СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«УПРАВЛІННЯ ПЕРСОНАЛОМ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

<table>
<tr><td colspan="3">Лектор курсу</td><td colspan="2">Мужанова Тетяна Михайлівна, кандидат наук з держ.упр., доцент кафедри управління інформаційною та кібербезпекою</td><td>Контактна інформація лектора (e-mail), сторінка курсу в Moodle</td><td colspan="2">e-mail:muzanovat@gmail.com;
сторінка курсу в Moodle –
http://dl.dut.edu.ua/course/view.php?id=1742</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</td><td>Семестр</td><td colspan="2">7</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">Вибіркова</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>5</td><td>150</td><td>Лекцій
-</td><td>Семінарських занять
-</td><td>Практичних занять
72</td><td>Лабораторних занять
-</td><td>Самостійна підготовка
78</td></tr>
</table>

АНОТАЦІЯ КУРСУ

Мета курсу:	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

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	Hard-skills / Спеціальні компетентності (СК(ПП))
ЗК 1. Здатність застосовувати знання у практичних ситуаціях **ЗК 2.** Знання та розуміння предметної області та розуміння професії. **ЗК 3.** Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово. **ЗК 6**. 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 і Україні. **ЗК 7.** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.	**ПП 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. **ПП 8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ПП 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам.

Програмні результати навчання (ПРН)

ПРН 1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.
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 8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.\
ПРН 12. Розробляти моделі загроз та порушника.
ПРН 23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
ПРН 26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
ПРН 35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 «БЕЗПЕКА ПЕРСОНАЛУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 1. ***Основні засади управління персоналом. Специфіка управління персоналом у сфері ІБ.*** ***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:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6, 11-13.	Практичне заняття 1 Практичне заняття 2 Практичне заняття 3 Практичне заняття 4 Практичне заняття 5	5,5*	Читання і переклад зі словником спеціалізованих текстів наукового та довідкового характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Розповідь, ведення дискусії на зазначену тему Підготовка повідомлень, ессе на тему «Управління персоналом: сучасні тренди», «Управління персоналом: специфіка у сфері ІБ» Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 2 ***Управління персоналом у сфері ІБ відповідно до стандарту ISO 27002*** ***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:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6, 8, 11-13.	Практичне заняття 6 Практичне заняття 7 Практичне заняття 8 Практичне заняття 9	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника Індивідуальні розповіді, ведення дискусії на зазначену тему Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми

Тема 3. ***Навчання і формування обізнаності персоналу з питань 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:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6, 11.	Практичне заняття 10 Практичне заняття 11 Практичне заняття 12 Практичне заняття 13	5,5*	Читання і переклад зі словником спеціалізованих текстів наукового та довідкового характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка анотацій статей з Інтернет-ресурсів про форми і методи навчання і формування обізнаності персоналу з питань інформаційної безпеки на тему Прослуховування спеціалізованих текстів за фахом, обговорення змісту почутого, вивчення лексики Опитування за результатами вивчення теми
Тема 4. ***Формування у персоналу корпоративної лояльності як основа ефективного забезпечення 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:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6, 13.	Практичне заняття 14 Практичне заняття 15 Практичне заняття 16 Практичне заняття 17 Практичне заняття 18	5,5*	Читання і переклад зі словником спеціалізованих текстів наукового та довідкового характеру за темою, вивчення спеціалізованої лексики Підготовка тез та повідомлень за темою Індивідуальні розповіді, ведення дискусії на зазначену тему Прослуховування спеціалізованих текстів за фахом, обговорення змісту та лексики Опитування за результатами вивчення теми Проведення модульного контролю № 1 «Безпека персоналу у сфері інформаційної безпеки»
Тема 1. Сутність та відмінності концепцій управління персоналом та управління людськими ресурсами. **Тема 2.** Засади розробки програми навчання та формування обізнаності персоналу з ІБ. **Тема 3**. Процедури підбору й оцінювання персоналу ІБ. **Тема 4**. Роль заходів стимулювання й мотивації персоналу в управлінні ІБ.	Самостійна робота		1. Управління людськими ресурсами: основні положення. 2. Порівняльна характеристики положень концепцій управління персоналом та управління людськими ресурсами. 3. Структура та етапи розробки програми навчання та формування обізнаності персоналу з ІБ. 4. Форми і види заходів навчання та формування обізнаності персоналу з ІБ. 4. Огляд спеціалізованого ПЗ з навчання та формування обізнаності персоналу у сфері ІБ. 5. Специфіка наймання й оцінювання персоналу у сфері ІБ. 6. Огляд спеціалізованого ПЗ з підбору й оцінювання персоналу ІБ.

