ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних управляючих систем та технологій

«ЗАТВЕРДЖУЮ»
Декан факультету
інформаційних технологій
_____ Ігор ПОВХАН
«___» _____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ

Рівень вищої освіти	**Бакалавр**
Галузь знань	**F Інформаційні технології**
Спеціальність	**F3 Комп'ютерні науки**
Спеціалізація	
Освітня програма	**Інформатика**
Статус дисципліни	**Обов'язкова**
Мова навчання	**Українська**

Ужгород 2025

Робоча програма навчальної дисципліни **«Захист інформації»** для здобувачів вищої освіти галузі знань **F Інформаційні технології** спеціальності **F3 Комп'ютерні науки** освітньої програми **«Інформатика».**

Розробник: Ігор Шапочка, доцент, кандидат фізико-математичних наук, доцент кафедри інформаційних управляючих систем та технологій.

Робочу програму розглянуто та затверджено на засіданні кафедри інформаційних управляючих систем та технологій протокол №11 від 06 червня 2025 р.

Завідувач кафедри _____ Олександр МІЦА

Схвалено науково-методичною комісією факультету інформаційних технологій протокол №10 від 12 червня 2025 р.

ТВО голова науково-методичною комісії _____ Ігор ПОВХАН

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Найменування показників</td><td colspan="2">Розподіл годин за навчальним планом</td></tr>
<tr><td>Денна форма навчання</td><td>Заочна форма навчання</td></tr>
<tr><td rowspan="2">Кількість кредитів – 4</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>4-й</td><td>4-й</td></tr>
<tr><td rowspan="2">Кількість модулів – 2</td><td colspan="2">Семестр:</td></tr>
<tr><td>1-й</td><td>1-й</td></tr>
<tr><td rowspan="4">Тижневих годин:
для денної форми навчання:
аудиторних – 4 год
самостійної роботи студента – 4 год</td><td colspan="2">Лекції:</td></tr>
<tr><td>34 год</td><td>10 год</td></tr>
<tr><td colspan="2">Практичні:</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="2">Вид підсумкового контролю: залік</td><td colspan="2">Лабораторні:</td></tr>
<tr><td>26 год</td><td>6 год</td></tr>
<tr><td rowspan="2">Форма контролю: усне опитування</td><td colspan="2">Самостійна робота:</td></tr>
<tr><td>60 год</td><td>104 год</td></tr>
</table>

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни **«Захист інформації»** є одержання теоретичних знань і практичних навичок щодо методів кодування, шифрування та захисту інформації; ознайомлення з типовими загрозами та методами протидії; опанування принципів проектування, програмування й налаштування засобів контролю захисту в програмних системах та для даних, що в них зберігаються, з метою забезпечення безперебійного й ефективного використання комп'ютерних технологій..

Відповідно до освітньої програми **«Інформатика»** вивчення дисципліни сприяє формуванню у здобувачів вищої освіти спеціальності **F3 Комп'ютерні науки** таких компетентностей: ЗК–1, ЗК–2, ЗК–3, ЗК–6, ЗК–7, ЗК–11, ЗК–12, ФК–1, ФК–14.

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Вивчення навчальної дисципліни «Захист інформації» потребує попередніх знань з предметів «Дискретна математика та теорія алгоритмів», «Алгебра та аналітична геометрія», «Математичний аналіз», «Математичні методи дослідження операцій», «Чисельні методи».

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми **«Інформатика»** вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти спеціальності **F3 Комп'ютерні науки** таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	Шифр ПРН
Застосовувати знання основних форм і законів абстрактно-логічного мислення, основ методології наукового пізнання, форм і методів вилучення, аналізу, обробки та синтезу інформації в предметній області комп'ютерних наук.	ПРН–1
Проектувати, розробляти та аналізувати алгоритми розв'язання обчислювальних та логічних задач, оцінювати ефективність та складність алгоритмів на основі застосування формальних моделей алгоритмів та обчислюваних функцій	ПРН–5
Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.	ПРН–15

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни **«Захист інформації»**:

