СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Запорожченко Михайло Михайлович, асистент кафедри управління інформаційною та кібернетичною безпекою</td><td>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail: zaporozhchenkomm@gmail.com; сторінка курсу в Moodle – https://dn.dut.edu.ua/course/view.php?id=825</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">125 «Кібербезпека та захист інформації»</td><td>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>Тип дисципліни</td><td colspan="2">Основна</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>
</table>

АНОТАЦІЯ КУРСУ

Мета курсу:

- формування у студентів комплексного бачення сфери діяльності, пов’язаної з управлінням процесом забезпечення інформаційної безпеки підприємства (установи, організації);
- забезпечення усвідомлення студентами порядку та особливостей вирішення різних завдань управління інформаційною безпекою підприємства (установи, організації), їхнього кадрового та ресурсного забезпечення;
- здобуття теоретичних знань, умінь, навичок та інших компетентностей щодо різних аспектів менеджменту інформаційної безпеки (адміністративного, виробничого, кадрового, ресурсного).

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	Hard-skills / Фахові компетенції
ЗК 1. Здатність застосовувати знання у практичних ситуаціях. **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 4**. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації.	**ПП 1**. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки. **ПП 9**. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. **ПП 11**. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційнотелекомунікаційних (автоматизованих) систем. **ПП 12**. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресур

Програмні результати навчання (ПРН)

ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 4. Аналізувати, аргументувати, приймати рішення при розв’язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 7. Діяти на основі законодавчої та нормативноправової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
ПРН 28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.
ПРН 29. Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
ПРН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
ПРН 33. Вирішувати задачі забезпечення неперервності бізнес процесів організації.
ПРН 34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та кібербезпеки відповідно до цілей і завдань організації.
ПРН 43. Вирішувати задачі забезпечення неперервності бізнес процесів організації на основі встановленої системи управління інформаційною безпекою, згідно вітчизняних та міжнародних вимог і стандартів.
ПРН 44. Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
ЗМІСТОВИЙ МОДУЛЬ 1 "СЕРЕДОВИЩЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА"			
Тема 1. ***Середовище управління інформаційною безпекою підприємства (установи, організації)*** ***Знати***: процедури опису сфери діяльності та бізнес-процесів підприємства (установи, організації); систему вимог до інформаційної безпеки підприємства (установи, організації); порядок та особливості визначення та оцінювання загроз інформаційній безпеці підприємства (установи, організації); стандарти, порядок та особливості оцінювання ризиків інформаційної безпеки підприємства (установи, організації); порядок та особливості захисту персональних даних згідно національного законодавства України та GDPR; правові механізми захисту об'єктів інтелектуальної власності підприємства (установи, організації); сутність та зміст основних стандартів забезпечення інформаційної безпеки (кібербезпеки); ***Вміти***: оцінювати загрози та ризики інформаційної безпеки підприємства (установи, організації), визначати джерела загроз та ризиків; організувати моніторинг зовнішнього інформаційного простору в інтересах інформаційної безпеки підприємства (установи, організації); організувати контроль та внутрішній аудит стану інформаційної безпеки підприємства (установи, організації);	Лекція 1 2 год	5,5*	Лекція-візуалізація
	Практичне заняття 1 2 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 2 2 год		Лекція-візуалізація
	Практичне заняття 2 2 год		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 3 2 год	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 3 2 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
	Лекція 4 2 год		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 4		Усне опитування, навчальна дискусія, обговорення ситуаційного завдання

реагувати на факти дискредитації та негативну інформацію про діяльність підприємства (установи, організації); захищати репутацію підприємства (установи, організації); ***Формування компетенцій:*** ЗК 1, ЗК 2, ЗК 4, ЗК 5, ПП 1 ***Результати навчання:*** ПРН 3, ПРН 6, ПРН 7, ПРН 28 ***Рекомендовані джерела:*** *1-16*	2 год Лекція 5 2 год Практичне заняття 5 2 год		 Лекція-візуалізація, експрес-опитування студентів Тестування, навчальна дискусія, обговорення ситуаційного завдання
Тема 1. ***Середовище управління інформаційною безпекою підприємства (установи, організації)***	Самостійна робота		1. Міжнародні стандарти щодо заходів управління інформаційною безпекою 2. Характеристики захищеності інформаційних ресурсів 3. Модель CIA. Задачі забезпечення цілісності, доступності та конфіденційності 4. Бізнес-процеси підприємства (установи, організації) з точки зору інформаційної безпеки 5. Вимоги до забезпечення інформаційної безпеки підприємства (установи, організації) 6. Визначення та оцінювання загроз інформаційній безпеці підприємства (установи, організації) 7. Оцінювання ризиків інформаційної безпеки підприємства (установи, організації) 8. Система органів підприємства (установи, організації), призначена для забезпечення інформаційної безпеки 9. Політика інформаційної безпеки підприємства (установи, організації)
ЗМІСТОВИЙ МОДУЛЬ 2 " СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА"			
Тема 2. ***Управління інформаційною безпекою підприємства (установи, організації).*** ***Знати***: порядок створення та впровадження на підприємстві (в установі, організації) КСЗІ та СУІБ; зміст Політики інформаційної безпеки підприємства (установи, організації); сутність та порядок управління інцидентами інформаційної безпеки (кібербезпеки) підприємства (установи, організації); сутність та порядок проведення Державної експертизи та аудиту інформаційної безпеки підприємства (установи, організації). ***Вміти***: визначити та сформувати систему органів підприємства (установи, організації), необхідних для забезпечення інформаційної безпеки; здійснювати розмежування доступу до інформаційних активів; визначати необхідні заходи та засоби технічного та криптографічного захисту інформації; організовувати роботу з	Лекція 6 2 год Практичне заняття 6 2 год Лекція 7 2 год Практичне заняття 7 2 год Лекція 8 2 год Практичне заняття 8	5,5*	Лекція-візуалізація, експрес-опитування студентів Тестування, навчальна дискусія, обговорення ситуаційного завдання Лекція-візуалізація, експрес-опитування студентів Усне опитування, навчальна дискусія, обговорення ситуаційного завдання Лекція-візуалізація, експрес-опитування студентів Тестування, навчальна дискусія, обговорення ситуаційного завдання