			6. Заходи стимулювання й мотивації персоналу. 7. Передовий зарубіжний досвід стимулювання й мотивації персоналу з ІБ.
Розділ 2 «ВИМОГИ ДО МЕНЕДЖЕРА З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 5. ***Вимоги до менеджера з інформаційної безпеки: підходи експертних організацій (ISACA, NIST)*** ***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:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6, 10.	Практичне заняття 19 Практичне заняття 20 Практичне заняття 21 Практичне заняття 22 Практичне заняття 23 Практичне заняття 24	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного та наукового характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка повідомлень і доповідей щодо вимог до менеджера з інформаційної безпеки ISACA, NIST Проведення презентацій з результатами вивчення вимог до менеджера з інформаційної безпеки Опитування за результатами вивчення теми
Тема 6. ***Вимоги до менеджера з інформаційної безпеки: аналіз актуальних очікувань роботодавців*** ***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:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6.	Практичне заняття 25 Практичне заняття 26 Практичне заняття 27 Практичне заняття 28 Практичне заняття 29 Практичне заняття 30	5,5*	Читання і переклад зі словником спеціалізованих текстів науково-популярного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка повідомлень і доповідей щодо основних вимог до претендента на зайняття посади менеджера з ІБ на основі вивчення актуальних Інтернет-оголошень про вакансії Проведення презентацій із результатами дослідження вимог роботодавців Опитування за результатами вивчення теми
Тема 7. ***Види сертифікатів з управління інформаційною безпекою*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою; 2.спілкуватися на зазначену тему;	Практичне заняття 31 Практичне заняття 32	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології

3.писати повідомлення, документи, пов'язані з професією; 4.сприймати на слух і розуміти спеціалізовану інформацію за фахом. ***Формування компетенцій:*** ЗК1, ЗК2, ЗК3, ПП4, ПП8, ПП12 ***Результати навчання:*** ПРН1, ПРН4, ПРН8, ПРН12, ПРН23, ПРН26, ПРН35 ***Рекомендовані джерела:*** 1-6.	Практичне заняття 33 Практичне заняття 34 Практичне заняття 35 Практичне заняття 36		Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка повідомлень і доповідей щодо видів сертифікатів з управління ІБ (CISM, CISA, CISSP) Проведення презентацій з результатами вивчення видів сертифікатів з управління ІБ Опитування за результатами вивчення теми Проведення модульного контролю № 2 «Вимоги до менеджера з інформаційної безпеки»
Тема 5. Вимоги до управлінських та аналітичних здібностей і навичок менеджера з інформаційної безпеки. **Тема 6.** Вимоги щодо безпечного поводження персоналу на робочому місці та в мережі Інтернет. **Тема 7.** Огляд електронних ресурсів у сфері інформаційної та кібербезпеки для самоосвіти фахівця з управління ІБ.	Самостійна робота		1. Бажані управлінські навички менеджера з інформаційної безпеки. 2. Очікувані аналітичні здібності менеджера з інформаційної безпеки. 3. Вимоги щодо безпечного поводження персоналу на робочому місці. 4. Правила етичної та безпечної поведінки в Інтернеті - Нетікет. 5. Правила безпечного користування е-поштою. 6. Огляд безкоштовних курсів у сфері інформаційної та кібербезпеки на онлайн-платформах.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерний клас для проведення 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. Cyber-Security Standards, Benchmarking & Best Practices Overview. SAINT Consortium, 2018. 155 p. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5bab62342&appId=PPGMS
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
7. ISO/IEC 27000:2018(E) Information technology - Security techniques - Information security management systems - Overview and vocabulary. 27 p.
8. ISO/IEC 27001:2013(E) Information technology - Security techniques - Information security management systems – Requirements. 34 p.
9. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. 80 p.
10. http://www.isaca.org/

11. Pavlo Shchypanskyi, Vitalii Savchenko, Volodymyr Akhramovych, Tetiana Muzhanova, Svitlana Lehominova, Volodymyr Chegrenets. The Model of Secure Social Networks Activity Based on Graph Theory : International Journal of Innovative Technology and Exploring Engineering (IJITEE). Volume-9 Issue-4, February 2020, ISSN: 2278-3075 (Online). P 1803-1810. http://www.warse.org/IJATCSE/static/pdf/file/ijatcse291942020.pdf
12. Мужанова Т.М., Клюквін С., Матковський Б. ІТ-рішення для роботи з персоналом у сфері інформаційної безпеки. Тези доповідей Всеукраїнської наукової конференції «Актуальні проблеми кібербезпеки», м. Київ, 22 жовтня 2020 р. Державний університет телекомунікацій. С.177-179. http://www.dut.edu.ua/uploads/p_1739_27992763.pdf
13. Мужанова Т.М., Мосійчук В.М., Клименко О.І. Формування лояльності персоналу як чинник запобігання порушенням інформаційної безпеки. Збірник тез Всеукраїнської науково-практичної конференції «Цифрова трансформація кібербезпеки», м. Київ, 26 березня 2020 р. Державний університет телекомунікацій. С.30. http://www.dut.edu.ua/uploads/p_1739_99516793.pdf

