Черкаський державний технологічний університет
Факультет інформаційних технологій і систем

	«ЗАТВЕРДЖУЮ» Голова вченої ради факультету _____ _____ / _____ Протокол № 5 «17» лютого 2020

СИЛАБУС

навчальної дисципліни

«Безпека та захист програм і даних»

Шифр за ОПП – ВППБ5

Освітній рівень -	бакалаврський
Галузь знань -	12 – інформаційні технології
Спеціальність -	126 – інформаційні системи та технології
Освітня програма -	«Web-технології, Web-дизайн»

2019 - 2020 навчальний рік

Силабус навчальної дисципліни «Безпека та захист програм і даних»
(назва навчальної дисципліни)
підготовки здобувачів освітнього ступеня «бакалавр» за спеціальністю 126 – Інформаційні системи та технології, освітня програма «Web-технології , Web-дизайн» - 12 стор.

Силабус складений на основі програми навчальної дисципліни «Безпека та захист програм і даних», шифр (за ОПП) – ВППБ5.

Розробник силабусу:
Рудницький Сергій Володимирович, к.т.н., старший викладач кафедри ІТП
(ПІБ, наук.ст., вчене зв., посада НПП кафедри, що розробив силабус)

Силабус затверджений на засіданні кафедри інформаційних технологій проектування

Протокол № 8 від "10" січня 2020 року

Обговорено та рекомендовано до затвердження методичною комісією факультету інформаційних технологій і систем

«14» лютого 2020 р., протокол № 4

Голова методичної комісії
факультету інформаційних технологій і систем _____ /А.Р. Карапетян/
підпис *ПІБ*

1. ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

Прізвище, ім'я, по батькові	Рудницький Сергій Володимирович
Науковий ступінь	к.т.н.
Наукове звання	-
Посада	старший викладач
Місце роботи	Черкаський державний технологічний університет
Адреса кафедри	18006, м. Черкаси, бул. Шевченка 460, каб. 603-1 корпус

Контактний телефон	(0472)51-15-86
Профайл викладача	https://chdtu.edu.ua/fitis/kitp/staff/item/1171-rudnytskyi-serhii-volodymyrovych
e-mail:	s.v.rudnitskiy@gmail.com
Профайл дисципліни	http://fitis.moodle.chdtu.edu.ua/course/view.php?id=571
Розклад консультацій	

2. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

<table>
<tr><td rowspan="2">Галузь знань, спеціальність, освітня програма, освітній рівень</td><td colspan="2" rowspan="2">Загальні характеристики</td><td colspan="2">Навчальне навантаження з дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td rowspan="2"><u>Галузь знань</u>
12 – інформаційні технології</td><td colspan="2" rowspan="2">Вибіркова</td><td>Курс підготовки:</td><td></td></tr>
<tr><td>3-й</td><td></td></tr>
<tr><td rowspan="4"><u>Спеціальність</u>

126 – інформаційні системи та технології</td><td>Загальна кількість кредитів ЄКТС</td><td>4</td><td colspan="2">Семестр підготовки:</td></tr>
<tr><td>Загальна кількість годин</td><td>120</td><td>6-й</td><td></td></tr>
<tr><td rowspan="4"><u>Освітня програма</u>

«Web-технології, Web-дизайн»</td><td rowspan="2">Кількість аудиторних годин</td><td rowspan="2">54</td><td colspan="2">Лекції</td></tr>
<tr><td>18 год.</td><td></td></tr>
<tr><td rowspan="2">Кількість годин самостійної роботи</td><td rowspan="2">66</td><td colspan="2">Практичні, семінарські</td></tr>
<tr><td></td><td></td></tr>
<tr><td rowspan="8"><u>Освітній рівень</u>

бакалаврський</td><td colspan="2" rowspan="8">Мова навчання - українська</td><td colspan="2">Лабораторні</td></tr>
<tr><td>36 год.</td><td></td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>66 год</td><td></td></tr>
<tr><td colspan="2">Форма підсумкового контролю</td></tr>
<tr><td>Залік</td><td></td></tr>
</table>

3. МЕТА І ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета викладання дисципліни	Оволодіння студентами комплексом знань у галузі захисту інформації, системами й методами визначення захищеності програмних продуктів, пристроїв; комп'ютерних мереж, їх складових та набуття на основі цих знань практичних навичок та теоретичних знань, необхідних для творчого підходу в питанні сучасного та майбутнього оперативного захисту програм та даних.