персоналом з дотриманням вимог інформаційної безпеки; розраховувати ресурси, необхідні для забезпечення інформаційної безпеки підприємства (установи, організації). ***Формування компетенцій:*** ЗК 1, ЗК 2, ЗК 4, ЗК 5, ПП 1, ПП 9, ПП 11 ***Результати навчання:*** ПРН 3, ПРН 6, ПРН 7, ПРН 15, ПРН 18, ПРН 28, ПРН 29 ***Рекомендовані джерела:*** *1-16*	2 год		
	Лекція 9 2 год		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9 2 год		Тестування, навчальна дискусія, обговорення ситуаційного завдання
Тема 2. ***Управління інформаційною безпекою підприємства (установи, організації).***	Самостійна робота		1. Загальні правила управління безпекою підприємства 2. Система управління інформаційною безпекою 3. Функції технологічного управління інформаційною безпекою 4. Організація захисту інформації (інформаційних активів) підприємства (установи, організації) 5. Кадровий менеджмент інформаційної безпеки підприємства (установи, оргнаізації) 6. Ресурсний менеджмент інформаційної безпеки підприємства (установи, організації) 7. Управління інцидентами інформаційної безпеки підприємства (установи, організації) 8. Контроль стану та аудит інформаційної безпеки підприємства (установи, організації)

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять.
- Перелік питань для самостійної підготовки, перелік навчальної літератури та доступ до тексту лекцій та слайдів до лекцій через систему MOODLE для підготовки до практичних занять.
- Програма навчальної дисципліни, робоча програма навчальної дисципліни
- Білети до диференційованого заліку.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Рекомендовані джерела та інші навчальні ресурси:

1. Закон України «Про захист персональних даних». URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text
3. Закон України «Про авторське право і суміжні права». URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text;
4. Закон України «Про захист від недобросовісної конкуренції». URL: https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text;
5. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27 вересня 1999 року N 1229/99. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text;
6. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22 травня 1998 року N 505/98. URL: https://zakon.rada.gov.ua/laws/show/505/98#Text;

7. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені Постановою Кабінету Міністрів України від 29 березня 2006 р. N 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text;
8. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури, затверджені Постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text;
9. Накази Адміністрації ДССЗЗІ України, державні стандарти України та нормативні документи України у сфері технічного та криптографічного захисту інформації. URL: https://cip.gov.ua/ua/docs;
10. Міжнародні стандарти серії ISO/IEC 2700x:2018 «Information technology. Security techniques»;
11. Стандарт безпеки даних індустрії платіжних карток Payment Card Industry Data Security Standard (PCI DSS);
12. Стандарти інформаційної безпеки США NIST Special Publications 800 Series;
13. Відкритий IT-стандарт Асоціації з аудиту та контролю інформаційних система (ISACA) спільно із Інститутом управлінням IT (ITGI) CoBiT (Control Objectives for Information and Related Technology – «Контрольні цілі для інформаційних та суміжних технологій»);
14. Загальний регламент про захист даних ЄС GDPR (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679
15. Манжай О. В., Манжай І.А. Правові засади захисту інформації: підручник. – Харків : Панов, 2020. – 162 с. URL: http://univd.edu.ua/science-issue/issue/4315;
16. Менеджмент інформаційної безпеки : навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О .Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. Ніжин : ФОП Лук'яненко В.В. ТПК «Орхідея», 2019. 408 с. : іл. URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19244/%d0%9c%d0%b5%d0%bd%d0%b5%d0%b4%d0%b6%d0%bc%d0%b5%d0%bd%d1%82%20%d1%96%d0%bd%d1%84%d0%be%d1%80%d0%bc.%20%d0%b1%d0%b5%d0%b7%d0%bf.%20New%20booklet%201.pdf?sequence=1&isAllowed=y;

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 40 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 балу
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 балу
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти	за кожну презентацію (реферат) максимум 3 бали

	розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 балу
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 3 бали
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «СЕРЕДОВИЩЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА»	максимальна оцінка – 20 балів
	Модульний контроль № 2 «СИСТЕМА МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	максимальна оцінка – 20 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.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** /*запис в заліковій 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 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 (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.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни.	Добре / Зараховано (С)

	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.	Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	
64-74	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)
60-63	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 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*