Очікувані результати навчання з дисципліни	Шифр ПРН
Вміння пояснювати базові поняття та принципи інформаційної безпеки.	ПРН–15
Вміння класифікувати загрози та вразливості інформаційних ресурсів.	ПРН–15
Вміння застосовувати основні методи кодування та шифрування даних.	ПРН–5, ПРН–15
Вміння реалізовувати класичні та сучасні криптографічні алгоритми.	ПРН–5, ПРН–15
Вміння використовувати методи автентифікації та контролю доступу.	ПРН–15
Вміння аналізувати політики безпеки інформаційних систем.	ПРН–1, ПРН–15
Вміння застосовувати засоби забезпечення цілісності та конфіденційності даних.	ПРН–15
Вміння проводити аудит інформаційної безпеки програмних систем.	ПРН–1, ПРН–15
Вміння використовувати програмні інструменти для виявлення загроз і вразливостей.	ПРН–15
Вміння оцінювати ризики порушення інформаційної безпеки.	ПРН–5, ПРН–15

Вміння проектувати програмні системи з урахуванням вимог безпеки.	ПРН–15
Вміння реалізовувати механізми захисту інформації у базах даних.	ПРН–5, ПРН–15
Вміння забезпечувати безпеку під час передачі інформації мережею.	ПРН–15
Вміння налаштовувати засоби контролю доступу до програмних ресурсів.	ПРН–15
Вміння документувати заходи та процедури інформаційної безпеки.	ПРН–1, ПРН–15
Вміння аналізувати та реагувати на інциденти інформаційної безпеки.	ПРН–15
Вміння застосовувати стандарти та нормативні вимоги у сфері захисту інформації.	ПРН–1, ПРН–15
Вміння інтегрувати засоби захисту у процеси програмування та тестування.	ПРН–5, ПРН–15
Вміння розробляти рекомендації щодо удосконалення систем захисту даних.	ПРН–1, ПРН–15
Вміння працювати з командою над впровадженням комплексних заходів безпеки.	ПРН–15
Вміння застосовувати принципи «безпечного програмування» у власних проєктах.	ПРН–5, ПРН–15
Вміння оцінювати ефективність використаних методів та засобів захисту.	ПРН–1, ПРН–15

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Засоби оцінювання та методи демонстрування результатів навчання

Засобами оцінювання та методами демонстрування результатів навчання з навчальної дисципліни є:

- усні та письмові опитування на лабораторних заняттях;
- перевірка виконаних завдань для самостійної роботи;
- тести для перевірки теоретичних знань на сайті електронного навчання ДВНЗ «УжНУ»;
- 8 лабораторних робіт;
- 2 модульні контрольних оцінювання, які включають розв’язування комплексних задач із захисту даних і програмних систем;
- підсумковий семестровий залік.

Форми контролю та критерії оцінювання результатів навчання

Форми поточного контролю: вибіркове усне опитування перед початком розв’язування завдань під час лабораторних занять; фронтальна перевірка виконання завдань для самостійної роботи; оцінка активності студента у процесі занять, внесених пропозицій, оригінальних рішень, уточнень і визначень, доповнень попередніх відповідей і т. ін.; письмова (до 15 хв.) контрольна робота, що має одне тематичне завдання; тестування на сайті електронного навчання ДВНЗ «Ужгородський національний університет» в курсі «Захист інформації».

Форма модульного контролю: тести у електронному середовищі Moodle, кожен з яких складається з 20-ти питань.

Форма підсумкового семестрового контролю: усне опитування студента за випадково вибраним білетом, що містить одне теоретичне і одне практичне завдання.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне оцінювання та самостійна робота											Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	Т10	Т11	40	**100**
5	6	5	6	5	6	5	6	5	6	5		

Т1, Т2, Т3, …, Т11 – теми

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне оцінювання та самостійна робота								Модульна контрольна робота	Сума
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	40	**100**
7	8	8	8	8	7	7	7		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторна заняття (усні та письмові опитування на лабораторних заняттях)	6	24	6	24
Лабораторні роботи	4	36	4	36
Модульна контрольна робота	1	40	1	40
Разом		**100**		**100**

Критерії оцінювання модульної контрольної роботи

Протягом семестру проводяться два підсумкові модульні контролі, зміст яких відповідає змістовним модулям. Максимальна кількість балів при оцінюванні кожного модульного контролю становить 40 балів. Модульна контрольна робота складається з двадцяти типових тематичних завдань. Максимальна оцінка за правильне розв’язання кожного завдання складає 2 бали (0 або 2 бали) і виставляється згідно критеріїв викладених у таблиці 1.

