

Затверджено

Завідувач кафедри УКБЗІ

“ 31 “ серпня 2026 р.

С. Легомінова

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

Лектор курсу			Рабчун Дмитро Ігорович, кандидат технічних наук, доцент кафедри управління інформаційною та кібернетичною безпекою		Контактна інформація лектора (e-mail), сторінка курсу в Google Classroom		e-mail: d.rabchun@duikt.edu.ua сторінка курсу в Google Classroom – https://classroom.google.com/c/NzExOTY3OTEyNTgy?cjc=c3n2zog	
Галузь знань			12 «Інформаційні технології»		Рівень вищої освіти		магістр	
Спеціальність			125 «Кібербезпека та захист інформації»		Семестр		9	
Освітня програма			«Управління інформаційною та кібернетичною безпекою»		Тип дисципліни		Основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
	5	150	Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
			18		36		96	
АНОТАЦІЯ КУРСУ								
Взаємозв'язок у структурно-логічній схемі								
Освітні компоненти, які передують вивченню			Прикладна загальна теорія систем інформаційної та кібербезпеки, Системи управління інформаційною безпекою, Управління інцидентами інформаційної безпеки, Корпоративна та професійна етика в кібербезпеці, Науково-технічний переклад, Організація проведення наукових досліджень.					
Освітні компоненти для яких є базовою			Організація проведення наукових досліджень, Переддипломна практика					
Мета курсу:		формування у студентів необхідної системи знань із системного аналізу категорії інформаційного ризику на підґрунті використання фінансового аналізу, якісних підходів, економіко-математичних методів і моделей управління ризиками інформаційної безпеки.						
Компетентності відповідно до освітньої програми								
Soft- skills / Компетентності загальні (КЗ)					Hard-skills / Компетентності фахові спеціальні (КФ)			
КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.					КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності			

	бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
Програмні результати навчання (ПРН)	
ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах. ПРН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації. ПРН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації. ПРН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. ПРН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому. ПРН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Розділ 1 «Базові поняття»			
Тема 1. Базові поняття управління ризиками Знати: 1. Засвоїти основні поняття ризиків 2. Опанувати класифікацію ризиків Вміти: 1. Класифікувати ризики. Формування компетенцій: КФ2, КЗ-2 Результати навчання: ПРН10 Рекомендовані джерела: 1, 3–5	Лекція 1	7,8*	Лекція-візуалізація
	Практичне заняття 1		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 2		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 4		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання

Тема 2. Класифікація ризиків Знати: 1. Засвоїти основні поняття ризиків 2. Опанувати класифікацію ризиків Вміти: 1. Оперувати понятійним апаратом теорії ризиків Формування компетенцій: КФ2 Результати навчання: РН10 Рекомендовані джерела: 1, 3–8	Лекція 3	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 6		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 4		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 7		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 8		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
Тема 3. Прогнозування розвитку Знати: 1. Засвоїти основні закономірності та моделі розвитку 2. Опанувати використання основних залежностей розвитку Вміти: 1. Вивчення підходів щодо використання прогностичних математичних моделей розвитку Формування компетенцій: КФ2 Результати навчання: РН10 Рекомендовані джерела: 1, 3–8	Лекція 5	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9		Мозковий штурм, навчальна дискусія, вирішення практичних задач
	Практичне заняття 10		Мозковий штурм, навчальна дискусія, вирішення практичних задач
	Лекція 6		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 11		Мозковий штурм, навчальна дискусія, вирішення практичних задач
	Практичне заняття 12		Мозковий штурм, навчальна дискусія, вирішення практичних задач
Тема 4. Системний підхід до управління ризиками Знати: 1. Засвоїти основні складові системного підходу 2. Опанувати окремі методи системного підходу 3. Вивчити теоретичні основи функціонально-вартісного підходу Вміти: Прийняття рішень за допомогою функціонально-вартісного підходу Формування компетенцій: КФ2, КФ5, КЗ-4, КЗ-5 Результати навчання: РН10, РН31	Лекція 7	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 13		Тестування, навчальна дискусія, вирішення практичних задач
	Практичне заняття 14		Тестування, навчальна дискусія, вирішення практичних задач

