СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Стандарти інформаційної та кібербезпеки»

Лектор курсу			**Якименко Юрій Михайлович**, кандидат військових наук, доцент, доцент кафедри "Управління інформаційною та кібернетичною безпекою"		**Контактна інформаціялектора (e-mail), сторінка курсу в Moodle**		**e-mail:**yakum14@ukr.net; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/view.php?id=1150
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**		перший (бакалавр)
Спеціальність			125 Кібербезпека		**Семестр**		3
Освітня програма			КІБЕРБЕЗПЕКА		**Тип дисципліни**		професійної та практичної підготовки
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:	Формування у студентів професійних знань вимог стандартів та умінь, необхідних для забезпечення інформаційної та кібербезпеки підприємств.

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Фахові компетенції (ПП)**
ЗК3. Здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.	**ПП6.** Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз , здійснення кібератак, збоїв та відмов різних класів та походження. **ПП7**. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) .

Програмні результати навчання (ПРН)

ПРН4. 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.
ПРН16. Реалізовувати комплексні системи захисту інформації в автоматизованій системі організації (підприємства) відповідно до вимог нормативно-правових документів.
ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**

<table>
<tr><th colspan="4">Розділ 1 «СТАНДАРТИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СТАН ЇХ ВПРОВАДЖЕННЯ В УКРАЇНІ»</th></tr>
<tr><td rowspan="4">Тема 1. Вимоги основних міжнародних стандартів у сфері інформаційної безпеки та стан їх впровадження в Україні
<u>Знати</u>: основні терміни інформаційної та кібернетичної безпеки та їх визначення, процеси управління інформаційною безпекою (ІБ) та управління ризиками, ролі інформаційної безпеки та домени кібербезпеки; вимоги основних міжнародних стандартів у сфері інформаційної безпеки та стан їх впровадження в Україні; аналіз вимог до обґрунтування і розробки стандартів систем менеджменту та можливості стандартизованих моделей менеджменту в системі корпоративного управління.
<u>Вміти:</u> використовувати вимоги стандартів, як нормативних документів для вирішення проблем з забезпеченням інформаційної та кібербезпеки.
<u>Формування компетенцій:</u> ЗК3, ПП6
<u>Результати навчання:</u> ПРН 4
<u>Рекомендовані джерела:</u> 1,3,5,8,14</td><td>Лекція 1</td><td rowspan="4">5,5*</td><td>Лекція-візуалізація</td></tr>
<tr><td>Лекція 2</td><td>Експрес-опитування студентів</td></tr>
<tr><td>Лекція 3</td><td>Лекція-візуалізація, експрес-опитування студентів</td></tr>
<tr><td>Практичне заняття 1</td><td>Ознайомлення з моделями корпоративного управління інформаційними технологіями (ІТ) та інформаційною безпекою організації. Обговорення питань</td></tr>
<tr><td rowspan="5">Тема 2. Створення систем управління інформаційною безпекою відповідно до вимог стандартів в сфері ІБ
<u>Знати</u>: нормативні документи з питань безпеки комп'ютерних систем, підходи до оцінки безпеки інформаційних систем в США та критерії оцінки безпеки комп'ютерних систем; критерії і методологію оцінки безпеки ІТ, єдині критерії оцінки безпеки ІТ, загальна методологія оцінки безпеки ІТ,
основні положення загальних критеріїв безпеки ІТ,
методику застосування процесного підходу до створення СУІБ організації з використанням вимог по стандартизації до систем і процесів управління інформаційною безпекою,
методику впровадження процесного підходу до створення СУІБ організації (згідно вимог ISO IEC 27035),
методику впровадження вимог до створення системи управління ризиками інформаційної безпеки організації, концепцію прийнятного (допустимого) ризику ІБ, вимоги стандарту ISO31000, досвід управління ризиками;
<u>Вміти</u>: впроваджувати процесний підхід до створення СУІБ, СУІБ та системи управління ризиками інформаційної безпеки організації.
<u>Формування компетенцій:</u> ПП7
<u>Результати навчання:</u> ПРН16
<u>Рекомендовані джерела:</u> 5,8,9,12,14,15,18,19,23, 24</td><td>Лекція 4</td><td rowspan="5">5,5*</td><td>Лекція-візуалізація. Експрес-опитування студентів</td></tr>
<tr><td>Лекція 5</td><td>Навчальна дискусія за темою Загальні критерії безпеки ІТ</td></tr>
<tr><td>Практичне заняття 2</td><td>Вивчення методики та впровадження процесного підходу до створення СУІБ на прикладі</td></tr>
<tr><td>Практичне заняття 3</td><td>Розробка та впровадження системи управління інцидентами інформаційної безпеки. Обговорення питань</td></tr>
<tr><td>Практичне заняття 4</td><td>Модульний контроль №1. Виконання кваліфікаційних завдань</td></tr>
</table>

