Затверджено
Завідувач кафедри УКБЗІ_____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ “ТЕОРІЯ РИЗИКІВ”

Лектор курсу			**Лозова Ірина Леонідівна**, доцент кафедри «Управління інформаційною та кібернетичною безпекою»		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** i.iryna@duikt.edu.ua **сторінка курсу в Google Classroom –** https://classroom.google.com/c/Nzc1MTg1MzI0NDc1?cjc=bzvynuy5	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	бакалавр	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	5	
Освітньо-професійна програма			Інформаційна та кібернетична безпека		**Тип дисципліни**	Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у студентів знань, умінь і практичних навичок щодо ідентифікації, оцінювання, аналізу та управління ризиками у сфері інформаційної безпеки, а також засвоєння методології побудови системи менеджменту ризиків відповідно до міжнародних стандартів ISO.
Освітні компоненти для яких є базовою	Система менеджменту інформаційної безпеки, Безпека web-ресурсів, Комплексні системи захисту інформації

Компетентності відповідно до освітньої програми

Інтегральна компетентність (ІК)	**Фахові компетентності (СК)**
Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.	**СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

Програмні результати навчання (РН)

РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків

Затверджено
Завідувач кафедри УКБЗІ_____ С. Легомінова
“ 31 “ серпня 2026 р.

СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ “ТЕОРІЯ РИЗИКІВ”

Лектор курсу			**Лозова Ірина Леонідівна**, доцент кафедри «Управління інформаційною та кібернетичною безпекою»		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** i.iryna@duikt.edu.ua **сторінка курсу в Google Classroom –** https://classroom.google.com/c/Nzc1MTg1MzI0NDc1?cjc=bzvynuy5	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	бакалавр	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	5	
Освітньо-професійна програма			Інформаційна та кібернетична безпека		**Тип дисципліни**	Основна компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:	формування у студентів знань, умінь і практичних навичок щодо ідентифікації, оцінювання, аналізу та управління ризиками у сфері інформаційної безпеки, а також засвоєння методології побудови системи менеджменту ризиків відповідно до міжнародних стандартів ISO.
Освітні компоненти для яких є базовою	Система менеджменту інформаційної безпеки, Безпека web-ресурсів, Комплексні системи захисту інформації

Компетентності відповідно до освітньої програми

Інтегральна компетентність (ІК)	**Фахові компетентності (СК)**
Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.	**СК7.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

Програмні результати навчання (РН)

РН17. Забезпечувати функціонування системи управління кібербезпекою і захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 “ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ”			
Тема 1. ***Основи теорії ризиків і принципи управління ними*** ***Знати***: Ключові поняття, пов’язані з ризиками, їхні основні види та класифікацію; різницю між поняттями ризику та невизначеності; основні джерела виникнення ризиків; взаємозв’язок між ризиком, загрозою та вразливістю; чинну нормативно-правову базу у сфері управління ризиками; міжнародні й національні стандарти, що регулюють управління ризиками інформаційної безпеки; передумови, причини та фактори формування ризиків; послідовність етапів процесу управління ризиками; методи ідентифікації ризиків та підходи до вибору стратегій реагування. ***Вміти:*** Виконувати класифікацію ризиків; застосовувати сучасні методи та інструменти для їх ідентифікації; обґрунтовувати та реалізовувати стратегії реагування; використовувати підходи оптимізаційного моделювання для прийняття управлінських рішень; визначати джерела, причини й фактори, що впливають на рівень ризику. ***Формування компетенцій:*** СК7 ***Результати навчання:*** РН17 ***Рекомендовані джерела:*** 1-12	Лекція 1 2 год	12	Лекція-візуалізація
	Практичне заняття 1 2 год		Навчальна дискусія, обговорення ситуаційного завдання
	Лекція 2 2 год		Лекція-візуалізація
	Практичне заняття 2 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 3 2 год		Лекція-візуалізація
	Практичне заняття 3 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 4 2 год		Лекція-візуалізація
	Практичне заняття 4 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
Тема 1. Основи теорії ризиків і принципи управління ними	Самостійна робота 30 год	3	1. Концептуальна різниця між ризиком та невизначеністю: аналіз джерел та наслідків. 2. Структура та взаємозв'язок понять: ризик, загроза та вразливість у системі безпеки. 3. Комплексна класифікація ризиків: систематизація за джерелами, характером та можливістю управління. 4. Фактори формування ризиків: передумови, причини та чинники виникнення ризиків у бізнес-середовищі.