<u>Рекомендовані джерела:</u> 1, 3–8	Лекція 8		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 15		Мозковий шторм, навчальна дискусія, вирішення практичних задач
	Практичне заняття 16		Проведення модульного контролю № 1
Тема 1. <i>Базові поняття управління ризиками</i> Тема 2. <i>Класифікація ризиків</i> Тема 3. <i>Прогнозування розвитку</i> Тема 4. <i>Системний підхід до управління ризиками</i>	Самостійна робота		1 Порівняльна характеристика ризиків вірусних атак 2 Порівняльна характеристика засобів антивірусного захисту 3 Засоби захисту від мережових атак 4 Класифікація комп'ютерних немережових атак 5 Засоби захисту від комп'ютерних немережових атак 6 Класифікація загроз інформаційної безпеці державного підприємства 7 Класифікація загроз інформаційної безпеці приватного підприємства
Розділ 2 «Міри ризику»			
Тема 5. <i>Базові показники ймовірностей</i> <u>Знати:</u> Засвоїти основні ймовірнісні міри ризику, Опанувати методи чисельного розрахунку ймовірнісних мір ризику <u>Вміти:</u> Чисельний розрахунок базових показників ймовірностей <u>Формування компетенцій</u> КФ2, КФ5, КЗ-2 <u>Результати навчання:</u> РН10, РН31 <u>Рекомендовані джерела:</u> 1–8	Лекція 9	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 17		Тестування, навчальна дискусія, вирішення практичних задач
	Практичне заняття 18		Тестування, навчальна дискусія, вирішення практичних задач
	Лекція 10		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 19		навчальна дискусія, вирішення практичних задач
	Практичне заняття 20		навчальна дискусія, вирішення практичних задач
Тема 6. <i>Ймовірнісні міри ризику</i> <u>Знати:</u> Засвоїти основні ймовірнісні міри ризику Опанувати методи чисельного розрахунку ймовірнісних мір ризику <u>Вміти:</u> Проводити чисельний розрахунок ймовірнісних мір ризику <u>Формування компетенцій:</u> КФ2, КФ5 <u>Результати навчання:</u> РН10, РН31 <u>Рекомендовані джерела:</u> 1–8	Лекція 11	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 21		Усне опитування, тестування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 22		Усне опитування, тестування, навчальна дискусія, обговорення ситуаційного завдання

	Лекція 12		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 23		навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 24		Усне опитування, тестування, навчальна дискусія, обговорення ситуаційного завдання
Тема 7. <i>Міри корисності та Одноетапні процедури прийняття рішень</i> Знати: Засвоїти основні міри корисності Опанувати методи чисельного розрахунку мір корисності Вміти: Здобути та закріпити практичні навички щодо застосування одно етапних процедур прийняття рішень Формування компетенцій: КФ2, КФ5 Результати навчання:РН10, РН31 Рекомендовані джерела: 1–8	Лекція 13	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 25		Усне опитування, навчальна дискусія, кейс-метод
	Практичне заняття 26		Усне опитування, навчальна дискусія, кейс-метод
	Лекція 14		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 27		дискусія, кейс-метод
	Практичне заняття 28		дискусія, кейс-метод
Тема 8. <i>Ризики інвестиційних проектів та Норма доходу</i> Знати: Засвоїти основні ризики інвестиційних проектів Опанувати методи чисельного розрахунку ризиків інвестиційних проектів Вміти: застосовувати одноетапні процедури прийняття рішень Формування компетенцій: КФ2, КФ5, КЗ-5 Результати навчання:РН10, РН31 Рекомендовані джерела: 1, 3–8	Лекція 15	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 29		Усне опитування, тестування, навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 30		Усне опитування, тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 16		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 31		навчальна дискусія, обговорення ситуаційного завдання
	Практичне заняття 32		навчальна дискусія, обговорення ситуаційного завдання