Завдання вивчення дисципліни	Ознайомити студентів із законодавчим, адміністративним, організаційним і інженерно-технічним рівнями забезпечення інформаційної безпеки, особливостями криптографічного і стеганографічного захисту інформації, навчити їх реалізовувати практично захищені програми та комп'ютерні системи.

4. РЕЗУЛЬТАТИ НАВЧАННЯ

№ з/п	Результати навчання
1	Здатність визначати загрози безпеці програм і даних.
2	Здатність застосовувати положення правових актів для забезпечення інформаційної безпеки.
3	Вміти організовувати безпечну роботу в Internet.
4	Вміти проектувати і класифікувати захищені комп'ютерні системи.

5. ПРЕРЕКВІЗИТИ

«Бази даних та знань», «Проектування інформаційних систем».

6. ПОСТРЕКВІЗИТИ

«Професійний практикум».

7. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1 *Основні поняття теорії побудови системи безпеки комп'ютерних систем та мереж.*
1.1. Проблема захисту інформації в КСМ (комп'ютерні системи та мережі). 1.2. Периметр відповідальності засобів захисту інформації (ЗЗІ) в залежності від типу КС (комп'ютерної системи). 1.3. Класифікація учасників КС. 1.4. Класифікація вторгнень. 1.5. Канали витоку інформації. Основні напрямки захисту інформації в КС. 1.6. Базові моделі побудови ЗЗІ. 1.7. Модель моніторингу безпеки КС. 1.8. Алгоритм найбільших статистичних аномалій.
Тема 2 *Ідентифікація, Автентикація, Права розмежування доступу в КСС.*
2.1. Прості паролі. Оцінка стійкості пароля. Модифікація механізму простих паролів. Список паролів. Механізм "рукостискань". 2.2. Багатофакторна автентикація (Multiway authentication). 2.3. Біометрична автентикація. Рекомендації по вибору механізмів автентикації. 2.4. Засоби розділення доступу в КСС. 2.5. СРД – Системи розділення доступу. Операційний журнал. 2.6. Мандатні списки та списки доступу. Механізм замків та ключів.
Тема 3 *Криптографічні моделі.*

3.1. Основні визначення в області криптографії. 3.2. Класифікація криптографічних систем. Шифр Цезаря. Шифр Шенона. Люцифер. 3.3. Криптоалгоритм DES (Схема. Особливості шифрування по алгоритму DES. Модифікації алгоритму DES). 3.4. Цифровий підпис (Digital signature). AES. ГОСТ 28147-89. ANUBIS. 3.5. Асиметричні криптосистеми. RSA. Al-gamal. 3.6. Сьогодення. Потокові криптосистеми. Алгоритм B-Crypt.
Тема 4 *Протоколи автентикації.*
4.1. Класифікація протоколів автентикації в КСС. 4.2. Протоколи автентикації суб'єктів на основі симетричних криптосистем. 4.3. Протоколи автентикації суб'єктів на основі асиметричних криптосистем. 4.4. Протокол автентикації повідомлень на основі симетричних криптосистем. 4.5. Загальна схема. Пртоколи автентикації повідомлень на основі асиметричних криптосистем. 4.6. Протокол відкритих угод. 4.7. Оцінка пропускної здатності мереж, в яких реалізуються протоколи автентикації. 4.8. Структура електронної платіжної системи.
Тема 5 *Проектування і класифікація захищених комп'ютерних систем.*
5.1. Два підходи до проектування засобів захисту. 5.2. Класифікація КС по рівню захищеності.

8. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ теми	Назва модулів і тем	Форми організації навчання, кількість годин						Література, інформаційні ресурси
		Денна форма			Заочна форма			
		Лекції	Практичні, лабораторні роботи	Самостійна робота	Лекції	Практичні, лабораторні роботи	Самостійна робота	
Змістовий модуль №1. *Основи об`єктно-орієнтоване програмування мовою Java.*								
1	**Тема 1.** Основні поняття теорії побудови системи безпеки комп'ютерних систем та мереж.	2	4	12	-	-	-	4, 8, 11
2	**Тема 2.** Ідентифікація, Автентикація, Права розмежування доступу в КСС.	4	8	14	-	-	-	1, 3
3	**Тема 3.** Криптографічні моделі.	2	8	14	-	-	-	5, 9
4	**Тема 4.** Протоколи автентикації.	6	8	12	-	-	-	11, 12
5	**Тема 5.** Проектування і класифікація захищених комп'ютерних систем.	4	8	14	-	-	-	7, 14
	Разом	18	36	66	-	-	-	

9. ПРАКТИЧНІ / СЕМІНАРСЬКІ ЗАНЯТТЯ, ЛАБОРАТОРНІ РОБОТИ

№ з/п	Назва лабораторної роботи	Кількість годин	
		Денна	Заочна
1	Симетричні алгоритми шифрування даних	6	-

4	Захист програм від несанкціонованої експлуатації за рахунок прив'язки до носія інформації	4	-
4	Програмування змін характеристик файлу	4	-
6	Захист програмного забезпечення від несанкціонованого використання та копіювання	5	-
4	Алгоритми поведінки вірусних та інших шкідливих (зловмисних) програм	5	-
4	Алгоритми попередження і виявлення вірусних загроз	4	
4	Аналіз та дослідження сучасних засобів захисту програмного забезпечення	4	
6	Реалізація міжмережного екрану та сніффера	4	
4			

МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

Методичні рекомендації до виконання лабораторних робіт з дисципліни «Безпека та захист програм і даних» для здобувачів освітнього ступеня бакалавр спеціальності № 126 «Інформаційні системи та технології» (освітня програма «Web-технології, web-дизайн») для денної форми навчання / Укл. Бабенко В.Г., Лада Н.В., Рудницький С.В. – Черкаси

10. САМОСТІЙНА РОБОТА

Поглиблене опрацювання розглянутих на лекціях та розгляд суміжних тем.

№ з/п	Назва теми	Кількість годин	
		Денна	Заочна
1	Сервіси і механізми захисту	4	-
2	Принципи побудови блочних шифрів та криптосистем з відкритим ключем	8	-
3	Сучасні алгоритми симетричного та асиметричного шифрування	6	-
4	Сучасні алгоритми хешування	8	-
5	Основні методи безпечного написання коду програм	8	-
6	Методи і засоби аналізу безпеки програмних засобів	6	-
7	Використовувати функції Microsoft CryptoAPI для розробки прикладного ПЗ	6	-
8	Оцінка та аналіз безпеки ПЗ	4	-
9	Протоколи автентифікації	6	
10	Програмна реалізація криптографічних алгоритмів	6	
11	Методи безпечної реалізації ПЗ	4	
Разом		66	-

11. СИСТЕМА ОЦІНЮВАННЯ НАВЧАЛЬНИХ ДОСЯГНЕНЬ

11.1 МЕТОДИ КОНТРОЛЮ

В організації навчального процесу застосовуються контрольні заходи у формі вхідного, поточного, модульного, рейтингового і підсумкового контролю.

Вхідний контроль проводиться перед вивченням нового курсу з метою визначення рівня підготовки здобувачів вищої освіти з дисциплін, які забезпечують цей курс. За результатами вхідного контролю розробляються заходи з надання індивідуальної допомоги здобувачам вищої освіти, коригування навчального процесу з відповідного курсу.