Таблиця 1

Зміст завдання	Бали
Отримано правильну відповідь.	2
Учасник не приступив до розв’язування завдання або вказав неправильну відповідь	0

Критерії оцінювання підсумкового семестрового контролю

Підсумковий залік представляє собою усне опитування студента за випадково вибраним заліковим білетом. Кожен заліковий білет складається з одного теоретичного питань і одного стандартизованого (типового) практичного завдання Орієнтований перелік питань до заліку:

1. Основні принципи інформаційної безпеки.
2. Класифікація загроз інформаційним системам.
3. Моделі порушників та методи оцінки ризиків.
4. Структура та функції політики безпеки.
5. Методи організаційного й технічного захисту інформації.
6. Особливості симетричних алгоритмів шифрування (приклади).
7. Особливості асиметричних алгоритмів шифрування (приклади).
8. Властивості хеш-функцій.

9. Призначення електронного цифрового підпису.
10. Протоколи обміну ключами та їх безпека.
11. Методи автентифікації користувачів.
12. Моделі контролю доступу (DAC, MAC, RBAC).
13. Захист інформації під час передавання мережею.
14. Основні функції Firewall.
15. IDS/IPS системи: призначення та відмінності.
16. Типові атаки на комп'ютерні мережі (DoS, MITM).
17. Основи криптоаналізу та його завдання.
18. Стандарти ISO/IEC 27001 у сфері інформаційної безпеки.
19. Законодавча та нормативна база України щодо захисту інформації.
20. Сучасні тенденції в галузі інформаційної безпеки (хмари, стеганографія).

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка ECTS	Залікова оцінка за національною шкалою
90–100	**A**	*Зараховано*
82–89	**B**	
74–81	**C**	
64–73	**D**	
60–63	**E**	
35–59	**FX**	*Незараховано з можливістю повторного складання*
0–34	**F**	*Незараховано з обов'язковим повторним вивченням дисципліни*

— **«A»** (90 та вище балів) заслуговує студент, який виявив всебічне і глибоке знання програмового матеріалу, вміння вільно виконувати завдання, передбачені програмою, засвоїв основну і ознайомився з додатковою літературою, розуміє взаємозв'язок головних понять дисципліни та їх значення для майбутньої професії;
— **«B»** (82–89 балів) заслуговує студент, який виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисциплін і здатний до самостійного доповнення, але під час відповіді допустив деякі неточності;
— **«C»** (74–81 балів) заслуговує студент, що виявив не цілком повне знання програмного матеріалу, не завжди успішно виконує передбачені програмою завдання, частково засвоїв основну літературу, рекомендовану програмою, виявив не систематичний характер знань з дисциплін і не завжди здатний до їх самостійного доповнення і під час відповіді допускає деякі неточності;
— **«D»** (64–73 балів) заслуговує студент, що виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою. Як правило, оцінка "D" виставляється студентам, що допустили помилки у відповіді на заліку та при виконанні залікових завдань, але які володіють необхідними знаннями для їх усунення за допомогою викладача;

— **«E»** (60–63 балів) заслуговує студент, що виявив часткове знання основного програмового матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою. Як правило, оцінка "E" виставляється студентам, що допустили грубі помилки у відповіді на заліку та при виконанні залікових завдань, але які частково володіють необхідними знаннями для їх усунення за допомогою викладача.
— **«FX»** (35–59 балів) виставляється студенту, який виявив суттєві прогалини в знаннях основного програмового матеріалу, допустив принципові помилки у виконанні передбачених програмою завдань.
— **«F»** (0–34 балів) виставляється студенту коли протягом семестру він допустив грубі помилки у виконанні передбачених програмою завдань.

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1. Теоретичні основи та базові методи захисту.

Тема 1. Вступ до інформаційної безпеки.

Поняття інформації та її властивостей. Основні принципи захисту (CIA-тріада). Історія розвитку криптографії та інформаційної безпеки. Поняття «інформаційна загроза», «вразливість», «ризик». Роль інформаційної безпеки у сучасному IT-середовищі. Приклади порушень безпеки в реальних системах.

Тема 2. Загрози інформаційній безпеці та їх класифікація.

Класифікація загроз: природні, техногенні, антропогенні. Зовнішні та внутрішні загрози. Моделі атак і порушників. Класифікація шкідливого ПЗ. Методи оцінки ризиків (кількісні, якісні). Приклади сучасних кіберзагроз.

Тема 3. Політика безпеки.

Поняття політики безпеки. Рівні політики (корпоративна, локальна). Структура та основні розділи політики. Управління доступом і аудит. Контроль виконання політики. Приклади політик у відомих компаніях.

Тема 4. Основи криптографії.

Поняття шифрування та дешифрування. Симетричні алгоритми (DES, AES). Асиметричні алгоритми (RSA, ElGamal). Блокові та потокові шифри. Управління ключами. Вступ до криптоаналізу.

Тема 5. Хеш-функції та цифровий підпис.

