

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

Лектор курсу			Легомінова Світлана Володимирівна доктор економічних наук, професор.		Контактна інформація лектора (e-mail), сторінка курсу в Google Class		e-mail: s.legominova@duikt.edu.ua ; сторінка курсу в Google Class – https://classroom.google.com/r/ODA1NTY0Nzc0NTA1/sort-last-name	
Галузь знань			F «Інформаційні технології»		Рівень вищої освіти		бакалавр	
Спеціальність			F2 Інженерія програмного забезпечення		Семестр		1	
Освітня програма			Інженерія програмного забезпечення		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		Безпека розробки програмного забезпечення	
Мета курсу:	сформувати базис знань та вмінь щодо забезпечення інформаційної та кібербезпеки із урахуванням сьогочасних небезпек у кіберпросторі та кваліфіковано застосовувати засоби забезпечення КБ		

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)				Hard-skills / Спеціальні (фахові, предметні) компетентності (СК)				
ЗК 3. Здатність спілкуватися державною мовою як усно, так і письмово. ЗК 6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел. ЗК11. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.				СК6. Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки).				

Програмні результати навчання (ПР)

ПРН 4. Знати і застосовувати професійні стандарти і інші нормативно-правові документи в галузі інженерії програмного забезпечення. ПРН 10. Проводити передпроектне обстеження предметної області, системний аналіз об'єкта проектування. ПРН 21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.								
--	--	--	--	--	--	--	--	--

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	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 <u>Рекомендовані джерела:</u> 1-9			
Заняття 1.1 Основи кібербезпеки та захисту інформації: розуміння, роль, термінологічний базис, загрози безпеки даних.	Лекція 1 2 год		Пояснювально-ілюстративний матеріал, лекція-візуалізація
Заняття 1.2. Основи кібербезпеки та захисту інформації: розуміння, роль, термінологічний базис, загрози безпеки даних.	Практичне заняття 1 2 год	2 бали	Усне опитування, експрес-опитування (на платформі Kahoot), навчальна дискусія
Тема 2. Інформаційні ресурси. Роль інформаційних ресурсів та їх захист в цифровому суспільстві <u>Рекомендовані джерела:</u> 1–2			
Заняття 2.1 Інформаційні ресурси. Роль інформаційних ресурсів та їх захист в цифровому суспільстві	Лекція 2 2 год		Пояснювально-ілюстративний матеріал, лекція-візуалізація
Заняття 2.2. Інформаційні ресурси. Роль інформаційних ресурсів та їх захист в цифровому суспільстві	Практичне заняття 2 2 год	0,5 бала	Усне опитування, виконання завдань на платформі GWSforE
Тема 3. Загрози інформаційній безпеці та кібербезпеці, їх аналіз <u>Рекомендовані джерела:</u> 1;_16-22			
Заняття 3.1 Загрози інформаційній безпеці та кібербезпеці, їх аналіз	Лекція 3 2 год		Пояснювально-ілюстративний матеріал, лекція-візуалізація
Заняття 3.2. Загрози інформаційній безпеці та кібербезпеці, їх аналіз	Практичне заняття 3 2 год	2 бали	Усне опитування, виконання завдань на платформі GWSforE, експрес-опитування (на платформі Kahoot)
Тема 4. Безпека даних <u>Рекомендовані джерела:</u> 22-31			
Заняття 4.1 Безпека даних	Лекція 4 2 год		Пояснювально-ілюстративний матеріал, лекція-візуалізація
Заняття 4.2. Безпека даних	Практичне заняття 4 2 год	2 бали	Усне опитування, виконання завдань на платформі GWSforE. Опитування, обговорення за матеріалами від НБУ та «Талан» (участь у марафоні із платіжної безпеки). Мета заходів: навчити розпізнавати шахрайські схеми й