			5. Нормативно-правове регулювання управління ризиками: огляд чинної бази України. 6. Міжнародні стандарти в управлінні ризиками інформаційної безпеки: детальний аналіз ISO 27001 та його співвідношення з ISO 31000. 7. Процес управління ризиками за ISO 31000: послідовність етапів та їхня роль у прийнятті рішень. 8. Методи ідентифікації ризиків: порівняльний аналіз якісних та кількісних підходів (SWOT, Ісікава, Чек-лісти). 9. Стратегії реагування на негативні ризики: уникнення, зниження, передача та прийняття – критерії вибору. 10. Кількісна оцінка ризиків: застосування матриці ризиків та критеріїв прийнятності.
Тема 2. ***Ймовірнісні методи та кількісні підходи до аналізу й управління ризиками інформаційної безпеки.*** ***Знати***: основні поняття теорії ймовірностей: типи випадкових величин, функція розподілу та функція щільності розподілу; ймовірнісні показники ризику: математичне сподівання, дисперсію, стандартне відхилення, коефіцієнт варіації та їх роль у процесі оцінювання ризику; основні критерії ухвалення рішень в умовах невизначеності та ризику (критерії Вальда, Лапласа, Гурвіца, Севиджа тощо); методології управління ризиками інформаційної безпеки (ISO/IEC 27005, OCTAVE, NIST SP 800-30 та ін.); типові методи кількісного аналізу ризику: метод очікуваного збитку (ALE), оцінювання ймовірності загроз, моделі впливу та критичності, матриці ризиків; призначення та можливості спеціалізованого програмного забезпечення для оцінювання та обробки ризиків ІБ. ***Вміти***: застосовувати математико-ймовірнісні показники ризику для порівняння альтернатив та вибору оптимального рішення в умовах невизначеності; використовувати критерії прийняття рішень у ситуаціях ризику та неповної інформації; виконувати кількісний аналіз загроз і вразливостей, визначати рівень очікуваних збитків і формувати профіль ризиків; працювати з програмними інструментами та сервісами для аналізу й управління ризиками (наприклад, RiskLens, CRAMM, Egeria, Risk Analyzer тощо); формувати рекомендації щодо оптимізації системи захисту на основі отриманих кількісних показників ризику. ***Формування компетенцій:*** СК7	Лекція 5 2 год	12	Лекція-візуалізація
	Практичне заняття 5 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 6 2 год		Лекція-візуалізація
	Практичне заняття 6 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 7 2 год		Лекція-візуалізація
	Практичне заняття 7 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 8 2 год		Лекція-візуалізація
	Практичне заняття 8 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 9 2 год		Лекція-візуалізація
	Практичне заняття 9 2 год		Модульний контроль. Виконання кваліфікаційних завдань. Тестування