Поточний контроль здійснюється під час проведення лекцій та лабораторних занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретних видів навчальної діяльності.

Модульний контроль успішності здобувачів вищої освіти здійснюється для перевірки рівня засвоєння навчального матеріалу в кінці кожного навчального модуля.

Рейтинговий контроль є інструментом комплексного оцінювання якості навчальної роботи здобувача вищої освіти з усіх кредитних модулів на певному етапі навчання. Рейтинговий контроль успішності здобувачів вищої освіти проводиться на 8-9 навчальних тижнях.

Семестровий контроль з дисципліни проводиться відповідно до навчального плану у вигляді заліку в терміни, встановлені графіком навчального процесу, та в обсязі навчального матеріалу, визначеному робочою програмою дисципліни.

Залік – це вид підсумкового контролю, за якого засвоєння здобувачем вищої освіти навчального матеріалу з дисципліни оцінюється на підставі результатів поточного, проміжного контролів (тестування, поточного опитування, виконання індивідуальних завдань та певних видів робіт на лабораторних заняттях) протягом семестру і модульного контролю.

Іспити - це підсумковий етап вивчення усієї дисципліни з метою перевірки знань студентів по теорії і виявлення навичок застосування отриманих знань при вирішенні практичних завдань, а також навиків самостійної роботи з навчальною і науковою літературою.

Іспит дає можливість кожному студенту у порівняно короткий проміжок часу осмислити весь пройдений курс у цілому, сконцентрувати увагу на вузлових його моментах, закріпити у пам'яті його основний зміст.

Оцінка навчальних досягнень здобувачів вищої освіти за всіма видами контролю здійснюється за національною системою та ECTS:

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	

60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

11.2 ПИТАННЯ ДО ЗАЛІКУ

1. Чому криптографічні алгоритми, що вимагають збереження в таємниці послідовності перетворення даних, не знаходять нині широкого застосування?
2. Яким має бути об'єм ключового простору для забезпечення криптографічної стійкості алгоритму?
3. Чи залежить криптографічна стійкість алгоритму від набору можливих символів ключа?
4. Що таке ключ?
5. Чи можна використати послідовності цифр фундаментальних констант при формуванні гами?
6. Назвіть основні показники криптостійкості.
7. Охарактеризуйте заходи по захисту ключів.
8. Виходячи з чого визначається необхідність зміни ключів шифрування?
9. Які способи захисту від несанкціонованого копіювання програм Ви знаєте?
10. Охарактеризуйте спосіб захисту, що ґрунтується на використанні міток носія інформації.
11. Охарактеризуйте спосіб захисту, що ґрунтується на фізичних дефектах носія інформації.
12. Охарактеризуйте спосіб захисту, що ґрунтується на тимчасових характеристиках читання носія інформації.
13. Як грамотно з точки зору захисту від злому представляти в початковому тексті програми шаблони для порівняння строкових змінних?
14. Як організувати процедури, що виконують одні і ті ж дії, але що мають різну «операторну начинку»?
15. Чи можна зберігати значення серійного номера пристрою, що перевіряється, не в тілі програми, а в окремому файлі?
16. Чи доцільно виділяти процедури, що здійснюють дії по захисту, в окремі динамічні бібліотеки?
17. Як коректно іменувати процедури, які здійснюють захисні механізми?
18. Які способи розповсюдження програмних продуктів ви знаєте?

