МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ВІННИЦЬКИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ ІНСТИТУТ
Кафедра фінансів

СИЛАБУС

ФІНАНСОВА КІБЕРБЕЗПЕКА / FINANCIAL CYBERSECURITY

Інформація про викладача	
Викладач	Маршук Ліна
Науковий ступінь	Кандидат економічних наук
Вчене звання	Доцент
Посада	Доцент кафедри фінансів
Адреса кафедри	м. Вінниця, вул. Театральна, 21
Контактний телефон	0967029082
E-mail:	l.marshuk@vtei.edu.ua
Електронна сторінка курсу в системі дистанційного навчання	https://m.vtei.edu.ua/course/index.php?categoryid
Інформація про освітній компонент	
Статус компонента	Вибірковий
Освітній ступінь	Бакалавр
Навчальний рік	2025/2026
Анотація курсу	Фінансова кібербезпека вибірковий освітній компонент обумовлений необхідністю формуванням у здобувачів вищої освіти поглиблених знань та практичних навичок захисту фінансової інформації в умовах цифрової трансформації економіки. У межах освітнього компоненту розглядаються основи кібербезпеки, види кіберзагроз, методи захисту електронних платежів, конфіденційних даних і фінансових систем. Особлива увага приділяється практичним аспектам управління кіберризиками, протидії фінансовому шахрайству та використанню інноваційних технологій, таких як блокчейн та штучний інтелект. Освітній компонент «Фінансова кібербезпека» аналізує реальні кейси кіберзлочинів у фінансовій сфері та правові аспекти їх попередження. Отримані знання допоможуть здобувачам вищої освіти стати фахівцями, здатними ефективно працювати у фінансових установах та забезпечувати їхню інформаційну безпеку.
Мова викладання	Українська мова
Результати навчання	Вміти ідентифікувати та класифікувати основні види кіберзагроз і ризиків у фінансовій сфері. Знати та окреслювати вразливість фінансових систем і розробляти стратегію їхнього захисту. Вміти застосовувати сучасні технології, таких як криптографія, блокчейн та штучний інтелект, для забезпечення фінансової кібербезпеки.

	Оцінювати кіберризити у фінансових установах і впроваджувати ефективні заходи їх мінімізації. Розробляти та впроваджувати політики захисту фінансових даних та електронних платежів. Вміти інтерпретувати правові та етичні аспекти кібербезпеки у фінансовій діяльності на міжнародному та національному рівнях. Проводити кіберобізнаність працівників фінансових установ та ефективно протидіяти методам соціальної інженерії.

Тематичний план та оцінювання результатів навчання

Назва теми	Кількість годин				Форми контролю	Бальна оцінка
	Усього годин / кредитів	з них				
		лекції	практичні	СРС		
Тема 1. Основи фінансової кібербезпеки	18	4	4	10	В, РПЗ, УД, К, Д, Т, П	10
Тема 2. Кіберзагрози у фінансовій сфері	18	4	4	10	В, УД, Д, К, РЗ, КТ, П	10
Тема 3. Фінансові шахрайства у цифровому середовищі	18	4	4	10	В, РПЗ, УД, К, Д, Т, П	10
Тема 4. Правові аспекти фінансової кібербезпеки	18	4	4	10	В, УД, Д, К, РЗ, КТ, П	10
Тема 5. Кіберризики в електронних платіжних системах	18	4	4	10	В, РПЗ, УД, К, Д, Т, П	10
Тема 6. Захист фінансових даних і конфіденційності клієнтів	9	2	2	5	В, К, Т, Д	5
Тема 7. Роль цифрових технологій у забезпеченні фінансової безпеки	9	2	2	5	РПЗ, Т, РЗ	5
Тема 8. Інформаційна безпека фінансових установ	9	2	2	5	В, Т, К, УД	5
Тема 9. Управління кіберризиками у фінансах	9	2	2	5	П, Т, РМГ	5
Тема 10. Кібербезпека на фінансових ринках	9	2	2	5	П, Т, РМГ	5
Тема 11.Навчання персоналу та підвищення кіберобізнаності	9	2	2	5	В, Т, К, Д	5
Тема 12. Кібезпезпека в умовах глобальної цифрової трансформації	9	2	2	5	В, РМГ, П	5
Індивідуальне завдання	27			27	ІЗ	15

