СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«КРАЩІ ПРАКТИКИ ОРГАНІЗАЦІЇ 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">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">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>Лекцій</td><td>Семінарських занять</td><td>Практичних занять</td><td>Лабораторних занять</td><td>Самостійна підготовка</td></tr>
<tr><td>5</td><td>150</td><td>-</td><td>-</td><td>56</td><td>-</td><td>94</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.	**ПП1**. 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 3.** Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах. **ПП 4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. **ПП 6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. **ПП 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою. **ПП 12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам.

Програмні результати навчання (ПРН)

ПРН 2. Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв’язування складних спеціалізованих задач та практичних

проблему професійній діяльності, оцінювати їхню ефективність.
ПРН 3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
ПРН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
ПРН 12. Розробляти моделі загроз та порушника.
ПРН 16. Реалізовувати комплексні системи захисту інформації в автоматизованій системі організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки
ПРН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
ПРН 51. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Розділ 1 «ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
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:*** ЗК1, ЗК2, ЗК3, ПП3, ПП4, ПП6, ПП9, ПП12 ***Результати навчання:*** ПРН2, ПРН3, ПРН6, ПРН12, ПРН16, ПРН22, ПРН31, ПРН51 ***Рекомендовані джерела:*** 1-6, 7-12.	Практичне заняття 1 Практичне заняття 2 Практичне заняття 3 Практичне заняття 4 Практичне заняття 5	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:*** ЗК1, ЗК2, ЗК3, ПП3, ПП4, ПП6, ПП9,	Практичне заняття 6 Практичне заняття 7 Практичне заняття 8	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

ПП12 ***Результати навчання:*** ПРН2, ПРН3, ПРН6, ПРН12, ПРН16, ПРН22, ПРН31, ПРН51 ***Рекомендовані джерела:*** 1-6, 7-10.	Практичне заняття 9 Практичне заняття 10		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:*** ЗК1, ЗК2, ЗК3, ПП3, ПП4, ПП6, ПП9, ПП12 ***Результати навчання:*** ПРН2, ПРН3, ПРН6, ПРН12, ПРН16, ПРН22, ПРН31, ПРН51 ***Рекомендовані джерела:*** 1-6, 7, 10.	Практичне заняття 11 Практичне заняття 12 Практичне заняття 13 Практичне заняття 14 Практичне заняття 15	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 Проведення модульного контролю № 1 «ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»
Тема 1. Моделі зрілості управління інформаційною безпекою (O-ISM3, BPMMM, PCM, CCSMM) **Тема 2.** Класифікація загроз і вразливостей інформаційної безпеки відповідно 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. 8. Модель управління ризиками відповідно до стандарту COBIT.
Розділ 2 «ВНУТРІШНЯ ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 4. ***Безпека інформаційних активів організації*** ***Знати***: базову професійно-орієнтовану лексику за темою. ***Вміти:*** 1.читати спеціалізовані тексти нормативного характеру за темою;	Практичне заняття 16 Практичне заняття 17	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника,

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, ПП3, ПП4, ПП6, ПП9, ПП12 ***Результати навчання:*** ПРН2, ПРН3, ПРН6, ПРН12, ПРН16, ПРН22, ПРН31, ПРН51 ***Рекомендовані джерела:*** 1-6, 8, 11.	Практичне заняття 18 Практичне заняття 19		перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка анотацій статей з Інтернет-ресурсів про актуальні факти загроз інформаційним активам Представлення анотацій, відповіді на запитання Опитування за результатами вивчення теми
Тема 5. ***Розробка та впровадження політики інформаційної безпеки 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:*** ЗК1, ЗК2, ЗК3, ПП3, ПП4, ПП6, ПП9, ПП12 ***Результати навчання:*** ПРН2, ПРН3, ПРН6, ПРН12, ПРН16, ПРН22, ПРН31, ПРН51 ***Рекомендовані джерела:*** 1-6, 7-9.	Практичне заняття 20 Практичне заняття 21 Практичне заняття 22 Практичне заняття 23	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка галузевих політик інформаційної безпеки організації Проведення презентацій галузевих політик інформаційної безпеки організації Опитування за результатами вивчення теми
Тема 6. ***Внутрішня організація ІБ. Безпека дистанційної роботи та мобільних 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:*** ЗК1, ЗК2, ЗК3, ПП3, ПП4, ПП6, ПП9, ПП12 ***Результати навчання:*** ПРН2, ПРН3, ПРН6, ПРН12, ПРН16, ПРН22, ПРН31, ПРН51 ***Рекомендовані джерела:*** 1-6, 7-9.	Практичне заняття 24 Практичне заняття 25 Практичне заняття 26 Практичне заняття 27	5,5*	Читання і переклад зі словником спеціалізованих текстів нормативного характеру за темою Вивчення спеціалізованої лексики за темою, ведення словника, перевірка знання термінології Індивідуальні розповіді, ведення дискусії на зазначену тему Підготовка повідомлення про типові вимоги безпеки у випадку дистанційної роботи та мобільних пристроїв Опитування за результатами вивчення теми Проведення модульного контролю № 2 «ВНУТРІШНЯ ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»
Тема 4. Класифікація інформації обмеженого доступу на організаційному та урядовому рівні: досвід інших держав. **Тема 5**. Законодавство про безпеку даних США та ЄС. **Тема 6.** Ієрархія внутрішньо організаційної документації з ІБ та	Самостійна робота		1. Види урядової інформації обмеженого доступу на рівні організації та Уряду у США. 2. Види конфіденційної інформації, яка може оброблятися організацією.

вимоги до їх розробки.			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. 8. Вимоги до розробки організаційних процедур та інструкцій з ІБ.

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. ISO/IEC 27005:2008 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 телекомунікацій. С.44. http://www.dut.edu.ua/uploads/p_1739_99516793.pdf
12. Мужанова Т.М. Організаційне забезпечення інформаційної безпеки підприємства: основні засади. Сучасний захист інформації. 2016. № 2. С.78-82. 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 тощо	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 «ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»	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 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	**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 (А)

	робочою програмою, або невпевненістю у тлумаченні окремих теоретичних положень.		
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)
60-63	Студент володіє певними неґрунтовними знаннями, передбаченими в робочій програмі 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.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / 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*