19. Файлам якого формату віддають перевагу для зберігання лічильника запусків програми?
20. У якому вигляді краще зберігати дату та час?
21. Як організувати в тілі програми додаткові перевірки?
22. Що розуміють під незадокументованими точками входу в програму?
23. Сформулюйте рекомендації для забезпечення тестових перевірок роботи додатку у випадку використання захисту, який базується на використанні лічильника запусків програми.
24. Як раціонально організувати ведення протоколу при захисті, що базується на підрахунку кількості запусків програми?
25. Як протистояти використанню налагоджувачів при спробі злому програми?
26. Що собою являє захист від несанкціонованого використання та копіювання?
27. Які технології захисту від НСК та НСВ відомі на сьогоднішній день?
28. Наведіть короткий опис технології захисту від НСК – створення особливо обумовлених носіїв;
29. Назвіть, будь ласка, групи систем захисту від несанкціонованого використання та копіювання.
30. Які існують методи захисту програмного забезпечення, шляхом прив’язки до параметрів комп’ютера?
31. Що відносять до шкідливого програмного забезпечення і як його класифікують?
32. Класифікуйте комп’ютерні віруси за середовищем їх існування та за способом зараження комп’ютерів.
33. Наведіть класифікацію вірусів за алгоритмами, які вони використовують при функціонуванні, та за своїми деструктивними можли-вос¬тями.
34. Наведіть алгоритм роботи файлових вірусів.
35. В чому полягає принцип дії завантажувального вірусу?
36. Наведіть алгоритм роботи завантажувального вірусу: резидентного і нерезидентного.
37. Дайте загальну характеристику макро-вірусам, їх особливостям та розташуванню.
38. В чому особливості мережевих вірусів?
39. Охарактеризуйте стелс-віруси. Які різновиди цих вірусів ви знаєте?
40. Для чого існують і як функціонують конструктори вірусів та поліморфік-генератори?
41. Які існують методи і засоби для захисту від комп’ютерних вірусів?
42. За якими ознаками можна виявити факт зараження комп'ютерним вірусом?
43. Які заходи рекомендується вживати, щоб запобігти зараженню комп'ютерним вірусом?
44. Що таке антивірусна програма? Які типи антивірусів ви знаєте?
45. Охарактеризуйте різновиди антивірусних програм.
46. Які правила треба знати та виконувати, щоб не наражати свій комп'ютер на небезпеку зараження комп'ютерними вірусами?

47. Що треба робити, якщо ви виявили зараження комп'ютера вірусом?
48. Що таке антивірус?
49. Наведіть, будь ласка, класифікацію антивірусних програм.
50. Наведіть приклади антивірусів. Коротко охарактеризуйте їх.
51. Які основні функції антивірусів ви знаєте?
52. Чи можна заразити вірусом простий текстовий файл, що має розширення txt?
53. Вкажіть основні функції антивірусу Касперського.
54. Проведіть порівняльний аналіз антивірусного ПЗ Panda Antivirus та Norton AntiVirus вказуючи на їх переваги та недоліки.
55. Які є методи контролю трафіку між локальної та зовнішньою мережею?
56. Яким чином може здійснюватися перехоплення трафіку?
57. Які є принципи дії брандмауера?
58. Що дозволяє виявити аналіз трафіку, який пройшов через сніффер?
59. За допомогою яких засобів можна знизити погрозу сніффингу пакетів?

11.3 КРИТЕРІЇ ОЦІНЮВАННЯ

ДЕННА ФОРМА

Для студентів денної форми навчання	
Вид навчальної роботи	Кількість балів *максимум*
Постійна частина	
ЗМІСТОВИЙ МОДУЛЬ №1 120 годин	
Захист лабораторної роботи № 1 Захист лабораторної роботи № 2 Захист лабораторної роботи № 3 Захист лабораторної роботи № 4 Захист лабораторної роботи № 5 Модульна контрольна робота № 1	5 5 10 10 10 20
Всього за змістовим модулем № 1	20
Додаткова частина	
Підготовка та захист реферату за індивідуальною темою	20
Участь у Днях студентської науки	20
Участь у науковій конференції чи семінарі за темою дисципліни	20
Оформлення наочного стенда за індивідуальною темою	20
Штрафна частина	
Пропуск одного заняття без поважної причини	-5
Несвоєчасний захист звіту з лабораторної роботи	-5
ІСПИТ	30
ПІДСУМКОВА СЕМЕСТРОВА ОЦІНКА	**100**

12. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1.Куприянов А.И. Основы защиты информации: учеб. пособие для студ. высш. учеб. заведений / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов.— М.: Издательский центр «Академия», 2006.— 256 с. – 3 екз.

