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

СИЛАБУС ОСВІТНЬОЇ КОМПОНЕНТИ
«Основи управління інформаційною та кібербезпекою»

Лектор курсу			Капелюшна Тетяна Вікторівна, доктор економічних наук, доцент, професор кафедри управління кібербезпекою та захистом інформації		Контактна інформація лектора (e-mail), сторінка курсу в GWE	e-mail: t.kapeliushna@duikt.edu.ua сторінка курсу в GWE - https://classroom.google.com/c/ODA1NTM1MzAxMzMz	
Галузь знань			12 Інформаційні технології		**Освітній рівень**	бакалавр	
Спеціальність			F5 Кібербезпека та захист інформації		**Семестр**	1	
Освітньо-професійна програма			Управління кібербезпекою та захистом інформації Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18		36		36

АНОТАЦІЯ КУРСУ

Взаємозв’язок у структурно-логічній схемі

Освітні компоненти для яких є базовою	Захист від шкідливого програмного засобу; Кінцеві пристрої інформаційних систем; Операційні системи; Філософія; Ознайомча практика
Мета курсу:	є формування базису знань та вмінь щодо забезпечення інформаційної та кібербезпеки із урахуванням сьогочасних небезпек у кіберпросторі

Компетенції відповідно до освітньо-професійної програми

Soft- skills / Загальні компетентності (ЗК)	Hard-skills / Спеціальні (фахові) компетенції
ІК Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації. **ЗК6** Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства прав та свобод людини і громадянина в Україні.	**СК1** Здатність застосовувати законодавчу нормативно-правову базу, а також державні міжнародні вимоги, практики і стандарти професійній діяльності. **СК2** Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації. **СК3** Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

Результати навчання відповідно до освітньо-професійної (програмні результати навчання – ПРН)

РН9 Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10 Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН11 Планувати підготовку та забезпечувати неперервність бізнес-процесів в організаціях згідно зі встановленою політикою кібербезпеки з урахування вимог до захисту інформації.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Політика оцінювання за темою**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1. Теоретичні аспекти управління кібербезпекою та захистом інформації			
Тема 1. **Основи кібербезпеки та захисту інформації: розуміння, роль, термінологічний базис, загрози безпеки даних** ***Знати***: сутність та зміст понять «кіберпростір», «інформаційний простір», «кібербезпека», «кіберінцидент», «кібератака», «інформаційна безпека», роль та значення кібербезпеки в умовах цифровізації, ландшафт кіберзагроз та передумови їх виникнення, моделі інформаційної безпеки (CIA, Parkerian Hexad, STRIDE). ***Вміти:*** оперувати категоріальним апаратом із кібербезпеки та захисту інформації; розмежовувати категорії «кібербезпека», «інформаційна безпека», аналізувати ландшафт кіберзагроз та проводити поділ загроз на внутрішні та зовнішні, застосовувати моделі забезпечення інформаційної безпеки, зважаючи на умови функціонування підприємств. ***Рекомендовані джерела:*** 1-10	Лекція 1	4*	Лекція-візуалізація
	Практичне заняття 1		Опрацювання ситуаційних завдань; кейси, усне опитування, тестування Kahoot , навчальна дискусія
	Практичне заняття 2		Виконання завдань за вказівками. Експрес опитування
Тема 2. **Інформаційні ресурси. Роль інформаційних ресурсів та їх захист в цифровому суспільстві** ***Знати***: Інформаційні ресурси. Види інформації. Захист комерційної інформації як об'єкта інтелектуальної власності. Теорії інформації, їх розвиток, що обумовлюється інформатизацією, цифровізацією. Роль інформаційних ресурсів у цифровому суспільстві та для бізнесу. Управління безпекою інформаційних ресурсів. ***Вміти***: вміти класифікувати інформаційні ресурси; провадити захист комерційної інформації як об'єкта інтелектуальної власності; розрізняти теорії інформації, їх розвиток, що обумовлюється інформатизацією, цифровізацією для формування ефективних напрямків захисту інформації; визначати роль інформаційних ресурсів у цифровому суспільстві та їх вплив на безпеку функціонування бізнесу; сформувати концепт управління безпекою інформаційних ресурсів для забезпечення кібербезпеки. ***Рекомендовані джерела:*** 1; 11-16	Лекція 2	6*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3		Мозковий штурм; інтерактивні завдання; опитування (відкриті питання)
	Практичне заняття 4		Усне опитування, тематична дискусія: презентація матеріалів
Тема 3. **Загрози інформаційній безпеці та кібербезпеці, їх аналіз** ***Знати***: Загрози та ризики інформаційній безпеці організацій. Поширені загрози кібербезпеці. Ризики та алгоритм управління ними. Послідовність та особливості аналізу загроз та викликів інформаційній безпеці (відповідно до стратегії ІБ) ***Вміти***: виявляти загрози та ризики інформаційній безпеці організацій; ідентифікувати поширені загрози кібербезпеки; аналізувати ризики; розуміти	Лекція 3	6*	Лекція-візуалізація
	Практичне заняття 5		Опрацювання ситуаційних завдань. Усне опитування. Презентації доповідей
	Практичне заняття 6		Усне опитування, тестування у Kahoot , навчальна дискусія

