СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ОСНОВИ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Легомінова Світлана Володимирівна, доктор економічних наук, професор.</td><td>Контактна інформація лектора (e-mail), сторінка курсу в Google Classroom</td><td colspan="2">e-mail: s.legominova@duikt.edu.ua
сторінка курсу в Google Classroom – https://classroom.google.com/c/NzIxMjE5NjkzMjgy?cjc=3tqvxdw</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">12 Інформаційні технології</td><td>Рівень вищої освіти</td><td colspan="2">бакалавр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">124 Системний аналіз</td><td>Семестр</td><td colspan="2">3</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">Системний аналіз</td><td>Тип дисципліни</td><td colspan="2">Обов’язкова</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="5">За видами занять:</td></tr>
<tr><td>3</td><td>90</td><td>Лекцій
18</td><td>Семінарських занять
-</td><td>Практичних занять
18</td><td>Лабораторних занять</td><td>Самостійна підготовка
54</td></tr>
<tr><td colspan="9">АНОТАЦІЯ КУРСУ</td></tr>
<tr><td colspan="9">Взаємозв’язок у структурно-логічній схемі</td></tr>
<tr><td colspan="3">Освітні компоненти, які передують вивченню</td><td colspan="6">1. Основи телекомунікацій.</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6">1. Інформаційні мережі
2.Основи системного аналізу
3. Аналіз та застосування технологій програмуваня</td></tr>
<tr><td>Мета курсу:</td><td colspan="8">надати систематизовані знання щодо формування у здобувачів базових теоретичних знань, необхідних для забезпечення цілісного уявлення щодо управління інформаційною та кібербезпекою; набуття студентами основних навиків щодо захисту інформаційних систем.</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="4">Soft- skills / Загальні компетентності (ЗК)</td><td colspan="5">Hard-skills / Спеціальні компетентності (СК)</td></tr>
<tr><td colspan="4">ЗК 2. Здатність застосовувати знання у практичних ситуаціях.</td><td colspan="5">ПК6. Здатність до комп’ютерної реалізації математичних моделей реальних систем і процесів; проектувати, застосовувати і супроводжувати програмні засоби моделювання, прийняття рішень, оптимізації, обробки інформації, інтелектуального аналізу даних.
ПК8. Здатність організовувати роботу з аналізу та проектування складних систем, створення відповідних інформаційних технологій та програмного забезпечення.
ПК13. Здатність організовувати роботу з проектування, розробки, впровадження., використання і супроводу сучасних інфокомунікаційних систем на основі технологій комп’ютерних систем та мереж, штучного інтелекту, Інтернету речей та захисту інформації.</td></tr>
<tr><td colspan="9">Програмні результати навчання (ПР)</td></tr>
<tr><td colspan="9">ПРН 8. Володіти сучасними методами розробки програм і програмних комплексів та прийняття оптимальних рішень щодо складу програмного забезпечення, алгоритмів процедур і операцій.
ПРН 20. Знати основні поняття та методи організації захисту інформації в інфокомунікаційних системах.</td></tr>
</table>

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. Концептуальні основи інформаційної та кібербезпеки ***Формування компетентностей:*** **ЗК 2, ПК8**. ***Програмні результати навчання:*** **ПРН 20.** ***Рекомендовані джерела: 1-3***			
Заняття 1.1 Концептуальні основи інформаційної та кібербезпеки	Лекція 1.1 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 1.2. Основні концепції інформаційної та кібербезпеки.	Практичне заняття 1.2 2 год	8 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Тема 2. Нормативно-правова база в основах інформаційної безпеки та кібербезпеки ***Формування компетентностей:*** **ЗК 2, ПК8.** ***Програмні результати навчання:*** **ПРН 20.** ***Рекомендовані джерела: 4-6***			
Заняття 2.1 Нормативно-правова база в основах інформаційної безпеки та кібербезпеки	Лекція 2.1 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 2.2. Міжнародні стандарти в основах інформаційної безпеки та кібербезпеки. Національне законодавство в основах інформаційної безпеки та кібербезпеки	Практичне заняття 2.2 2 год	9 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Тема 3. Організаційні аспекти в основах управління інформаційною та кібернетичною безпекою ***Формування компетентностей:*** **ЗК 2, ПК8*, ПК13.*** ***Програмні результати навчання:*** **ПРН 20.** ***Рекомендовані джерела: 7-9***			
Заняття 3.1 Організаційні аспекти в основах управління інформаційною та кібернетичною безпекою.	Лекція 3.1 4 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування

Заняття 3.2. Структура служб безпеки в управлінні інформаційною та кібернетичною безпекою. Процеси управління інформаційною та кібернетичною безпекою	Практичне заняття 3.2 4 год	15 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Тема 4. Технічні засоби у сфері інформаційної та кібербезпеки ***Формування компетентностей:*** **ЗК 2, ПК6, ПК8, *ПК13.*** ***Програмні результати навчання:*** **ПРН 8, ПРН 20.** ***Рекомендовані джерела: 10-12***			
Заняття 4.1 Технічні засоби у сфері інформаційної та кібербезпеки	Лекція 4.1 4 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 4.2. Засоби захисту інформації в сфері інформаційної та кібербезпеки. Системи управління інцидентами у сфері інформаційної та кібербезпеки.	Практичне заняття 4.2 4 год	15 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Тема 5. Людський фактор у концепції інформаційної та кібербезпеки ***Формування компетентностей:*** **ЗК 2, ПК8, *ПК13.*** ***Програмні результати навчання:*** **ПРН 20.** ***Рекомендовані джерела: 13-15***			
Заняття 5.1 Людський фактор у концепції інформаційної та кібербезпеки	Лекція 5.1 2 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 5.2. Обізнаність персоналу у сфері інформаційної та кібербезпеки. Управління ідентифікацією та доступом до інформаційних ресурсів.	Практичне заняття 5.2 2 год	8 балів	Усне опитування, виконання завдань на практичне застосування знань і вмінь
Тема 6. Перспектива розвитку управління інформаційною та кібербезпекою ***Формування компетентностей:*** **ЗК 2, ПК6, *ПК13.*** ***Програмні результати навчання:*** **ПРН 8, ПРН 20.** ***Рекомендовані джерела: 16-18***			
Заняття 6.1 Перспектива розвитку управління інформаційною та кібербезпекою	Лекція 6 4 год		Пояснювально-ілюстративний, лекція-візуалізація, бліц опитування
Заняття 6.2. Штучний інтелект та машинне навчання в концепції інформаційної та кібербезпеки. Хмарні технології у сфері інформаційної та кібербезпеки.	Практичне заняття 4 год	15 балів	Усне опитування, виконання завдань на практичне застосуван знань і вмінь

Самостійна робота			
Тема 1. Концептуальні основи інформаційної та кібербезпеки		5 балів	Виконання рефератів за обраною темою
Тема 2. Нормативно-правова база в основах інформаційної безпеки та кібербезпеки		5 балів	Виконання рефератів за обраною темою
Тема 3. Організаційні аспекти в основах управління інформаційною та кібернетичною безпекою		5 балів	Виконання рефератів за обраною темою
Тема 4. Технічні засоби у сфері інформаційної та кібербезпеки		5 балів	Виконання рефератів за обраною темою
Тема 5. Людський фактор у концепції інформаційної та кібербезпеки		5 балів	Виконання рефератів за обраною темою
Тема 6. Перспектива розвитку управління інформаційною та кібербезпекою		5 балів	Виконання рефератів за обраною темою

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор.
- Комп'ютерний клас для проведення практичних занять з встановленими програмно-технічними комплексами AlienVault, Nessus, Kali Linux.
- Мережа Інтернет.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. *Часопис Київського університету права*. 2018. № 3. С. 235-239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54
2. Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. Основи кіберпростору, кібербезпеки та кіберзахисту. Київ.: Видавництво Ліра-К, 2020. 554 с. URL: https://jurkniga.ua/contents/osnovi-kiberprostoru-kiberbezpeki-ta-kiberzakhistu.pdf
3. Богуш В.М., Бровко В.Д., Кобус О.С., Козюра В.Д. Технічний захист інформації. Київ.: Видавництво Ліра-К, 2022, 286с. URL: https://knushop.com.ua/image/catalog/lira20230617/pdf/13054.pdf
4. Гребенюк А.М., Рибальченко Л.В. Основи управління інформаційною безпекою. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с. URL: https://er.dduvs.edu.ua/bitstream/123456789/5717/1/%d0%9f%d0%9e%d0%a1I%d0%91%d0%9d%d0%98%d0%9a%20%d0%9e%d0%a3I%d0%91%20.pdf
5. Костирко Т. М., Т. Д. Корольова Т. Д., Жигалкіна М. С. Основи медіаграмотності. Миколаїв : НУК, 2019.
6. Легомінова С.В., Мужанова Т.М., Якименко Ю.М., Щавінський Ю.В., Нестеренко Г.П. Розвиток політики кібербезпеки ЄС: підходи та рішення. *Кібербезпека: освіта, наука, техніка.* 2024. № 4 (24). С. 77-84. URL:https://csecurity.kubg.edu.ua/index.php/journal/article/view/577/469
7. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
8. Криворучко О.В., Звєрєв В.П., Десятко А.М. Кібергігієна. Кібербезпека. Безпека держави: : матеріали наукових семінарів. Київ : КНТЕУ, 2020, 101с. URL: https://knute.edu.ua/file/MjExMzA=/d8e24930571c0d91476be247343bb902.pdf