Поняття хеш-функції, основні властивості. Алгоритми MD5, SHA-1, SHA-2. Поняття електронного цифрового підпису. Протоколи підпису та перевірки достовірності. Використання ЕЦП у практиці. Приклади уразливостей хеш-функцій.

Модуль 2. Прикладні аспекти та сучасні технології захисту.

Тема 1. Криптографічні протоколи.

Криптографічні протоколи та їх роль. Протокол Діффі-Хеллмана. Ідентифікація та автентифікація користувачів. Схеми цифрового підпису (Ель-Гамаля, Шнорра). SSL/TLS як приклад сучасного протоколу. Напади на криптографічні протоколи..

Тема 2. Захист інформації в комп'ютерних системах.

Основи управління доступом. Моделі DAC, MAC, RBAC. Методи автентифікації (паролі, біометрія, токени). Системи управління ключами. Моніторинг подій безпеки. Аналіз інцидентів.

Тема 3. Захист інформації в комп'ютерних мережах.

Атаки на комп’ютерні мережі (DoS, MITM, Sniffing). Засоби захисту від атак. Протоколи SSL/TLS, HTTPS, SSH. VPN-технології. Захист бездротових мереж. Методи аналізу мережевого трафіку.

Тема 4. Комплексні системи інформаційної безпеки.

Архітектура комплексної системи захисту. Firewall: функції та налаштування. IDS/IPS системи. Засоби SIEM. Аудит і моніторинг. Приклади впровадження комплексних рішень.

Тема 5. Стандарти та нормативно-правова база.

Законодавство України про захист інформації. ДСТУ у сфері інформаційної безпеки. Міжнародні стандарти ISO/IEC 27001. Аудит інформаційної безпеки. Організаційні та правові заходи. Приклади впровадження стандартів.

Тема 6. Актуальні тенденції інформаційної безпеки.

Хмарні технології та безпека. Віртуалізація та контейнеризація. Стеганографія. Квантова криптографія. Інтернет речей і проблеми безпеки.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
2-й семестр						
Модуль 1						
Тема 1. Вступ до інформаційної безпеки.	10	2		2		6
Тема 2. Загрози інформаційній безпеці та їх класифікація.	10	2		2		6
Тема 3. Політика безпеки.	10	2		2		6
Тема 4. Основи криптографії.	16	6		4		6
Тема 5. Хеш-функції та цифровий підпис.	12	4		2		6
Разом за модуль	58	16		12		30
Модуль 2						
Тема 1. Криптографічні протоколи.	11	4		2		5
Тема 2. Захист інформації в комп’ютерних системах.	13	4		4		5
Тема 3. Захист інформації в комп’ютерних мережах.	11	4		2		5
Тема 4. Комплексні системи інформаційної безпеки.	9	2		2		5
Тема 5. Стандарти та нормативно-правова база.	9	2		2		5
Тема 6. Актуальні тенденції інформаційної безпеки.	9	2		2		5
Разом за модуль	62	18		14		30
Разом за семестр	**120**	**34**		**26**		**60**

Назви змістових модулів і тем	Кількість годин					
	Заочна форма					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
2-й семестр						
Модуль 1						
Тема 1. Вступ до інформаційної безпеки.	10	1				9
Тема 2. Загрози інформаційній безпеці та їх класифікація.	10	1				9
Тема 3. Політика безпеки.	11	1		1		9
Тема 4. Основи криптографії.	12	1		1		10
Тема 5. Хеш-функції та цифровий підпис.	12	1		1		10
Разом за модуль	55	5		3		47
Модуль 2						
Тема 1. Криптографічні протоколи.	12	1		1		10
Тема 2. Захист інформації в комп'ютерних системах.	11	1		1		9
Тема 3. Захист інформації в комп'ютерних мережах.	12	1		1		10
Тема 4. Комплексні системи інформаційної безпеки.	10	1				9
Тема 5. Стандарти та нормативно-правова база.	10	0,5				9,5
Тема 6. Актуальні тенденції інформаційної безпеки.	10	0,5				9,5
Разом за модуль	65	5		3		57
Разом за семестр	**120**	**10**		**6**		**104**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1.	Базові інструменти ІБ	2	0.75
2.	Модель загроз і оцінка ризиків	4	0.75
3.	Симетричне шифрування	4	0.75
4.	Асиметричне шифрування та PKI	2	0.75
5.	Криптографічні протоколи	4	0.75
6.	Контроль доступу та автентифікація	4	0.75

