

C.

“ 31 “ серпня 2026 р.

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«КОМУНІКАЦІЇ В КІБЕРБЕЗПЕЦІ ТА ЗАХИСТІ ІНФОРМАЦІЇ»

Лектор курсу			Примаченко Діана Володимирівна викладач кафедри управління кібербезпекою та захистом інформації		Контактна інформація лектора (e-mail), сторінка курсу в Classroom		e-mail: d.prymachenko@duikt.edu.ua сторінка курсу в Classroom – https://classroom.google.com/c/ODI4Mjk4MzE5NzI2?cjc	
Галузь знань			F «Інформаційні технології»		Рівень вищої освіти		перший (бакалаврський)	
Спеціальність			F5 «Кібербезпека та захист інформації»		Семестр		2	
Освітня програма			«Управління інформаційною та кібернетичною безпекою» «Управління кібербезпекою та захистом інформації» «Інформаційна та кібернетична безпека» «Системи кіберзахисту та реагування на інциденти» «Технічні системи інформаційного та кібернетичного захисту» «Технічні системи кіберзахисту»		Тип дисципліни		Обов'язкова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:					
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка	
	3	90	18	-	18	-	54	
АНОТАЦІЯ КУРСУ								
Взаємозв'язок у структурно-логічній схемі								
Освітні компоненти, які передують вивченню			Базова					
Освітні компоненти для яких є базовою			Організація конфіденційного діловодства, Організаційне забезпечення захисту інформації, Стратегічні комунікації, Політики інформаційної безпеки, Корпоративна та професійна етика в кібербезпеці, Кваліфікаційна робота.					
Мета курсу:	формування у студентів знань, умінь та навичок ефективної професійної комунікації в галузі кібербезпеки та захисту інформації; розвиток здатності чітко, аргументовано та етично передавати інформацію в усній і письмовій формах у процесі командної роботи, реагування на кіберінциденти, взаємодії з колегами, клієнтами, керівництвом і громадськістю.							

Компетентності відповідно до освітньої програми			
Загальні компетентності (ЗК)		Спеціальні (фахові, предметні) компетентності (СК)	
ІК. Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації. ЗК1. Здатність застосовувати знання у практичних ситуаціях. ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності. ЗК6. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав та свобод людини і громадянина в Україні. ЗК7. Здатність ухвалювати рішення и діяти дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності.			
Програмні результати навчання (РН)			
РН3. Застосовувати принцип неприпустимості корупції та будь-яких інших проявів недоброчесності у професійній діяльності. РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.			
ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Тема 1. Роль комунікацій у кібербезпеці Знати: сутність, функції та види комунікацій; роль інформаційної взаємодії в управлінні безпекою; вплив ефективної комунікації на запобігання інцидентам. Вміти: визначати ключові елементи комунікаційного процесу, аналізувати ефективність взаємодії в кіберкоманді. Формування компетенцій: ІК, ЗК1, ЗК2, ЗК6, ЗК7 Результати навчання: РН3, РН4 Рекомендовані джерела: 1-2	Лекція 1 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 1.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 1 6 год	2*	Підготовка рефератів та презентацій за обраною темою
Тема 2. Основи міжособистісного спілкування Знати: вербальні та невербальні засоби комунікації; техніки активного слухання; бар'єри спілкування. Вміти: о застосовувати прийоми ефективного спілкування, усувати бар'єри, формувати довірчі комунікації у команді. Формування компетенцій: ІК, ЗК1, ЗК2, ЗК6, ЗК7 Результати навчання: РН3, РН4	Лекція 2 4 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 2.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, тестування
	Самостійна робота 2 6 год	2*	Підготовка рефератів та презентацій за обраною темою

<u>Рекомендовані джерела:</u> 3-4			
Тема 3. Ділова комунікація у сфері кібербезпеки <u>Знати:</u> особливості офіційного, неофіційного та корпоративного спілкування; правила етикету електронного листування. <u>Вміти:</u> формувати офіційні повідомлення, створювати ділові документи, підтримувати професійний тон комунікації. <u>Формування компетенцій:</u> ІК, ЗКІ, ЗК2, ЗК6, ЗК7 <u>Результати навчання:</u> РН3, РН4 <u>Рекомендовані джерела:</u> 5-6	Лекція 3 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 3.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 3 6 год	2*	Підготовка рефератів та презентацій за обраною темою
Тема 4. Командна взаємодія та комунікації в ІТ-проектах <u>Знати:</u> структуру команд кібербезпеки, ролі учасників, принципи ефективної взаємодії. <u>Вміти:</u> координувати дії команди, комунікувати при розв'язанні технічних і організаційних задач. <u>Формування компетенцій:</u> ІК, ЗКІ, ЗК2, ЗК6, ЗК7 <u>Результати навчання:</u> РН3, РН4 <u>Рекомендовані джерела:</u> 7-8	Лекція 4 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 4.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 4 6 год	3*	Підготовка рефератів та презентацій за обраною темою
Тема 5. Конфлікти та шляхи їх подолання у професійному середовищі <u>Знати:</u> причини та види конфліктів у команді, стратегії управління конфліктами. <u>Вміти:</u> визначати ознаки конфлікту, застосовувати техніки їх вирішення, підтримувати позитивний клімат у колективі. <u>Формування компетенцій:</u> ІК, ЗКІ, ЗК2, ЗК6, ЗК7 <u>Результати навчання:</u> РН3, РН4 <u>Рекомендовані джерела:</u> 9-10	Лекція 5 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 5.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 5 6 год	3*	Підготовка рефератів та презентацій за обраною темою
Тема 6. Етика професійних комунікацій і кіберетика <u>Знати:</u> принципи професійної етики, поняття кіберетики, нетикету, правила комунікацій у мережі. <u>Вміти:</u> дотримуватись етичних норм у цифровому середовищі, аналізувати приклади порушень кіберетики.	Лекція 6 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 6.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів

Формування компетенцій: ІК, ЗКІ, ЗК2, ЗК6, ЗК7 Результати навчання: РН3, РН4 Рекомендовані джерела: 11-12	Самостійна робота 6 6 год	3*	Підготовка рефератів та презентацій за обраною темою
Тема 7. Комунікації під час кіберінцидентів Знати: принципи кризових комунікацій, порядок інформування керівництва та громадськості. Вміти: складати план комунікацій під час кіберінциденту, взаємодіяти з медіа та PR-службами. Формування компетенцій: ІК, ЗКІ, ЗК2, ЗК6, ЗК7 Результати навчання: РН3, РН4 Рекомендовані джерела: 13-14	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 7.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 7 6 год	3*	Підготовка рефератів та презентацій за обраною темою
Тема 8. Міжкультурна та міжнародна комунікація у сфері ІБ Знати: культурні відмінності у професійній взаємодії, норми комунікації у міжнародних кіберпроектах. Вміти: адаптувати комунікаційні стратегії до культурного контексту, будувати міжкультурну взаємодію. Формування компетенцій: ІК, ЗКІ, ЗК2, ЗК6, ЗК7 Результати навчання: РН3, РН4 Рекомендовані джерела: 15-16	Лекція 8 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 8.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 8 6 год	3*	Підготовка рефератів та презентацій за обраною темою
Тема 9. Публічні комунікації та презентації у сфері кібербезпеки Знати: основи публічних виступів, структуру презентацій, правила донесення технічної інформації для різних аудиторій. Вміти: готувати та проводити презентації, формулювати аргументи, впевнено виступати публічно. Формування компетенцій: ІК, ЗКІ, ЗК2, ЗК6, ЗК7 Результати навчання: РН3, РН4 Рекомендовані джерела: 17-18	Лекція 9 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
	Практичне заняття 9.1 2 год	4*	Усне опитування, виконання завдань на практичне застосування знань і вмінь, аналіз кейсів
	Самостійна робота 9 6 год	3*	Підготовка рефератів та презентацій за обраною темою
МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
Комп'ютерне обладнання, мережа Інтернет, мультимедійний проектор, перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до матеріалів лекцій через систему Google Classroom для підготовки до практичних занять.			
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ			
1. Ляхно В. А. Increase the cybersecurity of transport information and communications systems. <i>Ukrainian scientific journal of information security</i> . 2016. Vol. 22, no. 1. URL: https://doi.org/10.18372/2225-5036.22.10453 2. Ali Dayoub. Integrating security, privacy, and advanced cyber technologies for Resilient Urban, IoT, and AI Systems. <i>World journal of advanced engineering technology and sciences</i> . 2024. Vol. 13, no. 1. P. 085–099. URL: https://doi.org/10.30574/wjaets.2024.13.1.0394			