9. Lehominova S., Shchavinsky Y., Muzhanova T., Rabchun D., Zaporozhchenko M. Application of Sentiment Analysis to Prevent Cyberattacks on Objects of Critical Information Infrastructure. *International Journal of Computing*. 2023. Vol. 22(4). P. 534-540.
10. Kapeliushna T., Lehominova S., Goloborodko A., Lysetskyi Yu., Nosova T. Methodological approaches to enterprise security management: traditional and transformed to the conditions of functioning. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu.* 2024, (3): 204 – 209. URL: https://nvngu.in.ua/index.php/en/archive/on-the-issues/1909-2024/content-3-2024/6934-204 (SCOPUS)
11. Подільчак О., Дунаєва Т. Інформаційні методики кібербезпеки як складової інформаційної безпеки під час війни в україні. *Наукові інновації та передові технології. 2023. № 13(27). URL: https://doi.org/10.52058/2786-5274-2023-13(27)-329-341*
12. Obodiak V., Kotukh Y. Основні виклики урядування у сфері кібербезпеки. *Theory and practice of public administration.* 2020. Т. 4, № 71. С. 38–46. URL: https://doi.org/10.34213/tp.20.04.05
13. Savchenko, V., Lehominova, S., Dzyuba, T., Havryliuk, I., Novikova, I. Model of Connectivity in a Mobile MESH Network for a Group of Unmanned Aerial Vehicles. 2022 *IEEE 4th International Conference on Advanced Trends in Information Theory,* ATIT 2022 – Proceedings. 2022, pp. 142–147. (SCOPUS) URL: https://ieeexplore.ieee.org/document/10024235 https://www.scopus.com/authid/detail.uri?authorId=57217034683
14. Легомінова С.В., Гайдур Г.І. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. *Кібербезпека: освіта, наука, техніка.* 2023. № 2 (22). С. 57-64. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/535/4
15. Котляров В. Основні підходи у концепції інформаційної безпеки. *Актуальні питання у сучасній науці.* 2023. № 1(7). URL: https://doi.org/10.52058/2786-6300-2023-1(7)-474-484
16. Легомінова С.В., Щавінський Ю.В., Будзінський О.В. Аналіз сучасних підходів до забезпечення кібербезпеки корпоративних баз даних. *Сучасний захист інформації.* 2024. №2(58). С. 84-91. URL: https://journals.dut.edu.ua/index.php/dataprotect/article/view/2979/287
17. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-49
18. Lehominova S.V., Shchavinskyy YU.V., Muzhanova T.M., Dzyuba T.M., Rabchun D.I. Legal mechanisms for ensuring information security in Ukraine in the conditions of hybrid war. *Телекомунікаційні та інформаційні технології.* 2023. № 1 (78). С. 101-110. URL: https://tit.dut.edu.ua/index.php/telecommunication/article/view/2460/2342

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики. Спілкуючись з учасниками навчального процесу, студенти мають дотримуватися етичних норм, утримуватися від гучних проявів емоцій, бути політично коректними й толерантними, поважати звичаї й традиції різних етнічних, культурних, соціальних груп і релігійних конфесій.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій, практичних занять, а також самостійну роботу.
- Студенти зобов'язані відвідувати заняття за обраним і затвердженим індивідуальним навчальним планом та вчасно інформувати викладача про неможливість із поважних причин відвідувати заняття, бути присутніми на заліку.
- 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 із поважних причин був відсутній на практичному занятті, він має право його відпрацювати. Відпрацювання полягає у виконанні індивідуального завдання за прикладом, наданим викладачем. Якщо для виконання завдання необхідно використання обладнання лабораторій кафедри, тоді час відпрацювання оговорюється з викладачем індивідуально і погоджується з завідувачем відповідної лабораторії, де розміщено обладнання.
- 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.
- За 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 ”Основи кібербезпеки та захисту інформації”.

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 заліку його у студента може приймати комісія, яка створюється директором ННІІТ. 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.

Для отримання додаткових балів, студент повинен надати копію друкованої публікації чи письмове повідомлення видавця, про прийняття до друку публікації. Тематика публікації повинна відповідати змісту освітньої компоненти ”Основи кібербезпеки та захисту інформації”і тільки в цьому випадку додаткові бали будуть зараховані. При пред’явленні публікації студент звільняється від виконання практичної роботи, тема якої відповідає тематиці публікації, при цьому студенту зараховується додаткові бали замість балів за виконання суміжних за тематикою практичних робіт. Максимальна кількість додаткових балів, що можуть бути зараховані за дисципліну – 10 балів.

Форми контролю	**Види навчальної роботи**	**Оцінювання**
ПОТОЧНИЙ КОНТРОЛЬ	● Виконання практичних робіт	70 балів
	● Самостійна робота	30 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Залік проходить в усній формі.	Згідно критеріїв оцінювання

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	**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	Відмінно / Зараховано (А)

	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.	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 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 формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни.	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни.	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*

1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену/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 заліковку книжку не проставляється*

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.