алгоритм управління ними та провадити послідовно аналіз загроз та викликів інформаційній безпеці (відповідно до стратегії ІБ) ***Рекомендовані джерела***: 1; 17-23			
Тема 4. **Безпека даних** ***Знати***: Персональні дані. Права суб'єкта персональних даних. Файли з інформацією про споживача. Регламент захисту даних. Права суб'єкта даних та безпека даних. Технології захисту даних. Паролі, управління доступом, двофакторна автентифікація ***Вміти***: використовувати технології захисту даних; практично застосовувати знання щодо прав захисту персональних даних задля забезпечення безпеки персональних даних. ***Рекомендовані джерела:*** 23-32	Лекція 4	6* (+15 МК1)	Лекція-візуалізація
	Практичне заняття 7		Опрацювання ситуаційних завдань. Усне опитування. Презентації доповідей
	Практичне заняття 8		Усне опитування. Проведення контролю знань №1
Розділ 2. Практичні аспекти управління кібербезпекою та захистом інформації			
Тема 5. **Безпека в інтернеті** ***Знати***: базові правила безпеки в Інтернеті; заходи захисту від шкідливих програм; правила скачування файлів і завантаження застосунків; правила безпечного користування Інтернетом задля безпеки персональних акаунтів в соціальних мережах; правила безпеки файлів; ризики надмірного поширення інформації в Інтернеті ***Вміти***: використовувати інструменти перевірки компрометації паролів; безпечні генератори паролів; користуватися надійними джерелами інформації; провадити захист від атак MitM, дотримуватися правил безпеки в мережах Wi-fi ***Рекомендовані джерела:*** 4; 33-40	Лекція 5	3*	Лекція-візуалізація
	Практичне заняття 9		Опрацювання ситуаційних завдань. Усне опитування. Презентації доповідей.
	Практичне заняття 10		Усне опитування, практичне опрацювання за матеріалами лекції
Тема5. **Безпека в інтернеті** ***(продовження)*** ***Знати:*** особливості конфігурації хмарних та поштових акаунтів та захисту ПК; правила безпеки налаштування браузерів; параметри безпеки налаштування месенджерів. ***Вміти:*** дотримуватися правил безпеки дописів; забезпечувати захист пристроїв, облікових записів та даних; перевіряти Windows на наявність кейлогерів. ***Рекомендовані джерела:*** 33-40	Лекція 6	3*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 11		Доповідь з презентацією за тематикою теми та її обговорення.
	Практичне заняття 12		Усне опитування, навчальна дискусія, ситуаційні завдання
Тема 6. **Соціальна інженерія. Фішинг. Кібершахрайство** ***Знати***: тенденції порушень безпеки даних та пристроїв; суть соціальної інженерії; фішингові технології (маніпуляції з посиланнями, телефонні дзвінки, обхід фільтрів, підробка вебсайтів); типи шкідливих програм; кібершахрайські способи порушення інформаційної та кібербезпеки. ***Вміти***: протидіяти фішингу; використовувати проактивні заходи безпеки проти соціальної інженерії; розпізнавати кібершахрайські дії та соціоінженерні техніки та протидіяти їм ***Рекомендовані джерела:*** 7; 41-46	Лекція 7	6*	Лекція-візуалізація
	Практичне заняття 13		Ситуаційні завдання
	Практичне заняття 14		Усне опитування, презентації та доповіді, обговорення.
Тема 7. **Законодавство та стандарти кібербезпеки**	Лекція 8	3*	Лекція-візуалізація, експрес-опитування студентів

