

№ з/п	Назва теми	Обсяг навчальних занять (год.)							
		Денна форма навчання				Заочна форма навчання			
		Усього	Лекції	Практ. заняття	СРС	*Усього*	Лекції	Практ. заняття	СРС
Модуль № 1 «Безпека і захист даних».									
		2 семестр				**2 семестри**			
1.1	Теоретичні основи інформаційної безпеки	10	2 2	2	4	10			10
1.2	Інформаційна система персональних даних.	8	2	2	4	8			8
1.3	Інформація, як основне джерело захисту.	8	2	2	4	8	1	1	6
1.4	Канали та методи несанкційованого доступу до інформації.	8	2	2	4	8	–		8
1.5	Модель загроз	8	2	2	4	8	1	1	6
1.6	Модель потенційного порушника.	8	2	2	4	9	1	2	6
1.7	Апаратні засоби захисту інформації	8	2	2	4	6			6
1.8	Програмні засоби, що містять небезпеку	8	2	2	4	4			4
1.9	Модульна контрольна робота № 1	3	-	2	1	1			1
	Усього за модулем №1	***69***	***18***	***18***	***33***	**62**	**3**	**4**	**55**
Модуль № 2 «Засоби криптографічного захисту»									
2.1	Розроблення політики безпеки.	8	2	2	4	11	1	2	8
2.2	Криптографічний захист інформації	7	2	2	3	10			10
2.3	Традиційні шифри із симетричним ключем	6	2	2	2	8			8
2.4	Сучасні блокові шифри	9	2	2	5	9	1		8
2.5	Режими роботи симетричних криптоалгоритмів	11	2	2 2	5	8			8
2.6	Безпека в комп'ютерних мережах	13	2 2	2 2	5	7	1	1	5
2.7	Захист інформації в глобальних мережах.	11	2 2	2	5	10			10

2.8	Контрольна робота					8	–	–	8
2.9	Модульна контрольна робота № 2	3		2	1	2		1	1
	Усього за модулем №2/ за 2 семестр (ЗФИ)	**66**	**18**	**18**	**30**	**73**	**3**	**4**	**66**
Усього за навчальною дисципліною		**135**	**36**	**36**	**63**	**135**	**6**	**8**	**121**

2.4. Завдання на контрольну (домашню) роботу .

Контрольна (домашня) робота .

Контрольна (домашня) робота з дисципліни виконується у третьому семестрі, відповідно до затверджених в установленому порядку методичних рекомендацій, з метою закріплення та поглиблення теоретичних знань та вмінь студента при вивченні дисципліни.

Теми та завдання для виконання практичної частини контрольної (домашньої) роботи здійснюється студентом в індивідуальному порядку відповідно до методичних рекомендацій, розроблених провідними викладачами кафедри.

Час, потрібний для виконання контрольної складає 8 годин самостійної роботи.

2.5. Перелік питань для підготовки до підсумкової контрольної роботи (ЗФН).

Перелік питань та зміст завдань для підготовки до підсумкової контрольної роботи 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

Під час вивчення навчальної дисципліни «Комплексні системи захисту інформації» 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. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІАЛИ З ДИСЦИПЛІНИ

3.2. Рекомендована література (базова і допоміжна)

Базова література

3.2.1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] / База законодавства України // № 80/94-ВР – Режим доступу: http://zakon4.rada.gov.ua/laws/ show/80

3.2.2. . Закон України «Про інформацію».

3.2.3. Закон України «Про державну таємницю».

3.2.4. Закон України «Про захист інформації в інформаційно-комунікаційних системах».

3.2.5. Закон України «Про захист персональних даних».

3.2.5. Закон України «Про основні засади забезпечення кібербезпеки України».

3.2.7. Положення «Про технічний захист інформації» (із змінами), затверджене Указом Президента України від 27.09.1999 № 1229/99.

3.2.8. ДСТУ 3396.0-96. «Захист інформації. Технічний захист інформації. Основні положення».

Допоміжна література

3.2.9. Information Security Handbook for Network Beginners. National Center of Incident Readiness and Strategy for Cybersecurity (NISC) ver. 2.11e

3.2.10. Nigel Cawthorne. Alan Turing: The Enigma Man. – Acturus, 2019. – 128 p.

3.2.11. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с.

3.2.12. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с.

3.2.13. Інформаційна безпека/ За ред. Ю. Я. Бобала та І. В. Горбатого. Львівська політехніка, 2019.-540 с.