			формувати навички безпечної поведінки у сфері платіжних послуг.
Тема 5. Законодавство та стандарти кібербезпеки <i>Рекомендовані джерела:</i> 5; 46-56			
Заняття 5.1 Законодавство та стандарти кібербезпеки.	Лекція 5 2 год		Пояснювально-ілюстративний матеріал, лекція-візуалізація, бліц опитування
Заняття 5.2. Законодавство та стандарти кібербезпеки Контроль знань №1	Практичне заняття 5 2 год	2 бали	Усне опитування
		30 балів	Контроль знань 1 (тест)
Самостійна робота			
<i>Тема 1. Основи кібербезпеки та захисту інформації: розуміння, роль, термінологічний базис, загрози безпеки даних</i> <i>Тема 2. Інформаційні ресурси. Роль інформаційних ресурсів та їх захист в цифровому суспільстві</i> <i>Тема 3. Загрози інформаційній безпеці та кібербезпеці, їх аналіз</i> <i>Тема 4. Безпека даних</i> <i>Тема 5. Законодавство та стандарти кібербезпеки</i>	6 год	0 балів	1. Опрацювати матеріали за питаннями лекції, використовуючи наведену до теми літературу, поглибити знання
	6 год	0,5 бала	2. Розглянути теорії інформації, визначити її суть та роль у кібербезпеці та захисті інформації.
	6 год	1 бал	3. Ознайомитися та опрацювати основні положення Стратегії інформаційної безпеки (глобальні та національні виклики інформаційної безпеки)
	6 год	2 бали	4. Перегляд відеоматеріалів для закріплення інформації за темою 4 (посилання на платформі GWSforE): 1) Що таке персональні дані? І Онлайн-курс «Захист персональних даних» 2) Суб'єкти обробки персональних даних І Захист персональних даних. Спеціалізований курс 3) Підстави для обробки персональних даних І Захист персональних даних 4) Як реалізувати право на поінформованість про обробку персональних даних? 5) Що таке право на заперечення проти обробки персональних даних? І «Захист персональних даних»
	6 год	0 балів	5. Закріплення знань за нормативно-правовим забезпеченням (розглянутим на лекційному занятті), яким регулюється питання забезпечення кібербезпеки та захисту інформації. Висновки щодо повноти та охоплення законодавством регуляції захисту інформації та

			кібербезпеки в Україні (формат представлення результатів опрацювання завдання - усний (опитування)).
Розділ 2. Практичні аспекти управління кібербезпекою та захистом інформації			
Тема 6. Безпека в інтернеті <i>Рекомендовані джерела:</i> 4; 32-39			
Заняття 6.1 Безпека в інтернеті.	Лекція 6 2 год		Пояснювально-ілюстративний матеріал, лекція-візуалізація
Заняття 6.2. Безпека в інтернеті	Практичне заняття 6 2 год	1 бал	Усне опитування, виконання завдань на платформі GWSforE (перевірка безпеки сайтів.; сервіси перевірки безпеки сайтів; сервіси перевірки файлів).
Тема 6. Безпека в інтернеті (продовження) <i>Рекомендовані джерела:</i> 32-39			
Заняття 7.1 Безпека в інтернеті	Лекція 7 2 год		Пояснювально-ілюстративний, лекція-візуалізація
Заняття 7.2. Безпека в інтернеті	Практичне заняття 7 2 год	1 бал	Усне опитування, виконання завдань з налаштування безпеки та перевірки персональних налаштувань на пристроях
Тема 7. Соціальна інженерія. Фішинг. Кібершахрайство <i>Рекомендовані джерела:</i> 6; 40-45			
Заняття 8.1 Соціальна інженерія. Фішинг. Кібершахрайство	Лекція 8 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 8.2. Соціальна інженерія. Фішинг. Кібершахрайство	Практичне заняття 8 2 год	4 бали	Усне опитування, виконання завдань на практичне застосування знань і вмінь.
Тема 8. Інформаційна та кібербезпека в умовах гібридної війни: протидія інформаційно-когнітивним загрозам <i>Рекомендовані джерела:</i> 57-64			
Заняття 9.1 Інформаційна та кібербезпека в умовах гібридної війни: протидія інформаційно-когнітивним загрозам	Лекція 9 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 9.2. Інформаційна та кібербезпека в умовах гібридної війни: протидія інформаційно-когнітивним загрозам. Контроль знань №2	Практичне заняття 9 2 год	1 бал	Усне опитування
		40 балів	Контроль знань 2 (тест)

Самостійна робота			
Тема 6. Безпека в інтернеті	12 год	1 бал	6. Глобальні запити щодо особистих даних користувачів. Провести аналіз для України (за запитами щодо особистих даних користувачів Google з України)
		5 балів	6.1. Основні правила безпеки в інтернеті, які допоможуть захистити свої дані від хакерів. Прослухати курс. По завершенню пройти фінальний тест та прикріпити сертифікат (на платформі GWSforE).
Тема 7. Соціальна інженерія. Фішинг. Кібершахрайство	6 год	5 балів	7. Кібергігієна: як захиститися від фішингу. Огляд сучасних методів фішингу й рекомендації, як їм протистояти та як карати шахраїв. Ознайомитися із матеріалами відео. Пройти тест, по завершенню прикріпити сертифікат (на платформі GWSforE).
Тема 8. Інформаційна та кібербезпека в умовах гібридної війни: протидія інформаційно-когнітивним загрозам	6 год	0 балів	8. Опрацювати матеріали за питаннями лекції, використовуючи наведену до теми літературу, поглибити знання