Знати: Законодавство України щодо регулювання кібербезпеки та захисту інформації (ЗУ «Про основні засади забезпечення кібербезпеки України»; основні положення Плану реалізації Стратегії кібербезпеки України, ЗУ «Про Державну службу спеціального зв'язку та захисту інформації України», ЗУ «Про захист персональних даних», Закон «Про цифрові послуги (DSA)», ЗУ «Про кібербезпеку» (ЄС), Загальний регламент про захист даних (GDPR), Акт «Про ШІ» (Artificial Intelligence Act), Міжнародні стандарти; Європейське законодавство щодо регулювання кібербезпеки та захисту інформації; Міжнародне законодавство щодо регулювання кібербезпеки та захисту інформації. CERT-UA. ***Вміти***: використовувати знання нормативно-правового регулювання питань кібер- та інформаційної безпеки в Україні та світі у практичній діяльності, враховувати особливості регулювання ЄС щодо питань кібер- та інформаційної безпеки у процесі інформаційної взаємодії із контрагентами ***Рекомендовані джерела:*** 6; 47-57	Практичне заняття 15		Усне опитування, презентації. Доповіді. Обговорення за результатами доповідей.
	Практичне заняття 16		Усне опитування, навчальна дискусія, ситуаційні завдання.
Тема 8. **Інформаційна та кібербезпека в умовах гібридної війни: протидія інформаційно-когнітивним загрозам** ***Знати***: концептуальну модель гібридних загроз, типи інформаційних і когнітивних загроз у гібридному середовищі; когнітивний та віртуальний вимір небезпек у кіберпросторі в умовах гібридної війни, заходи та засоби протидії інформаційно-когнітивним загрозам; роль стратегічних комунікацій у протидії когнітивній війні ***Вміти***: ідентифікувати та класифікувати інформаційні та кіберзагрози гібридного типу; виявляти та аналізувати інформаційно-когнітивні впливи; аналізувати інформаційні потоки для виявлення деструктивних впливів і маніпуляцій; застосовувати знання для протидії інформаційно-когнітивним загрозам ***Рекомендовані джерела:*** 58-65	Лекція 9	3* (+15 МК2)	Лекція-візуалізація Експрес-опитування.
	Практичне заняття 17		Навчальна дискусія, опрацювання опанованого матеріалу та усне опитування, тестування у Kahoot
	Практичне заняття 18		Доповіді з презентацією. Проведення контролю знань №1
Залік	Проведення заліку	40*	
Самостійна робота		*	Завдання із переліку запропонованих проблемних питань для дослідження за тематикою наукових інтересів здобувача освіти у межах дисципліни

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕНН ДИСЦИПЛІНИ

Комп'ютери с програмним забезпеченням для виконання практичних робіт: комп'ютери Asus, комп'ютерний клас для проведення занять
Спеціалізована лабораторія: «Security operation center» кафедри управління кібербезпекою та захистом інформації.
Мультимедійний проєктор, мультимедійна система Acer X113 DLP
Google Workspace for Education