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу індивідуально і в групах.
- Середовище в аудиторії є інтерактивним, творчим, відкритим до дискусії.
- Освоєння дисципліни передбачає обов'язкове відвідування практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем, які не ввійшли в теоретичний курс, або були розглянуті коротко, їх поглиблене опрацювання на основі рекомендованої літератури.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання в індивідуальному порядку.
- Під час роботи над завданнями не допустимо порушення вимог академічної доброчесності: при використанні Інтернет-ресурсів та інших джерел інформації студент має посилатися на використане джерело. У разі виявлення факту плагіату студент отримує за завдання 0 балів, аналогічну оцінку отримують автори тотожних робіт.
- 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.
- Використання телефонів і комп'ютерних засобів без дозволу викладача забороняється.

***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 відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• опитування за результатами вивчення теми, перевірка знання фахової термінології	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за темою, в тому числі вивченою самостійно (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді),	за кожну презентацію (реферат) максимум 3 бали
	• підготовка повідомлення, тез, ессе, анотації	за кожну правильну відповідь 2 бали
	• участь у дискусії, обговоренні положень нормативних актів, статей, відеоматеріалів	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «СТАНДАРТИЗАЦІЯ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «СЕРТИФІКАЦІЯ ФАХІВЦІВ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»	максимальна оцінка – 15 балів
Додаткова	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та	Звільняється від заліку

оцінка	Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	
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 у заліковій відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу й термінології в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано відповідає на поставлені запитання за темою. Студент показує високу якість спілкування з використанням спеціалізованої лексики, здатність вести діалог і дискусію на професійну тематику, повне сприйняття змісту прослуханих спеціалізованих текстів за фахом. За час навчання при проведенні практичних занять та виконанні індивідуальних / контрольних завдань студент проявляє вміння самостійно вирішувати поставлені завдання, активно долучатися до обговорення фахових питань іноземною мовою. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки обсягів матеріалу, передбаченого робочою програмою, або невпевненістю у тлумаченні окремих теоретичних положень.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента щодо виконання завдань підвищують його вміння використання знань, отриманих при вивчені інших дисциплін, а також знань, набутих при самостійному поглибленому вивченні питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (A)
82-89	Студент демонструє гарні знання змісту та професійної термінології, добре володіє матеріалом, що відповідає робочій програмі дисципліни, вміє застосовувати набуті знання та використовувати професійну лексику для самостійної роботи над текстами, але допускає одиничні неточності. Вміє самостійно виправляти допущені помилки, число яких є незначним. За час навчання при проведенні практичних занять, виконанні індивідуальних / контрольних завдань студент проявляє хорошу здатність самостійно вирішувати поставлені завдання, долучатися до обговорення фахових питань іноземною мовою із незначними прогалинами у володінні практичними навичками.	**Достатній** Забезпечує студенту самостійне виконання основних завдань за умов, коли вихідні дані в них змінюються порівняно з наданими у матеріалах дисципліни	Добре / Зараховано (B)
75-81	Студент загалом добре володіє матеріалом та професійною термінологією, знає основні теоретичні положення відповідно до робочої програми дисципліни, вміє застосовувати набуті знання та професійну лексику для самостійної роботи над текстами, але допускає окремі неточності, вміє пояснити основні положення виконаних завдань та дати правильні відповіді у ході опитування. Помилки у відповідях не є системними. Студент знає основні положення матеріалу, що мають визначальне значення при виконанні індивідуальних / контрольних завдань та поясненні представлених думок 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)
64-74	Студент засвоїв більшу частину теоретичного матеріалу та спеціалізованої лексики, передбачених робочою програмою дисципліни, розуміє постановку стандартних завдань, має уявлення щодо способів їх виконання. У ході виконання завдань допускає значну кількість неточностей і грубих помилок, які може усунути з допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
0 - 6	Студент володіє певними неґрунтовними знаннями, передбаченими в робочій програмі	**Середній**	Задовільно /

	дисципліни, на мінімально допустимому рівні. З використанням основних теоретичних положень студент з труднощами виконує поставлені викладачем завдання. У ході виконання практичних / індивідуальних / контрольних завдань демонструє формальне ставлення, відсутність глибокого розуміння роботи та взаємозв'язків з іншими темами.	Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Зараховано (E)
35-59	Студент може відтворити окремі фрагменти матеріалів курсу й окремі терміни. 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 та знання фахової лексики у студента відсутні.	**Низький** Не забезпечує практичної реалізації завдань, що формуються при вивченні 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 завдань, які встановляє програма дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*