2. Цирлов В.Л. Основы информационной безопасности автоматизированых систем. Краткий курс,— М.: Феникс, 2008.— 174 с. – 3 екз.

3. Белов Е.Б. и др. Основы информационной безопасности. Учебное пособие для вузов,— М.: Горячая линия-Телеком, 2006.— 544 с. – 3 екз.

4. Бармен, Скотт. Разработка правил информационной безопасности.: Пер. с англ.— М.: Издательский дом «Вильяме», 2002.— 208 с. – 3 екз.

5. Домарев В.В. Безопасность информационных технологий. Системный подход.- К.: ООО «ТИД «ДС», 2004.- 992 с. – 3 екз.

6. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия.— СПб.: БХВ-Петербург, 2003.— 752 с. – 3 екз.

7. Лужецький В.А., Войтович О.П., Кожухівський А.Д. Основи інформаційної безпеки. Посібник,— Черкаси: ЧДТУ, 2008.— 243 с. – 3 екз.

8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов.— М.: Горячая линия-Телеком, 2004.— 280 с. – 3 екз.

9. Про інформацію. Закон України від 2 жовтня 1992 р. № 2657–XII. –7 экз.

10. Про науково-технічну інформацію. Закон України від 25 червня 1993 р. № 3322–XII., - 7 экз.

11. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 5 липня 1994 р. № 80/94–ВР. В редакції від 31 травня 2005 р. – 3 екз.

12. Про електронний цифровий підпис. Закон України. Відомості Верховної Ради, 2003, № 36, ст.. 276. (Із змінами, внесеними згідно із Законом № 879–V I від 15.01.2009). – 3 екз.

13. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с. – 62 екз.

14. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – К.: Корнійчук, 2000. – 152 с.. – 100 екз.

15. Крижанівський В.Б. Безпека інформаційних систем. – Житомир: ЖДТУ, 2009. – 81 с.– 15 екз.

13. ІНФОРМАЦІЙНІ РЕСУРСИ

1. http://www.nbuv.gov.ua/node/208
2. http://jrnl.nau.edu.ua/index.php/ZI/article/view/3504
3. https://er.nau.edu.ua/handle/NAU/32583/

14. ПЕРЕЛІК НОРМАТИВНИХ ДОКУМЕНТІВ

1. Положення про організацію контролю та оцінювання якості навчання студентів (https://chdtu.edu.ua/normative/regulations/item/420-polozhennya-pro-organizatsiyu-kontrolyu-ta-otsinyuvannya-yakosti-navchannya-studentiv).

2. Положення про організацію освітнього процесу в Черкаському державному технологічному університеті (https://chdtu.edu.ua/normative/regulations/item/3636-polozhennya-pro-

orhanizatsiyu-osvitnoho-protsesu-v-cherkaskomu-derzhavnomu-tekhnolohichnomu-universyteti).

3. Кодекс академічної доброчесності Черкаського державного технологічного університету (https://chdtu.edu.ua/normative/regulations/item/8892-kodeks-akademichnoyi-dobrochesnosti-cherkaskoho-derzhavnoho-tekhnolohichnoho-universytetu-zi-zminamy).

15. ПОЛІТИКА ДИСЦИПЛІНИ

Для успішного вивчення дисципліни та проходження контрольних заходів здобувачі вищої освіти зобов'язані:

–не запізнюватися на заняття;

–не пропускати заняття (у разі хвороби надати довідку або її ксерокопію);

–своєчасно і самостійно виконувати всі передбачені програмою завдання до лабораторних робіт;

–брати очну участь у контрольних заходах;

–оволодіти навчальним матеріалом для самостійного вивчення з дисципліни у вільний від обов'язкових занять час;

–підтримувати зворотній зв'язок з викладачем на всіх етапах вивчення дисципліни;

–дотримуватися академічної доброчесності.