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проєктор;
- Комп'ютерний клас для проведення практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Матеріали на платформі Google Workspace for Education з дисципліни «ОКБЗІ» для студентів спеціальності F2 «Інженерія програмного забезпечення» <https://classroom.google.com/c/ODA1NTY0Nzc0NTA1>
2. Легомінова С., Якименко Ю., Мужанова Т., Капелюшна Т. 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>
3. Капелюшна Т., Мужанова Т., Берестяна, Т., Голобородько С., & Примаченко Д. 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>
4. 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>
5. 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
6. Капелюшна Т.В. Легомінова С.В., Тищенко В.С., Недодай М.Г., Дячук 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](https://doi.org/10.31673/2412-4338.2024.044748)
7. Ткаченко О.А, Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018, №1. С. 75-86.
8. Основи кіберпростору, кібербезпеки та кіберзахисту. Навч. посіб. / В. М. Богуш, В. В. Богуш, В. Д. Бровко, В. П. Настратин; під. ред. В. М. Богуша. — К.: Видавництво Ліра-К, 2020. — 554 с.
9. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
10. 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.

11. 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
12. 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>
13. Ткаченко О.А., Ткаченко К.О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018, №1. С. 75-86.
14. 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.
15. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
16. 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.
17. 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)
18. 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
19. С. В. Добринь, Д. С. Шкляр, ВИЗНАЧЕННЯ СУТНОСТІ ТА ВЗАЄМОЗВ'ЯЗКУ ПОНЯТЬ "РИЗИК", "НЕБЕЗПЕКА" ТА "ЗАГРОЗА". АГРОСВІТ № 9, 2017. С48-52/
20. Saveliyeva, 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>
21. Стратегія інформаційної безпеки <https://zakon.rada.gov.ua/laws/show/685/2021#n2>
22. 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-ocinky-vplyvu-v-systemah-upravlinnya-informacziynoi-bezpeky-pryklad-z-industriyi-it-konsaltingu-chastyna-2/>
23. 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
24. Що таке персональні дані? І Онлайн-курс «Захист персональних даних» <https://www.youtube.com/watch?v=aU-y23I74Og>
25. Суб'єкти обробки персональних даних І Захист персональних даних. Спеціалізований курс. <https://www.youtube.com/watch?v=dXyTfbl2JA>
26. Підстави для обробки персональних даних І Захист персональних даних. <https://www.youtube.com/watch?v=IAXt5YxzA8c>
27. Як реалізувати право на поінформованість про обробку персональних даних? https://www.youtube.com/watch?v=Ao3_jME5M-8
28. Що таке право на заперечення проти обробки персональних даних? І «Захист персональних даних» <https://www.youtube.com/watch?v=UCClhs9mRMI>
29. Microsoft Authenticator. <https://support.microsoft.com/uk-ua/account-billing/%D0%BF%D1%80%D0%BE-microsoft-authenticator-9783c865-0308-42fb-a519-8cf666fe0acc>
30. 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>
31. CASES – Creative industries social media. CASES. URL: <https://cases.media/en/cookie?srsId=AfmBOorGVc8kph-ODmwt5sqcGCiRELYiM3bwy9QdW8NeRuDtCSZX0dYd>
32. 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>
33. Перевірка сайту по URL. «Безпечний перегляд: статус сайту» <https://transparencyreport.google.com/safe-browsing/search>
34. BRAMA/ <https://stopfraud.gov.ua/guide>
35. Захистіть корпоративне середовище від кіберзагроз. https://www.eset.com/ua/business/enterprise/?srsId=AfmBOorJYq7EoBgxAVPZhJSQ_i9smWDAEoXPzWak88lEoghGcf6n_TN1#threat-intelligence
36. Безпека Ваших пристроїв: <https://dovidka.info/kiberbezpeka/>
37. Принципи запровадження кіберкультури: <https://moz.gov.ua/uk/principi-zaprovadzhennya-kiberkulturi>
38. 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
39. Особиста кібербезпека: захист персональних пристроїв: <https://mod.gov.ua/explanation/osobista-kiberbezpeka-zahist-personalnih-pristroyiv>

