СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«КРАЩІ ПРАКТИКИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Тищенко Віталій Сергійович
асистент кафедри управління інформаційною та кібербезпекою</td><td colspan="2">Контактна інформація лектора (e-mail), сторінка курсу в Google Classroom</td><td colspan="2">e-mail: v.tyshchenko@duikt.edu.ua;
сторінка курсу в Google Classroom – https://classroom.google.com/c/NzE5OTA2MDMxNDE2?hl=ru&cjc=ezhugjy</td></tr>
<tr><td colspan="3">Галузь знань</td><td colspan="2">F «Інформаційні технології»</td><td colspan="2">Рівень вищої освіти</td><td colspan="2">бакалавр</td></tr>
<tr><td colspan="3">Спеціальність</td><td colspan="2">F5 «Кібербезпека та захист інформації»</td><td colspan="2">Семестр</td><td colspan="2">6</td></tr>
<tr><td colspan="3">Освітня програма</td><td colspan="2">«Управління інформаційною та кібернетичною безпекою»</td><td colspan="2">Тип дисципліни</td><td colspan="2">Вибіркова</td></tr>
<tr><td rowspan="2">Обсяг:</td><td>Кредитів ECTS</td><td>Годин</td><td colspan="6">За видами занять:</td></tr>
<tr><td>5</td><td>150</td><td>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td colspan="3"></td><td></td><td>-</td><td>56</td><td>-</td><td>94</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">Компонента вільного вибору студента</td></tr>
<tr><td colspan="3">Освітні компоненти для яких є базовою</td><td colspan="6"></td></tr>
<tr><td>Мета курсу:</td><td colspan="8">набуття студентами компетенцій, знань, умінь і навичок щодо використання іноземної мови у сфері управління інформаційною безпекою з метою подальшого використання зазначених знань та навиків у подальшій практичній діяльності</td></tr>
<tr><td colspan="9">Компетентності відповідно до освітньої програми</td></tr>
<tr><td colspan="5">Загальні компетентності (ЗК)</td><td colspan="4">Спеціальні (фахові, предметні) компетентності (СК)</td></tr>
<tr><td colspan="5">ІК. Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.
ЗК4. Здатність спілкуватися іноземною мовою.</td><td colspan="4">.</td></tr>
<tr><td colspan="9">Програмні результати навчання (РН)</td></tr>
<tr><td colspan="9">РН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних проблему професійній діяльності, оцінювати їхню ефективність.</td></tr>
</table>

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Тема 1. ***Система управління інформаційною безпекою (СУІБ)*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою;2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ІК, ЗК4 ***Результати навчання:*** РН 2. ***Рекомендовані джерела:*** 1-6, 7-12.	Практичне заняття 1 2 год Практичне заняття 2 2 год Практичне заняття 3 2 год Практичне заняття 4 2 год Практичне заняття 5 2 год	5,5	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 2***. Загрози та вразливості інформаційній безпеці організації*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом ***Формування компетенцій:*** ІК, ЗК4 ***Результати навчання:*** РН 2.	Практичне заняття 6 2 год Практичне заняття 7 2 год Практичне заняття 8 2 год Практичне заняття 9 2 год Практичне заняття 10 2 год	5,5	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми

Тема 3. ***Управління ризиками інформаційної безпеки*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ІК, ЗК4 ***Результати навчання:*** РН 2. ***Рекомендовані джерела:*** 1-6, 7, 10.	Практичне заняття 11 2 год Практичне заняття 12 2 год Практичне заняття 13 2 год Практичне заняття 14 2 год Практичне заняття 15 2 год	5,5	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 1. Моделі зрілості управління інформаційною безпекою (O-ISM3,BPMMM, PCM, CCSMM) **Тема 2.** Класифікація загроз і вразливостей інформаційної безпекивідповідно до стандарту ISO 27005. **Тема 3**. Концепції управління ризиками NIST та COBIT.	Самостійна робота		1. Оцінка зрілості СУІБ на основі аналізу впроваджених процесів (O-ISM3). 2. Оцінка можливостей процесів, інтегрованих в IT організації (PCM). 3. Оцінка рівня реалізації процесів організації (BPMMM). 4. Порівняння зрілості різних організацій для координації спільних зусиль щодо забезпечення бажаного рівня безпеки (CCSMM). 5. Класифікація загроз ІБ відповідно до стандарту ISO 27005. 6. Класифікація вразливостей ІБ відповідно до стандарту ISO 27005. 7. Концепція управління ризиками NIST. Модель управління ризиками відповідно до стандарту COBIT
Тема 4. ***Безпека інформаційних активів організації*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом ***Формування компетенцій:*** ІК, ЗК4	Практичне заняття 16 2 год Практичне заняття 17 2 год Практичне заняття 18 2 год	5,5	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми

Результати навчання: РН 2. ***Рекомендовані джерела:*** 1-6, 8, 11.	Практичне заняття 19 2 год Практичне заняття 20 2 год		
Тема 5. ***Розробка та впровадження політики інформаційної безпекиорганізації*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ІК, ЗК4 ***Результати навчання:*** РН 2. ***Рекомендовані джерела:*** 1-6, 7-9.	Практичне заняття 21 2 год Практичне заняття 22 2 год Практичне заняття 23 2 год Практичне заняття 24 2 год	5,5	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 6. ***Внутрішня організація ІБ. Безпека дистанційної роботи тамобільних пристроїв*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою;2.спілкуватися на зазначену тему; 3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ІК, ЗК4 ***Результати навчання:*** РН 2. ***Рекомендовані джерела:*** 1-6, 7-9.	Практичне заняття 25 2 год Практичне заняття 26 2 год Практичне заняття 27 2 год Практичне заняття 28 2 год	5,5	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе з теми Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 4. Класифікація інформації обмеженого доступу наорганізаційному та урядовому рівні: досвід інших держав. **Тема 5**. Законодавство про безпеку даних США та ЄС. **Тема 6.** Ієрархія внутрішньо організаційної документації з ІБ та вимоги до їх розробки.	Самостійна робота		1. Види урядової інформації обмеженого доступу на рівні організації та Уряду у США. 2. Види конфіденційної інформації, яка може оброблятися організацією. 3. Положення Загального регламенту захисту даних ЄС (GDPR 4. Персональні дані. Захист персональних даних. 5. Захист прав інтелектуальної власності.

			6. Види кіберзлочинів відповідно до законодавства США та ЄС. 7. Етапи і структура загально організаційної політики ІБ. Вимоги до розробки організаційних процедур та інструкцій зІБ.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп‘ютерне обладнання, мережа Інтернет, мультимедійний проєктор, 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. Pauline Bowen, Joan Hash, Mark Wilson. Information Security Handbook: A Guide for Managers, NIST, 178 p. http://www.dut.edu.ua/uploads/l_1889_44919882.pdf
2. Tony Campbell, Burns Beach. Practical Information Security Management: A Complete Guide to Planning and Implementation. Apress. 237 p. http://www.dut.edu.ua/uploads/l_1888_50813661.pdf
3. Cybersecurity Fundamentals Study Guide, 2nd Edition. ISACA. 194 p. https://www.studocu.com/nl-be/document/odisee-hogeschool/cybersecurity- fundamentels/college-aantekeningen/cybersecurity-fundamentals-with-notes/7343872/view
4. OWASP Top 10. https://owasp.org/www-project-top-ten/
5. Information Security Management Handbook. Sixth Edition. Volume 7. Edited by Richard O’Hanley, James S. Tiller. CRC Press Taylor & Francis Group. 400 p.
6. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. National Institute of Standards and Technology, 2018. 48 p. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
8. ISO/IEC 27001:2022) Information technology - Security techniques - Information security management systems – Requirements. 34 p.
9. ISO/IEC 27002:2022 Information technology - Security techniques - Code of practice for information security controls. 80 p.
10. ISO/IEC 27005:2022 Information technology - Security techniques - Information security risk management. 55 p.
11. Мужанова Т.М., Стегнієнко А.Д. Організація інформаційної безпеки підприємства відповідно до стандарту ISO 27002. Збірник тез Всеукраїнської науково - практичної конференції «Цифрова трансформація кібербезпеки», м. Київ, 26 березня 2020 р. Державний університет телекомунікаці й. С.44. http://www.dut.edu.ua/uploads/p_1739_99516793.pdf
12 NIST Cybersecurity Framework (CSF) 2.0 . https://www.nist.gov/cyberframework

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 набрання студентом 30 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 відпрацюванняпройденого матеріалу)	за кожне відвідування 0,55 балу
	• опитування за результатами вивчення теми, перевірка знання фахової термінології	за кожну правильну

		відповідь 0,25 балу
	• доповідь з презентацією за темою, в тому числі вивченою самостійно (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якостіпрезентації і доповіді),	за кожну презентацію (реферат) максимум 3 бали
	• підготовка повідомлення, тез, ессе, анотації тощо	за кожну правильну відповідь 0,5 балу
	• участь у дискусії, обговоренні положень нормативних актів, статей, відеоматеріалів	за кожну правильну відповідь 2 бали
РУБІЖНЕ ОЦІНЮВАННЯ (КОНТРОЛЬ)	Модульний контроль № 1 «ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇБЕЗПЕКИ»	максимальна оцінка 15 балів
	Модульний контроль № 2 «ВНУТРІШНЯ ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка 15 балів
ДОДАТКОВА ОЦІНКА	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ Залік	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей,необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	30 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 вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені 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	**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 (В)

	проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.		
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)
40-59	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*
0-39	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*