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Навчально-методичні матеріали з дисципліни «Управління інформаційною та кібербезпекою» для студентів спеціальності F5 «Кібербезпека та захист інформації». Google Workspace for Education - https://classroom.google.com/c/NjgxMzM5NTk3MDc2
2. Капелюшна Т.В., Мужанова, Т.М., Дьячук О. С. Концепт управління інформаційною безпекою цифрового середовища в екосистемі підприємства. Кібербезпека: освіта, наука, техніка. 2026. № 1(33). С. 144–155. https://doi.org/10.28925/2663-4023.2026.33.1209
3. Легомінова С., Якименко Ю.,Мужанова Т., Капелюшна Т. (2025). Вплив управління інцидентами на функціонування системи управління інформаційною безпекою організації. *Телекомунікаційні та інформаційні технології.* 1 (25). С. 75-81. https://doi.org/10.31673/2412-4338.2025.014011
4. Капелюшна Т., Мужанова Т., Берестяна,Т., Голобородько С., & Примаченко Д. (2025). Механізм управління доступом до інформаційних ресурсів на підприємстві. *«Кібербезпека: освіта,*

наука, техніка». *3*(27). С. 205–219. https://doi.org/10.28925/2663-4023.2025.27.743
5. Легомінова, С., Капелюшна, Т., Щавінський, Ю., Запорожченко, М., & Будзинський, О. (2025). Концепція автоматизованого реагування на загрози в корпоративних базах даних у режимі реального часу. *«Кібербезпека: освіта, наука, техніка»*. 1(29), С. 676–686. https://doi.org/10.28925/2663-4023.2025.29.927
6. Капелюшна Т.В. Легомінова С.В., Мужанова Т.М., Тищенко В.С. Регуляторне поле формування політики управління інформаційною безпекою організації. Кібербезпека: освіта, наука, техніка. 2024, 2 (26), pp. 235-245. DOI 10.28925/2663-4023.2024.26.693
7. Капелюшна Т.В. Легомінова С.В., Тищенко В.С., Недодай М.Г., Дьячук О.С. Штучний інтелект та соціальні мережі: підходи до виявлення фейкової інформації. Телекомунікаційні та інформаційні технології. 2024, 4 (85), pp. 83-89. DOI 10.31673/2412-4338.2024.044748
8. Ткаченко О.А, Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018, №1. С. 75-86.
9. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
10. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
11. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерноінтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
12. CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf
13. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
14. Ткаченко О.А, Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018, №1. С. 75-86.
15. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настрадін; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
16. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.
17. Комплексна безпека інформаційних мережевих систем: навчальний посібник для студентів спеціальності 174 «Автоматизація, комп'ютерноінтегровані технології та робототехніка» / Укладачі: А.Г. Микитишин, М.М. Митник, О.С. Голотенко, В.В. Карташов. – Тернопіль : ФОП Паляниця В.А., 2023. – 324 с.
18. Авер'янова Н. М., Воропаєва Т. С. Інформаційна безпека України: соціально-філософські аспекти. «Молодий вчений». No10(86), Жовтень. 2020. С.297-303. URL: https://molodyivchenyi.ua/index.php/journal/article/view/319/308(дата звернення 10.12.2024)
19. Биков О. М. Інформаційна безпека: сучасні ризики та загрози у сфері зберігання та обміну інформації. Legal Bulletin No 4(10), 2023. С.166-174. DOI 10.31732/2708-339X-2023-10-166-174
20. С. В. Добринь, Д. С. Шкляр, ВИЗНАЧЕННЯ СУТНОСТІ ТА ВЗАЄМОЗВ'ЯЗКУ ПОНЯТЬ "РИЗИК", "НЕБЕЗПЕКА" ТА "ЗАГРОЗА". АГРОСВІТ № 9, 2017. С48-52/
21. Savelieva, T. , Panasko, O., & Prigodyuk , O. (2018). Analysis of methods and means to implement a risk-oriented approach in the context of providing enterprise information security . Bulletin of Cherkasy State Technological University, 23(1), 81-89. https://doi.org/10.24025/2306-4412.1.2018.153279