Тема 9. Планування, ідентифікація, якісний аналіз та Знати: Засвоїти сучасні підходи щодо управління ризиками в межах менеджменту проектів Вміти: проводити процедуру аналізу та оцінювання ризиків інформаційної безпеки відповідно до кращих світових практик Формування компетенцій: КФ2, КФ5 Результати навчання: РН10, РН31 Рекомендовані джерела: 1, 3–8	Лекція 17	7,8*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 33		Усне опитування, тестування, навчальна дискусія, вирішення практичних задач
	Практичне заняття 34		Усне опитування, тестування, навчальна дискусія, вирішення практичних задач
	Лекція 18		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 35		Тестування, навчальна дискусія, вирішення практичних задач
	Практичне заняття 36		Проведення модульного контролю № 2
Тема 5. <i>Базові показники ймовірностей</i> Тема 6. <i>Ймовірнісні міри ризику</i> Тема 7. <i>Міри корисності та одноетапні процедури прийняття рішень</i> Тема 8. <i>Ризики інвестиційних проектів та Норма доходу</i> Тема 9. Планування, ідентифікація, якісний аналіз та	Самостійна робота		1. Взаємодія служби інформаційної безпеки з іншими безпековими службами 2. Тенденції розвитку мережових атак 3. Тенденції розвитку вірусних атак 4. Тенденції розвитку інформаційних атак в державному секторі 5. Тенденції розвитку інформаційних атак в приватному секторі 6. Тенденції розвитку засобів інформаційної протидії 7. Статистичні оцінки ефективності засобів інформаційної протидії 8. Оцінка економічних втрат приватного підприємства від інформаційних атак
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
• Мультимедійний проектор; • Комп'ютерний клас для проведення практичних занять.			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
1. Рабчун Д.І. Бржевська З.М., Драгунцов Р.І. Принципи забезпечення безпеки архітектури інформаційної системи на базі клієнтських додатків для ОС Android. Кібербезпека: освіта, наука, техніка. м. Київ, 2020. Том 4, №8. С. 49-60. 2. Рабчун Д.І. Шевченко В. Л. Постановка задачі ресурсної оптимізації комплексу програмних засобів захисту інформації в умовах динамічного інформаційного протистояння. Системи озброєння і військова техніка: наук.-техн. журнал, 2017. №3(51). – С. 89-94 3. Cybersecurity Fundamentals Study Guide, 2nd Edition. ISACA, 2017, ISBN 978-1-60420-700-2			

4. ISO/IEC 27000:2009. Information technology – Security techniques – Information security management systems – Overview and vocabulary (Інформаційні технології. Методи безпеки. Системи управління інформ- маційною безпекою. Огляд і словник).
5. A Guide to the Project Management Body of Knowledge. (PMBOK Guide) – Fifth edition. Project Management Institute, 2013. URL : http://dinus.ac.id/repository/docs/ajar/PMBOKGuide_5th_Ed.pdf.
6. NIST Special Publication 800-30 Revision 1. Guide for Conducting Risk Assessments. NIST. Режим доступу: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>
7. OWASP risk rating Methodology. Режим доступу: https://web.archive.org/web/20160218160854/https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
8. Легомінова С.В., Мужанова Т.М., Щавінський Ю. В., Якименко Ю.М., Запорожченко М.М. Рабчун Д. І. Аудит інформаційної безпеки : навчальний посібник. Київ: Державний університет інформаційно-комунікаційних технологій, 2023. 135 с.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов’язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблене опрацювання за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп’ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

*КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КONTРоль	<i>Робота на заняттях, у т.ч.:</i>	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБіЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ KONTРоль)	Модульний контроль № 1	максимальна оцінка – 15 балів
	Модульний контроль № 2	максимальна оцінка – 15 балів

Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку	
ПІДСУМКОВЕ ОЦІНЮВАННЯ Залік	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов’язків. Залік проходить в усній формі.	30 балів	
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			
бали	Критерії оцінювання	Рівень компетентності	Оцінка / запис в екзаменаційній відомості
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об’єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов’язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об’єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	Високий Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивченні інших дисциплін, а також знання, набуті при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	Достатній Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивченні дисципліни	Добре / Зараховано (В)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але	Достатній Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання	Добре / Зараховано (С)

	допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	теоретичних положень для практичного використання викликають утруднення.	
67-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача.	Середній Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-66	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	Середній Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
40-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) В залікову книжку не представляється
0-39	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі заліку.	Незадовільний Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) В залікову книжку не представля- ється
ДОТРИМАННЯ АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ			
Виконання навчальних завдань на практичних заняттях та під час самостійної підготовки, проведення поточного контролю результатів навчання, з використанням самостійних (індивідуальних) форм роботи, зокрема за допомогою системи GWE перевіряється на плагіат у відповідності з Кодексом академічної доброчесності Державного університету інформаційно-комунікаційних технологій https://duikt.edu.ua/uploads/p_447_96297052.pdf?2			