40. Особиста кібербезпека: паролі та месенджери: <https://mod.gov.ua/osobista-kiberbezpeka-paroli-ta-mesendzheri>
41. Phishing Explained In 6 Minutes | What Is A Phishing Attack? URL: <https://youtu.be/XBkzBrXlle0>
42. Звіт 2025 Cyber Threat Report <https://www.sonicwall.com/resources/white-papers/2025-sonicwall-cyber-threat-report>
43. Савчук С.О. ДЕРЖАВНА ПОЛІТИКА ПРОТИДІЇ КАБЕРЗЛОУЧИННОСТІ. <https://hackyourmom.com/kibervijna/fishyngovi-kampaniyi-apt29-ta-apt35-analiz-klyuchovyh-atak/>
44. Офіційний сайт COREWIN. Найбільші та найвідоміші кібератаки в історії <https://corewin.ua/blog/biggest-cyber-attacks-in-history/>
45. ESET. <https://www.eset.com/ua/about/newsroom/press-releases/malware/reyting-internet-ugroz-ukraina-v-pyaterke-celey-programm-vymogateley/>
46. Про План реалізації Стратегії кібербезпеки України. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text>
47. Про основні засади забезпечення кібербезпеки України. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
48. Про захист персональних даних. Офіційний вебпортал парламенту України. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
49. 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).
50. ISO - International Organization for Standardization. URL: <https://www.iso.org/obp/ui/ru/#iso:std:iso-iec:27001:ed-3:v1:en>
51. ISO 55000:2024. ISO. URL: <https://www.iso.org/standard/83053.html>
52. Новини, статті, аналітика зі світу кібербезпеки – ІЖ "Кібербез". URL: https://cybersec.net.ua/images/2025/april/SSSCIP_CERT-UA_H2_2024-UA.pdf
53. CERT-UA. Офіційний сайт Держслужби спецзв'язку та захисту інформації. <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv>
54. Загальний регламент про захист даних (GDPR). <https://gdpr-text.com/uk/>
55. 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
56. Szwed, R. (2016) Framing of the Ukraine-Russia Conflict in Online and Social Media. NATO Strategic Communications Centre of Excellence. Latvia, Riga. 131 p.
57. Media. McLuhan M. (1964), "Understanding Media. The extensions of man. McGraw-Hill", available at: <https://design.opendata.files.wordpress.com/2014/05/understanding-media-mcluhan.pdf> (accessed: 07.09.2025).
58. 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).
59. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. : НІСД, 2014. – 328 с.
60. 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.
61. 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.
62. Schmid Johann. Der Archetypus hybrider Kriegführung. Hybride Kriegführung vs. Militärisch zentrierte Kriegführung. In: Österreichische Militärische Zeitschrift (ÖMZ), 2020. Heft 5/2020, P. 570–579.
63. Беляков 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
64. Курбан О. (2015). Theory of information warfare: basic framework, methodology and conceptual apparatus. ScienceRise. 11. 95. 10.15587/2313-8416.2015.53940

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 виконання всіх практичних робіт і виконання самостійних завдань, які передбачені структурою освітньої компоненти.

Якщо студента не допущено до складання заліку, як такого, що не виконав індивідуальний план, йому надається час до перескладання для виконання всіх вимог допуску. Студент має право на два перескладання. При повторному перескладанні екзамену його у студента може приймати комісія, яка створюється директором ННІТ. Оцінка комісії є остаточною. У випадку отримання студентом 0 балів (неприйнятно), що тягне відрахування за невиконання навчального плану.

Оцінювання студентів здійснюється за накопичувальною 100-бальною системою і складається із оцінкових блоків: бали напрацьовані впродовж семестру на практичних заняттях та за виконання самостійної роботи студента – 30 б.; контроль знань 1 - 30 б. та контроль знань 2 – 40 б.

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	Виконання практичних робіт	15,5 балів
	Самостійна робота	14,5 балів
	Контроль знань 1	30 балів
	Контроль знань 2	40 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ <i>Залік</i>	Залік (складається із оцінкових блоків: бали напрацьовані впродовж семестру на практичних заняттях та за виконання самостійної роботи студента – 30 б.; контроль знань 1 - 30 б. та контроль знань 2 – 40 б.)	100 балів

Додаткова оцінка

Види навчальної роботи	Оцінювання
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 балів.

Додаткова оцінка

Види навчальної роботи	Оцінювання
Участь у наукових конференціях, підготовка наукових публікацій за тематикою освітньої компоненти:	
- Тези доповіді на фаховій конференції	3 бали
- Стаття у фаховому виданні	5 балів
- Стаття в іноземному рецензованому виданні	10 балів

Максимальна кількість додаткових балів, які можуть бути зараховані здобувачу освіти - 10 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 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 (С)
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 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 відсутня.	Низький Не забезпечує практичної реалізації задач, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) <i>В залікову книжку не представляється</i>
0-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену/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 представляється</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.