3. A survey on cyber security for smart grid communications / Y. Yan et al. *IEEE communications surveys & tutorials*. 2012. Vol. 14, no. 4. P. 998–1010.
URL: <https://doi.org/10.1109/surv.2012.010912.00035>
4. Cavelti M. D. Cyber-Incidents. *The Politics of Cyber-Security*. New York, 2024. P. 129–154. URL: <https://doi.org/10.4324/9781003497080-7>
5. Communication in cybersecurity: a public communication model for business data breach incident handling. *Issues in information systems*. 2017.
URL: https://doi.org/10.48009/2_iis_2017_136-147
6. Cybersecurity and network security : novel approaches to protect computer systems and networks from threat. *International research journal of modernization in engineering technology and science*. 2023. URL: <https://doi.org/10.56726/irjmets44261>
7. Erwin E. Cyber warfare ethics. *Journal of military ethics*. 2022. P. 1–6. URL: <https://doi.org/10.1080/15027570.2022.2136119>
8. Guariniello C., DeLaurentis D. Communications, information, and cyber security in systems-of-systems: assessing the impact of attacks through interdependency analysis. *Procedia computer science*. 2014. Vol. 28. P. 720–727. URL: <https://doi.org/10.1016/j.procs.2014.03.086>
9. Jadhav S. M., Mahule R. V., Sontakke A. P. Advances in cybersecurity: a comprehensive review of emerging threats and defense mechanisms. *EPJ web of conferences*. 2025. Vol. 328. P. 01047. URL: <https://doi.org/10.1051/epjconf/202532801047>
10. John Mark B. Clemen, Jerry I. Teleron. Advancements in encryption techniques for secure data communication. *International journal of advanced research in science, communication and technology*. 2023. P. 444–451. URL: <https://doi.org/10.48175/ijarsct-13875>
11. Milina V. Security in a communications society: opportunities and challenges. *Connections: the quarterly journal*. 2012. Vol. 11, no. 2. P. 53–66.
URL: <https://doi.org/10.11610/connections.11.2.04>
12. Navigating the cyber battlefield: understanding threats and safeguarding digital frontiers / S. S. Shinde et al. *2024 international conference on electrical electronics and computing technologies (ICEECT)*, Greater Noida, India, 29–31 August 2024. 2024. P. 1–6. URL: <https://doi.org/10.1109/iceect61758.2024.10739310>
13. Pasupuleti M. K. Quantum communication and cybersecurity: advancements in cryptography and secure satellite networks. *Quantum communication and cybersecurity*. 2025. P. 83–95.
URL: <https://doi.org/10.6231/nesx/77548>
14. Peniuk V. Cybersecurity and communications: modern realities. *Business navigator*. 2025. No. 4(81). URL: <https://doi.org/10.32782/business-navigator.81-47>
15. Prof. Aarti R. Naik. Cybersecurity in business. *International journal of advanced research in science, communication and technology*. 2024. P. 367–374.
URL: <https://doi.org/10.48175/ijarsct-15764>
16. Quotes C. Cybersecurity engineer i'm not arguing i'm just explaining why i'm right. Independently Published, 2020.
17. Seuwou P. Cybersecurity. *Digital business*. London, 2025. P. 195–212. URL: <https://doi.org/10.4324/9781032672458-10>
18. Đukić S. Cyber security and data protection. *Moderna arhivistika*. 2025. Vol. 8, no. 1. P. 78. URL: <https://doi.org/10.54356/ma/2025/hazd7569>
19. Легомінова, С.В., Примаченко, Д.В. Роль ризик-менеджменту в підвищенні кіберстійкості організації за умов гібридних загроз. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Том 3, №31, С. 792–800. URL: <https://doi.org/10.28925/2663-4023.2025.31.1060>
20. Капелюшина Т.В., Мужанова Т.М., Берестяна Т.В., Голобородько С.О. Примаченко, Д. В. Механізм управління доступом до інформаційних ресурсів на підприємстві. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*. 2025. Том 3, № 27. С. 205–219. URL: <https://doi.org/10.28925/2663-4023.2025.27.743>

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.			
КРИТЕРІЙ ТА МЕТОДИ ОЦІНЮВАННЯ			
Умовою допуску до підсумкового контролю є набрання студентом 60 балів у сукупності за всіма темами дисципліни.			
Форми контролю		Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	Робота на заняттях, у т.ч.:		
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)		за кожне відвідування 0,55 балу
	• участь у експрес-опитуванні		за кожну правильну відповідь 0,25 балу
	• 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 балу
	• участь у навчальній дискусії, обговоренні ситуаційного завдання		за кожну правильну відповідь 2 бали
	• участь у діловій грі		за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (КОНТРОЛЬ)	Контроль № 1 ““Комунікаційна взаємодія в системі інформаційної безпеки””		максимальна оцінка 15 балів
	Контроль № 2 “Комунікаційний менеджмент і публічні комунікації в кібербезпеці”		максимальна оцінка 15 балів
ДОДАТКОВА ОЦІНКА	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових робіт за спеціальністю, створення кейсів тощо.		Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ Залік	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов’язків. Іспит проходить у письмовій формі.		40 балів
ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ			100 балів
бали	Критерії оцінювання	Рівень компетентності	Оцінка /зачис в екзаменаційній відомості
90	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в	Високий Повністю забезпечує вимоги до знань,	Відмінно / Зараховано (А)

	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.	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.	
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 (B)
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 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.	Достатній Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
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 розглядалися 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	Середній Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

	іншими дисциплінами.		
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 вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) <i>В залікову книжку не проставляється</i>
1-34	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) <i>В залікову книжку не проставляється</i>

ПОЛІТИКА ДОБРОЧЕСНОСТІ

Здобувач вищої освіти виконуючи самостійну або індивідуальну роботу повинен дотримуватись політики доброчесності. У разі наявності плагіату в будь-яких видах робіт здобувача, він отримує незадовільну оцінку і повинен повторно виконати завдання, які передбачені у Силабусі.