Разом	**180/6**	**34**	**3**	**112**		**100**
Підсумковий контроль-екзамен						
Поточний контроль / критерії оцінювання	**Перелік умовних позначень форм контролю та оцінка їх у балах:** В – відповідь на практичних заняттях – 1 бал. РПЗ – розв'язання практичних завдань – 2 бали. УД – участь у дискусії – 1 бал. КТ – комп'ютерне тестування – 1 бал. Т – тестування – 1 бал. РЗ – розв'язування задач – 2 бали. К – кейс-стаді – 2 бали. РМГ – робота в малих групах – 2 бали. Д – доповідь – 1 бали. П – презентація – 2 бали. ІЗ – індивідуальні завдання – 15 балів (курси на платформі Prometheus або на інших сервісах / участь у наукових заходах). **Загальна сума за поточну навчальну роботу (аудиторну та самостійну) за семестр – 100 балів.**					
Основні літературні та інформаційні джерела	1. Бараненко Р.В. Кібератаки як одна з форм кібертероризму. *Вчені записки ТНУ ім. В.І. Вернадського. Серія: Технічні науки.* 2021. Т. 32 (71), ч. 1. С. 45–50. URL: https://science.lpnu.ua 2. Бухтіярова А.Г., Гуща А.В. Протидія кіберзлочинності у банківській сфері. *Приазовський економічний вісник*. 2021. № 3 (14). С. 355–361. URL: https://science.lpnu.ua 3. Законодавство ЄС і України у сфері кібербезпеки. 2022. URL: https://www.undp.org 4. Офіційний сайт Міністерства фінансів України URL: https://mof.gov.ua/uk 5. Офіційний сайт Національного банку України URL: https:// https://bank.gov.ua/ 6. Фінансова безпека банків в умовах цифровізації. *MDPI.* 2023. URL: https://www.mdpi.com 7. Irtyshcheva, I., Boiko, Y., Pavlenko, O. Economic Monitoring of Transformation Processes: National Realities and Foreign International. *MDPI.* 2023. URL: https://www.mdpi.com 8. Irtyshcheva, I., Kramarenko, I., Stehnei, M. The Effect of Digital Technology Development on Economic Growth. *SHS Web of Conferences*. 2021. № 100. URL: https://www.shs-conferences.org/articles/shsconf/pdf/2021/17/shsconf_ies2021_01010.pdf 9. UNDP. Кращі практики управління кібербезпекою: аналітичний звіт. 2023. URL: https://www.undp.org					
Політика освітнього компонента						
Організація навчання	Відповідно до Положення про організацію освітнього процесу здобувачів вищої освіти					
Відпрацювання пропусків занять	У разі пропуску лекції студент може самостійно опрацювати навчальний матеріал за лекцією, скласти словник термінів, підготувати конспект лекції або скласти схему основних понять, виконати завдання, які були запропоновані викладачем на лекції. У разі пропуску практичного заняття студент має самостійно виконати практичне завдання, а потім захистити його перед викладачем. Відпрацювання пропусків занять є обов'язковим для всіх студентів, незалежно від джерел фінансування навчання.					
Допуск до	Підсумковий контроль-екзамен. До екзамену допускаються всі здобувачі.					

підсумкового контролю	які набрали за результатами поточної роботи протягом семестру 60 балів. Результат підсумкового контролю (екзамен) з освітнього компонента для здобувачів очної форми навчання визначається як середньоарифметична сума балів поточної роботи та екзамену. Кращим здобувачам, які повністю виконали програму з освітнього компонента, виявили активність в науково-дослідній роботі за відповідною тематикою, стали призерами студентських олімпіад, виступали на конференціях та за результатами поточної роботи набрали 90 і більше балів, науково-педагогічний працівник має право виставити результат екзамену без виконання екзаменаційного завдання (при письмовому екзамені), про що робить запис в екзаменаційному листі здобувача.
Академічна доброчесність	Для забезпечення академічної доброчесності студентам необхідно дотримуватися Положення про дотримання академічної доброчесності педагогічними та науково-педагогічними працівниками та здобувачами освіти
Інші складові політики компоненту	Основні принципи проведення практичних занять з курсу «Фінансової кібербезпеки» - відкритість до нових та неординарних ідей, толерантність, доброзичлива партнерська атмосфера взаєморозуміння та творчого розвитку. Усі завдання, передбачені програмою, мають бути виконані у встановлений термін. Різні моделі роботи на практичних заняттях (індивідуальна, в парах, в мікро-групах, групах) над вирішенням завдань дає можливість здобувачам вищої освіти якнайширше розкрити свій власний потенціал, навчитись довіряти своїм партнерам, розвинути навички інтелектуальної роботи в команді. Курс «Фінансова кібербезпека» передбачає інтенсивне використання мобільних технологій навчання, що дає можливість здобувачам вищої освіти та викладачеві спілкуватись один з одним у будь-який зручний для них час, а для здобувачів вищої освіти, які відсутні на заняттях, отримати необхідну навчальну інформацію та представити виконані завдання. Протягом усього курсу активно розвиваються автономні навички здобувачів вищої освіти, які можуть підготувати додаткову інформацію за темою, що не увійшла до переліку тем практичних занять та виступити з презентацією чи інформуванням додатково (оцінюється окремо).

Затверджено на засіданні кафедри протокол № 21 від 23.12.2024

Науково-педагогічний працівник Ліна МАРШУК

Завідувач кафедри Інна ГНИДЮК