22. Стратегія інформаційної безпеки https://zakon.rada.gov.ua/laws/show/685/2021#n2
23. Розробка основи стратегії аналізу ризиків для оцінки впливу в системах управління інформаційної безпеки: приклад з індустрії іт-консалтингу. https://tic-ua.com/uk/statti/rozrobka-osnovy-strategiyi-analizu-ryzykiv-dlya-oczinky-vplyvu-v-systemah-upravlinnya-informaczijnoyi-bezpeky-pryklad-z-industriyi-it-konsaltyngu-chastyna-2/
24. Аналіз загроз та викликів інформаційній безпеці (відповідно до стратегії ІБ) . https://www.rnbo.gov.ua/files/%D0%9D%D0%9A%D0%A6%D0%9A/2024/Cyber%20digest_Mar_2024_UA.pdf
25. Що таке персональні дані? І Онлайн-курс «Захист персональних даних» https://www.youtube.com/watch?v=aU-y23I74Og
26. Суб'єкти обробки персональних даних І Захист персональних даних. Спеціалізований курс. https://www.youtube.com/watch?v=dXyTfibl2JA
27. Підстави для обробки персональних даних І Захист персональних даних. https://www.youtube.com/watch?v=IAXt5YxzA8c
28. Як реалізувати право на поінформованість про обробку персональних даних? https://www.youtube.com/watch?v=Ao3_jME5M-8
29. Що таке право на заперечення проти обробки персональних даних? І «Захист персональних даних» https://www.youtube.com/watch?v=UCClhs9mRMI
30. Microsoft Authenticator. https://support.microsoft.com/uk-ua/account-billing/%D0%BF%D1%80%D0%BE-microsoft-authenticator-9783c865-0308-42fb-a519-8cf666fe0acc
31. Правила керування доступом – Veyon 4.9.7 documentation. Veyon Documentation – Veyon 4.9.7 documentation. URL: https://docs.veyon.io/uk/latest/admin/access-control-rules.html
32. CASES – Creative industries social media. CASES. URL: https://cases.media/en/cookie?srsltid=AfmBOorGVc8kph-ODmwt5sqcGCiRElYiM3bwy9QdW8NeRuDtCSZX0dYd
33. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
34. Перевірка сайту по URL. «Безпечний перегляд: статус сайту» https://transparencyreport.google.com/safe-browsing/search
35. BRAMA/ https://stopfraud.gov.ua/guide
36. Захистіть корпоративне середовище від кіберзагроз. https://www.eset.com/ua/business/enterprise/?srsltid=AfmBOorJYq7EoBgxAVPZhJSQ_i9smWDAEoXPzWak88lEoghGCf6n_TN1#threat-intelligence
37. Безпека Ваших пристроїв: 7https://dovidka.info/kiberbezpeka/
38. Принципи запровадження кіберкультури: https://moz.gov.ua/uk/principi-zaprovadzhennya-kiberkulturi
39. Куперштайн Л., Малиновський В, Каплун В. КІБЕРБЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ТА ІНТЕРНЕТУ РЕЧЕЙ / КІБЕРБЕЗПЕКА МОБІЛЬНИХ ПРИСТРОЇВ ТА ІНТЕРНЕТУ РЕЧЕЙ: https://www.researchgate.net/publication/379257182_CYBER_SECURITY_OF_MOBILE_DEVICES_AND_INTERNET_OF_THINGS_KIBERBEZPEKA_MOBILNIH_PRISTROIV_TA_INTERNETU_RECEJ
40. Особиста кібербезпека: захист персональних пристроїв: https://mod.gov.ua/explanation/osobista-kiberbezpeka-zahist-personalnih-pristroyiv
41. Особиста кібербезпека: паролі та месенджери: https://mod.gov.ua/osobista-kiberbezpeka-paroli-ta-mesendzheri
42. Phishing Explained In 6 Minutes | What Is A Phishing Attack? URL: https://youtu.be/XBkzBrXlle0
43. Звіт 2025 Cyber Threat Report https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report
44. Савчук С.О. ДЕРЖАВНА ПОЛІТИКА ПРОТИДІЇ КАБЕРЗЛОЧИННОСТІ. https://hackyourmom.com/kibervijna/fishyngovi-kampaniyi-apt29-ta-apt35-analiz-klyuchovyh-atak/
45. Офіційний сайт COREWIN. Найбільші та найвідоміші кібератаки в історії https://corewin.ua/blog/biggest-cyber-attacks-in-history/
46. ESET. https://www.eset.com/ua/about/newsroom/press-releases/malware/reyting-internet-ugroz-ukraina-v-pyaterke-celey-programm-vymogateley/