3.2.14. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.: Видавництво Ліра-К, 2021. – 412 с. 10

3.2.15. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв,О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с.

3.2.16. Кібербезпека в сучасному світі : матеріали III Всеукраїнської науково практичної конференції (м. Одеса, 19 листопада 2021 р.) / за ред. О. В. Дикого ;уклад.: С. А. Горбаченко, Н. І. Логінова. – Одеса, 2020. – 148 с.

3.2.17. Кібербезпека: лабораторний практикум з основ криптографічного захисту/ Євсеєв С.П. , Король О.Г. Новий світ-2000, 2021.-241 с.

3.2.18. Криптоаналіз. Криптографічні протоколи / О.М. Гапак // Навчальний посібник з курсу «Комп'ютерна криптографія» для студентів інженерно-технічного факультету спеціальності 123-«Комп'ютерна інженерія». Ужгород: видавництво ПП «АУТДОР-ШАРК», 2021р. – 96с..

3.2.19. Лісовська Ю. Кібербезпека. Ризики та заходи. - К.: Кондор, 2019. - 272 с.

3.2.20. Логінова Н. І. Правовий захист інформації : навч. посібн. / Н. І. Логінова, Р. Р. Дробожур. - Одеса : Фенікс, 2015. - 264 с.

3.2.21. Організаційно-правові основи захисту службової 0-64 інформації: навч. посіб. /І. П. Касперський, С. 0. Князєв, О. І. Матяш та ін. - Київ : Нац. акад. СБУ, 2017.-120 с.

3.2.22. Організація захисту інформації з обмеженим доступом: навч. посіб. /А.М.Гуз, І.П.Касперський, С.О.Князєв та ін. – К.: Нац. акад., СБУ, 2018. – 252 с

3.2.23. Стандарти захисту персональних даних в соціальній сфері / М. В. Бем., І. М. Городиський. –Львів: б.в., 2018. - 110 с.

3.2.24. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с

3.3. Інформаційні ресурси в інтернеті

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

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

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

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

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

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

- http://www.nau.edu.ua;
- http://www.kzzi.nau.edu.ua.

Також, для навчання використовується:

- https://www.coursera.org/learn/r-programming/;
-http://prometheus.org.ua/dataanalysis/.

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. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ НАБУТИХ СТУДЕНТОМ ЗНАНЬ ТА ВМІНЬ

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

Таблиця 4.1

Вид навчальної роботи	Max кількість балів	
	Денна форма навчання	Заочна форма навчання
№ Семестру	№ 2	№ 3
Модуля № 1 «Безпека і захист даних»		
Види навчальної роботи	Бали	Бали
Практичні заняття	32	30
Для допуску до виконання модульної контрольної роботи №1 студент має набрати не менше	19	
Виконання модульної контрольної роботи №1	18	

УСЬОГО ЗА МОДУЛЕМ №1	50	30
Модуль № 2 «Засоби криптографічного захисту»		
Практичні заняття	32	20
Для допуску до виконання модульної контрольної роботи №2 студент має набрати не менше	19	
Виконання модульної контрольної роботи №2	18	
Виконання контрольної (домашньої роботи) (ЗФН)		20
Підсумкова контрольна робота (ЗФН)		30
УСЬОГО ЗА МОДУЛЕМ №.2	50	70
УСЬОГО ЗА МОДУЛЕМ № 1.2	**100**	**100**
УСЬОГО ЗА ДИСЦИПЛІНОЮ	**100**	**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 модульних контрольних робіт		Виконання та захист домашнього завдання	
9-10	7	18-20	11-12	11-12	Відмінно
8	6	15-17	9-10	9-10	Добре
6-7	4-5	12-14	7-8	7-8	Задовільно
менше 6	менше 4	менше 12	менше 7	менше 7	Незадовільно

4.3. Сума рейтингових оцінок, отриманих студентом за окремі види виконаної навчальної роботи, становить підсумкову модульну рейтингову оцінку.

4.4. Сума підсумкових модульних рейтингових оцінок становить підсумкову семестрову рейтингову оцінку.

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.

Таблиця 4.3

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)

(Ф 03.02 01)

АРКУШ ПОШИРЕННЯ ДОКУМЕНТА

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

(Ф 03.02 – 04)

АРКУШ РЕЄСТРАЦІЇ РЕВІЗІЇ

№ з/п	Прізвище ім'я по-батькові	Дата ревізії	Підпис	Висновок щодо адекватності

(Ф 03.02 – 03)

АРКУШ ОБЛІКУ ЗМІН

№ зміни	Номер 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				