Тема 1 Вимоги основних міжнародних стандартів у сфері інформаційної безпеки та стан їх впровадження в Україні **Тема 2** Створення систем управління інформаційною безпекою відповідно до вимог стандартів в сфері ІБ	Самостійна робота		1. Процеси управління інформаційною безпекою (ІБ) 2. Ролі інформаційної безпеки та домени кібербезпеки; 3. Вимоги основних міжнародних стандартів у сфері інформаційної безпеки та стан їх впровадження в Україні; 4. Аналіз вимог до розробки стандартів систем менеджменту та можливості стандартизованих моделей менеджменту в системі корпоративного управління. 5. Нормативні документи з питань безпеки комп'ютерних систем, 6. Підходи до оцінки безпеки інформаційних систем в США та критерії оцінки безпеки комп'ютерних систем; 7. Методика застосування процесного підходу до створення СУІБ організації з використанням вимог по стандартизації до систем і процесів управління ІБ, 8. Методика впровадження процесного підходу до створення СУІБ організації (відповідно до вимог ISO IEC 27035), 9. Методика впровадження вимог до створення системи управління ризиками ІБ організації, концепцію 10. Концепція прийнятного (допустимого) ризику ІБ, 11. Вимоги стандарту ISO31000.
Розділ 2 « ВИКОРИСТАННЯ СТАНДАРТІВ ПРИ ПЕРЕВІРЦІ І ОЦІНЦІ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 3. ***Використання стандартів інформаційної безпеки при моніторингу та аудиті систем управління ІБ*** ***Знати:*** підходи до використання вимог стандарту COBIT в управлінні IT, концепцію та основні поняття зі стандарту, процесну модель COBIT ; умови забезпечення безперервності бізнес-процесів і управління інцидентами, концепція готовності до інцидентів і безперервності діяльності (ISO/PAS 22399:2007), вимоги до планування безперервності бізнесу. NIST SP 800-34; загальні відомості про бібліотеку ITIL і моделі ITSM, процеси підтримки та надання IT-сервісів у діяльності IT-служб;	Лекція 6	5,5*	Експрес-опитування студентів
	Лекція 7		Навчальна дискусія за темою Планування безперервності бізнесу.
	Практичне заняття 5		Впровадження вимог до аудиту інформаційної безпеки інформаційної системи організації на прикладі. Обговорення питань

вимоги до аудиту систем менеджменту та аудиту інформаційної безпеки інформаційних систем організації, вимоги стандарту ISO-19011-2018 Настанови щодо здійснення аудитів систем управління; вимоги стандартів ISO та можливості застосування програм Cobra і КОНДОР+ для перевірки СУІБ, методичні підходи до проведення перевірки СУІБ на відповідність вимогам стандартів ISO; підходи до побудови системи моніторингу інформаційної безпеки, типові структури SIEM-систем з моніторингу подій інформаційної безпеки; ***Вміти***: використовувати структуру SIEM-систем з моніторингу подій інформаційної безпеки та підхід для перевірки СУІБ підприємства на відповідність вимогам стандартів ISO. ***Формування компетенцій:*** ЗК3, ПП6, ПП7, 3 ***Результати навчання:*** ПРН16, 3 ***Рекомендовані джерела:*** **1,2,3,5,8,9,16**	Практичне заняття 6		Практика моніторингу подій інформаційної безпеки з використанням SIEM-системи. Обговорення результатів
	Практичне заняття 7		Практика проходження перевірки СУІБ на відповідність вимогам стандартів ISO. Обговорення результатів
Тема 4. ***Оцінка ефективності менеджменту безпеки інформаційних технологій та бізнес - процесів*** ***Знати***: методи менеджменту безпеки інформаційних технологій: способи управління безпекою ІТ, політику безпеки інформаційних технологій, основні варіанти стратегії (підходи) аналізу ризику організації; бізнес - процеси та стандарти управління з їх оцінкою, організація роботи бізнесу і процесний підхід, вимоги стандарту ISO/IEC 15504-4 до оцінки бізнес – процесів, вимоги до забезпечення готовності організації до інцидентів і безперервності її діяльності. ***Вміти***: оцінювати ефективність бізнес – процесів та організацію роботи бізнесу ***Формування компетенцій:*** ПП7, 3 ***Результати навчання:*** ПРН4, ПРН16, 3 ***Рекомендовані джерела:*** ***2,3,5,7,8,9,12,14,15,16,23***	Лекція 8	5,5*	Лекція-візуалізація. Експрес-опитування студентів
	Лекція 9		Навчальна дискусія за темою Організаційні передумови стратегії забезпечення безпеки кіберпростору
	Практичне заняття 8		Усне опитування за темою Організація роботи бізнесу і оцінки бізнес – процесів
	Практичне заняття 9		Модульний контроль №2. Виконання кваліфікаційних завдань
Тема 3. Використання стандартів інформаційної безпеки при моніторингу та аудиті систем управління ІБ **Тема 4.** Оцінка ефективності менеджменту безпеки інформаційних технологій та бізнес - процесів	Самостійна робота		1. Вимоги стандарту COBIT в управлінні IT (основні поняття, процесна модель) 2. Умови забезпечення безперервності бізнес-процесів і управління інцидентами 3. Концепція готовності до інцидентів і безперервності діяльності (ISO/PAS 22399:2007) 4. Вимоги до планування безперервності бізнесу відповідно до