47. Про План реалізації Стратегії кібербезпеки України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
48. Про основні засади забезпечення кібербезпеки України. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
49. Про захист персональних даних. Офіційний вебпортал парламенту України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
50. EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. EU Artificial Intelligence Act | Up-to-date developments and analyses of the EU AI Act. URL: https://artificialintelligenceact.eu (date of access: 08.06.2025).
51. ISO - International Organization for Standardization. URL: https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27001:ed-3:v1:en
52. ISO 55000:2024. ISO. URL: https://www.iso.org/standard/83053.html
53. Новини, статті, аналітика зі світу кібербезпеки – ІЖ "Кібербез". URL: https://cybersec.net.ua/images/2025/april/SSSCIP_CERT-UA_H2_2024_UA.pdf
54. CERT-UA. Офіційний сайт Держслужби спецзв'язку та захисту інформації. https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
55. Загальний регламент про захист даних (GDPR). https://gdpr-text.com/uk/
56. РЕГЛАМЕНТ ЄВРОПЕЙСЬКОГО ПАРЛАМЕНТУ І РАДИ (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу. https://zakon.rada.gov.ua/laws/show/984_008-16#Text
57. Szwed, R. (2016) Framing of the Ukraine-Russia Conflict in Online and Social Media. NATO Strategic Communications Centre of Excellence. Latvia, Riga. 131 p.
58. Media. McLuhan M. (1964), "Understanding Media. The extensions of man. McGraw-Hill", available at: https: https://design opendata.files. word press. com/2014/05/ understan ding-media-mcluhan.pdf (accessed: 07.09.2025).
59. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 28.08.2025).
60. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.
61. Рева Т. Гібридні загрози та гібридні війни: сутність та аспекти взаємодії. Вісник Львівського університету. Серія філос.-політолог. студії. 2022. Випуск 40, с.Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 40, p. 186–191.
62. Національна стійкість України: стратегія відповіді на виклики та випередження гібридних загроз: національна доповідь / ред. кол. С. І. Пирожков, О. М. Майборода, Н. В. Хамітов, Є. І. Головаха, С. С. Дембіцький, В. А. Смолій, О. В. Скрипнюк, С. В. Стоєцький / Інститут політичних і етнонаціональних досліджень ім. І. Ф. Кураса НАН України. Київ, 2022. 552 с.
63. Schmid Johann. Der Archetypus hybrider Kriegführung. Hybride Kriegführung vs. Militärisch zentrierte Kriegführung. In: Österreichische Militärische Zeitschrift (ÖMZ), 2020. Heft 5/2020, P. 570–579.
64. Бєляков К.І. Інформація в праві: теорія і практика. Монографія. – Київ: Видавництво "КВІЦ", 2006. – 116 с.; 1 іл. https://ippi.org.ua/sites/default/files/informaciya_v_prave.pdf
65. Курбан О. (2015). Theory of information warfare: basic framework, methodology and conceptual apparatus. ScienceRise. 11. 95. 10.15587/2313-8416.2015.53940

ПОЛІТИКА КУРСУ

- 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 зазначений 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

Форми контролю	Види навчальної роботи	* Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на лекціях,*** *у т.ч.:*	
	• ведення конспекту	за кожну лекцію 0,5 бала
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	Робота на практичних заняттях, *у т.ч.:*	
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді)	за кожну презентацію максимум 4 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 2 бали
РУБІЖНЕ ОЦІНЮВАННЯ (контроль знань)	Контроль знань № 1	за кожне правильно виконане завдання максимальна оцінка – 30 балів
	Контроль знань № 2	за кожне правильно виконане завдання

		максимальна оцінка – 30 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Згідно рішення кафедри
ПІДСУМКОВЕ ОЦІНЮВАННЯ *залік*	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у формі тестування	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 (A)
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 (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 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	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

	формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з 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 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 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 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