Результати навчання: РН17 ***Рекомендовані джерела:*** 1-12			
Тема 2. Ймовірнісні методи та кількісні підходи до аналізу й управління ризиками інформаційної безпеки	Самостійна робота 24 год	3	1. Побудова функції розподілу ризику для інформаційного інциденту та аналіз її характеристик. 2. Використання математичного сподівання та дисперсії для оцінки збитків від кібератаки. 3. Порівняння критеріїв ухвалення рішень у невизначених умовах: практичний приклад. 4. Моделювання ризиків за методом ALE (Annual Loss Expectancy) для вибраної інформаційної системи. 5. Побудова та інтерпретація матриці ризиків (Risk Matrix) для організації. 6. Оцінювання ймовірності загроз за статистичними даними CERT/CSIRT. 7. Аналіз моделі OCTAVE: етапи, переваги, недоліки, застосування на практиці. 8. Застосування критеріїв Гурвіца або Севиджа для вибору стратегії захисту інформації. 9. Огляд та порівняння програмних продуктів для управління ризиками інформаційної безпеки. 10. Оцінювання впливу інцидентів шляхом побудови сценаріїв та моделювання рівня критичності.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система
- комп'ютерний клас для проведення занять
- перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до тексту лекцій для підготовки до практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Коломійцев О.В., Панченко В.І., Лисиця Д.О. Теорія ризиків : навчальний посібник для студентів спеціальності 123 «Комп'ютерна інженерія» денної та заочної форм навчання. Харків: НТУ «ХПІ», 2025. 408 с. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/41734c32-fe4f-46b3-82df-a43e8c81ee38/content
2. Гончар С. Ф. Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури : автореф. дис. докт. техн. наук : спец. 05.13.21. Київ, 2020. 38 с.
3. Когут Ю. І. Кібербезпека та ризики цифрової трансформації компаній : практичний посібник. Київ : Консалтингова компанія «СІДКОН», 2021. 372 с.
4. Кравченко М. О., Бояринова К. О., Копішинська К. О. Управління ризиками : навч. посіб. для студ. спеціальності 073 «Менеджмент». Київ: КПІ ім. Ігоря Сікорського, 2021. 432 с. URL: https://ela.kpi.ua/handle/123456789/43528
5. Стратегія кібербезпеки України. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini
6. Терентьєв О. М., Зайченко С. В., Клешов А. Й., Шевчук Н. А. Технічні ризики. Теорія та практикум: навч. посібник. Київ : Інтерсервіс, 2020. 164 с.
7. Кущик А. П. Управління ризиками : навчальний посібник для здобувачів ступеня вищої освіти магістра спеціальності «Фінанси, банківська справа,

страхування та фондовий ринок» освітньо-професійної програми «Фінанси і кредит». Запоріжжя: Запорізький національний університет, 2024. 119 с. URL: https://dspace.znu.edu.ua/jspui/bitstream/12345/19178/1/0057681.pdf

8. Ризик-менеджмент. Методичні рекомендації до вивчення дисципліни для бакалаврів спеціальності 073 Менеджмент / Укладач: О.В. Заярнюк. Кропивницький: ЦНТУ, 2023. 40 с. URL: https://dspace.kntu.kr.ua/server/api/core/bitstreams/3acf00af-82d9-4e1c-aeba-cc69dd4aa6f7/content

9. Аналіз моделювання і управління ризиком (в схемах та прикладах) : навчальний посібник / Г. М. Азаренкова. – 2-ге видання, стереотипне. Львів : «Новий Світ-2000», 2025. 240 с.

10. Шульга В.П., Корченко О.Г., Заріцький О.В., Лозова І.Л., Педченко Є.М. Метод оцінювання негативних наслідків від порушення конфіденційності персональних даних. Захист інформації. 2023. Т. 25, № 4. С. 254-268. URL: https://doi.org/10.18372/2410-7840.25.18232

11. Корченко О.Г., Лозова І.Л. Структурна модель системи оцінки негативних наслідків втрати персональних даних. Наукові записки ДУІКТ. 2024. №2 (6). С. 165-170. URL: https://doi.org/10.31673/2786-8362.2024.028264

12. Pedchenko Y., Karpinski M., Lozova I., Kotyk O., Petrovska M. Damage assessment from the personal data loss. Problems of scientific, technical and legal support for cybersecurity in the modern world : monograph / ed. by S. Semenov, M. Muchacki, Krakow. 2024. P. 34-46. DOI: 10.24917/9788668020861 URL: https://bazawiedzy.uken.krakow.pl/info/article/UKENca47634692fd430697964f5fa8af695f/

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 поглиблена проробка 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 КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• 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, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали

РУБІЖНЕ ОЦІНЮВАННЯ (КОНТРОЛЬ)	Контроль № 1 «Основи теорії ризиків і принципи управління ними»	максимальна оцінка – 30 балів
	Контроль № 2 «Ймовірнісні методи та кількісні підходи до аналізу й управління ризиками інформаційної безпеки»	максимальна оцінка –30 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	звільнення від другого тестування та зарахування максимального балу за нього
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	40 балів
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ		**100 балів**

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 вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені 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 вивчені 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 допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни.	Добре / Зараховано (С)

	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.	Додаткові питання про можливість використання 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)
35-59	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 вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену.	**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 проставляється*
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**		