			NIST SP 800-34 5. Вимоги до аудиту систем менеджменту та аудиту інформаційної безпеки інформаційних систем організації 6. Основні положення загальних критеріїв безпеки IT, 7. Загальні відомості про бібліотеку ITIL і моделі ITSM, 8. Процеси підтримки та надання IT-сервісів у діяльності IT-служб; 9. Підходи до побудови системи моніторингу ІБ 10. Типові структури SIEM-систем з моніторингу подій ІБ 11. Вимоги стандартів ISO та можливості застосування програм Cobra і КОНДОР+ для перевірки СУІБ 10. Методичні підходи до проведення перевірки СУІБ на відповідність вимогам стандартів ISO 11. Методи менеджменту безпеки інформаційних технологій: 12. Способи управління безпекою IT 13. Політика безпеки інформаційних технологій 14. Основні варіанти стратегії (підходи) аналізу ризику організації 15. Основа кібербезпеки і забезпечення безпеки кіберпростору 16. Організаційні передумови стратегії забезпечення безпеки кіберпростору 17. Найважливіші пріоритети для забезпечення безпеки кіберпростору 18. Бізнес - процеси та стандарти управління з їх оцінкою 19. Організація роботи бізнесу і процесний підхід 20. Вимоги стандарту ISO/IEC 15504-4 до оцінки бізнес – Процесів

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп’ютери Asus
- комп’ютерний клас для проведення занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. /[КорченкоО.Г.,ГнатюкС.О., КазмірчукС.В.та ін.]. – Київ : Центр навч.-наук. та наук.-пр.виданьНАСБ України, 2014. –190с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
2. Маркіна І.А. Основи формування системи менеджменту інформаційної безпеки підприємства. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/3092/1/piprp_2016_3%281%29__18.pdf
3. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— Київ : ДУТ, 2015.— 288 с.
4. Варенко В. М. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – Київ : Університет «Україна», 2013. – 203 с. URL: http://er.nau.edu.ua:8080/handle/NAU/20105.

5. Суворова О.Р. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. Урок №12. URL: https://naurok.com.ua/keruvannya-mehanizmami-zahistu-mizhnarodni-standarti-informaciyno-bezpeki-104726.html
6. Рой Я.В., Мазур Н.П., Складанний П.М.Аудит інформаційної безпеки –основа ефективного захисту підприємств./ Кібербезпека: освіта, наука, техніка №1(1) - Київ: Київський університет імені Бориса Грінченка, 2018 с.87-93. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/23
7. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою.- Професійний розвиток фахівців у системі освіти дорослих: історія, теорія,технології: програма ІУ-ої Всеукраїнської Інтернет-конференції 16 жовтня 2019 р., м. Київ.-/за наук. ред. В.В. Сидоренко; упорядкування Я.Л. Швень, М.І. Скрипник. К.: Агроосвіта, 2019.- С.41-43.
8. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
9. ДСТУ ISO/IEC 27002:2015 (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014), Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
10. ДСТУ ISO/IEC 27003:2018 (ISO/IEC 27003:2017, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова . (ISO/IEC 27003:2010)
11. ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Управління інформаційною безпекою. Вимірювання
12. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ДСТУ ISO/IEC 27005:2015)
13. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. (ДСТУ ISO/IEC TR 27008:2018)
14. ДСТУ ISO/IEC 27009:2018 (ISO/IEC 27009:2016, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги
15. ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002. (ISO/IEC 27011:2008)
16. ДСТУ ISO/IEC 27031:2015 (ISO/IEC 27031:2011, IDT) Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу
17. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки
18. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами.
19. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти.
20. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.
21. ISO/IEC 27002:2013 Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information
22. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT)Настанови щодо проведення аудитів систем управління
23. ДСТУ ISO 31000:2018 (ISO 31000:2018, IDT) Менеджмент ризиків. Принципи та настанови
24. ДСТУ ISO/IEC 15408-1:2017 (ISO/IEC 15408-1:2009, IDT)
Інформаційні технології. Методи захисту. Критерії оцінки. Частина 1-3

ПОЛІТИКА КУРСУ

- 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 виконане 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 відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 балів
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 "СТАНДАРТИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА СТАН ЇХ ВПРОВАДЖЕННЯ В УКРАЇНІ"	максимальна оцінка – 15 балів
	Модульний контроль № 2 "ВИКОРИСТАННЯ СТАНДАРТІВ ПРИ ПЕРЕВІРЦІ І ОЦІНЦІ СИСТЕМ УПРАВЛІННЯ 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 іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит 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 (A)
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)
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 іспиту.	**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*