7.	Аналіз мережевого трафіку та виявлення атак	4	0.75
8.	Мережеві контролі: Firewall/WAF/IDS	2	0.75
	Разом	**26**	**6**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин	
		денна	заочна
1.	Вступ до інформаційної безпеки.	6	9
2.	Загрози інформаційній безпеці та їх класифікація.	6	9
3.	Політика безпеки.	6	9
4.	Основи криптографії.	6	10
5.	Хеш-функції та цифровий підпис.	6	10
6.	Криптографічні протоколи.	5	10
7.	Захист інформації в комп’ютерних системах.	5	9
8.	Захист інформації в комп’ютерних мережах.	5	10
9.	Комплексні системи інформаційної безпеки.	5	9
10.	Стандарти та нормативно-правова база.	5	9,5
11.	Актуальні тенденції інформаційної безпеки	5	9,5
	Разом	**60**	**104**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

- Технічні засоби: комп'ютер та проектор для демонстрації презентацій лекцій (в аудиторії), мережа Інтернет.
- Програмне забезпечення: браузер (веб переглядач), Acrobat Reader, Google Meet, Figma (для онлайн лекцій, практичних занять, консультацій), мова та середовище: Python 3.x (+ пакети cryptography/pycryptodome, Jupyter); криптографічні інструменти: OpenSSL, GnuPG.

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

Основна література

1. Міца О. В., Голомб Р. М. Методи захисту інформації: методичні вказівки до курсу для студентів спеціальності 122 «Комп'ютерні науки». Ужгород: ДВНЗ «УжНУ», 2020. 64 с.
2. Остапов С. Е., Євсеєв С. П., Король О. Г. Технології захисту інформації: навчальний посібник. Харків: Вид. ХНЕУ, 2013. 476 с. URL: https://repository.hneu.edu.ua/handle/123456789/22547?utm_source=chatgpt.com
3. Тарнавський Ю. А. Технології захисту інформації: підручник. Київ: КПІ ім. Ігоря Сікорського, 2018. 162 с.

Допоміжна література

1. Baignères T., Junod P., Lu Yi, Monnerat J., Vaudenay S. The Classical Introduction to Cryptography: Exercise Book. Springer, 2006. 288 p.
2. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2020. 784 p. URL: https://mrce.in/ebooks/Cryptography%20&%20Network%20Security%208th%20Ed.pdf
3. Stinson D. R., Paterson M. B. Cryptography: Theory and Practice. 4th ed. Boca Raton: CRC Press, Taylor & Francis Group, 2018. 603 p.
4. Шапочка І.В., Жуковський С.С., Міца О.В., Шапочка А.І. Деякі аспекти порівняння швидкодій різних криптоалгоритмів. Науковий пошук молодих дослідників: збірник наукових праць студентів, магістрантів та викладачів / за заг. ред. Постової Світлани, Вербівського Дмитрія, Карплюк Сваїтлани, Єремеєвої Віри. Житомир : Вид-во ЖДУ ім. І. Франка, 2025. С. 163-164.

Інформаційні ресурси в мережі Інтернет

1. https://moodle.uzhnu.edu.ua/course/view.php?id=25 — сторінка курсу на сайті електронного навчання ДВНЗ «Ужгородський національний університет».
2. http://www.nbuv.gov.ua — Національна бібліотека України імені В. І. Вернадського.

Результати перегляду
робочої програми навчальної дисципліни

Робоча програма перезатверджена на 20___ / 20___ н. р. без змін; зі змінами (Додаток ____).
(потрібне підкреслити)

Протокол № ___ від «____»__________ 20___ р. Завідувач кафедри ______________________
(підпис) (Ім’я ПРІЗВИЩЕ)

Робоча програма перезатверджена на 20___ / 20___ н. р. без змін; зі змінами (Додаток ____).
(потрібне підкреслити)

Протокол № ___ від «____»__________ 20___ р. Завідувач кафедри ______________________
(підпис) (Ім’я ПРІЗВИЩЕ)

Робоча програма перезатверджена на 20___ / 20___ н. р. без змін; зі змінами (Додаток ____).
(потрібне підкреслити)

Протокол № ___ від «____»__________ 20___ р. Завідувач кафедри ______________________
(підпис) (Ім’я ПРІЗВИЩЕ)

Робоча програма перезатверджена на 20___ / 20___ н. р. без змін; зі змінами (Додаток ____).
(потрібне підкреслити)

Протокол № ___ від «____»__________ 20___ р. Завідувач кафедри ______________________
(підпис) (Ім’я ПРІЗВИЩЕ)