СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ БАНКІВ»

Лектор курсу	Капелюшна Тетяна Вікторівна, кандидат економічних наук, доцент, доцент кафедри управління інформаційною та кібернетичною безпекою	Контактна інформація лектора (e-mail), сторінка курсу в Moodle	e-mail: e-skr@ukr.net; сторінка курсу в Moodle - Курс: управління інформаційною безпекою банків (dut.edu.ua)	
Галузь знань	12 Інформаційні технології	**Освітній рівень**	бакалавр	
Спеціальність	125 Кібербезпека	**Семестр**	5	
Освітньо-професійна програма	Управління інформаційною та кібернетичною безпекою	**Тип дисципліни**	основна	

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18		18	18	96

АНОТАЦІЯ КУРСУ

Мета курсу: є формування системи знань з основ банківської діяльності, інформаційних і телекомунікаційних технологій, які використовуються у банківській сфері, вирішення проблеми забезпечення інформаційної безпеки функціонування банків та управління інформаційною безпекою банків

Компетенції відповідно до освітньо-професійної програми

Soft- skills / Загальні компетентності (ЗК)	Hard-skills / Спеціальні (фахові) компетенції
ЗК1. Здатність застосовувати знання у практичних ситуаціях **ЗК2.** Знання та розуміння предметної області та розуміння професії	**ПП1**. Здатність застосовувати законодавчу та нормативно-правову базу, а також держані та міжнародні вимоги, практики, стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки. **ПП4.** Здатність забезпечувати неперервність бізнесу згідно встановленої політики безпеки. **ПП8.** Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку. **ПП12.** Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам

Результати навчання відповідно до освітньо-професійної (програмні результати навчання – ПРН)

ПРН 12. Розробляти моделі загроз та порушника.
ПРН 22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.
ПРН 33. Вирішувати задачі забезпечення неперевності бізнес-процесів організації.
ПРН 41. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Політика оцінювання за темою	Форми і методи навчання/питання до самостійної роботи

<table>
<tr><td colspan="4">Змістовний модуль 1. Теоретичні аспекти управління інформаційною безпекою банків</td></tr>
<tr><td rowspan="3">Тема 1. Вступ до управління інформаційною безпекою банків. Огляд банківських операцій
<u>Знати</u>: банк як об’єкт критичної інфраструктури, сутність та зміст управління інформаційною безпекою банків; об’єкти захисту в банківській сфері; основи автоматизації банківської діяльності в світі та Україні; огляд банківських операцій; критичні дані та процеси у банківській діяльності; ідентифікація критично важливих даних та процесів; визначення типів даних та процесів, які є найбільш важливими для діяльності та репутації банку; пріоритети захисту критично важливих активів банку
<u>Вміти:</u> розрізняти інформаційну безпеку банку та підприємства, визначати специфіку у діяльності фінансових установ для виявлення розбіжностей в управління інформаційною безпекою саме для банківських установ; ідентифікувати та ранжувати критично важливі дані та процеси.
<u>Формування компетенцій:</u> ЗК1, ЗК2, ПП1
<u>Результати навчання:</u> ПРН22
<u>Рекомендовані джерела:</u> 1,2,3,4,5,18</td><td>Лекція 1</td><td rowspan="3">4,45*</td><td>Лекція-візуалізація, експрес-опитування студентів</td></tr>
<tr><td>Практичне заняття 1</td><td>Опрацювання ситуаційних завдань; кейси</td></tr>
<tr><td>Лабораторне заняття 1</td><td>Вирішення завдань</td></tr>
<tr><td rowspan="3">Тема 2. Захист банківської інформації. Регулятор та правове забезпечення щодо інформаційної безпеки банків
<u>Знати</u>: особливості захисту банківської інформації; основні загрози автоматизованої банківської системи. рівні у банківській системі; держрегулятор, нормативне та правове регулювання функціонування банківських установ, стандарти, якими керуються. Перевірка клієнтів (CDD) та посиленої перевірки клієнтів з високим рівнем ризику (EDD), важливість комплаєнсу для захисту критично важливих бізнес-процесів. Регуляторні вимоги, що регулюють банківський сектор GDPR, Базель III
,<u>Вміти</u>: формувати основні задачі до захисту банківської інформації; вимоги до захисту банківської інформації з урахуванням її особливостей. формувати систему захисту інформації у банківській сфері з урахуванням норм та стандартів, нормативно-правових документів.
<u>Формування компетенцій:</u> ЗК2, ПП12, ЗК1, ЗК5, ПП4
<u>Результати навчання:</u> ПРН22, ПРН33
<u>Рекомендовані джерела:</u> 1,2,4,5,6,8,12</td><td>Лекція 2</td><td rowspan="3">4,45*</td><td>Лекція-візуалізація, експрес-опитування студентів</td></tr>
<tr><td>Практичне заняття 2</td><td>Мозковий штурм; інтерактивні завдання; опитування (відкриті питання)</td></tr>
<tr><td>Лабораторне заняття 2</td><td>Вирішення завдань</td></tr>
<tr><td rowspan="3">Тема 3. Організаційні аспекти захисту банківської таємниці. Конфіденційність даних
<u>Знати</u>: порядок захисту банківської таємниці, документи, якими регулюється організація захисту інформації та банківської таємниці; інциденти, за яких до інформації надається доступ і кому саме; огляд нормативно-правових актів про конфіденційність даних California Consumer Privacy Act (CCPA), Загальний регламент про захист даних (GDPR) Вимоги до обробки та захисту персональних даних відповідно до CCPA та GDPR
<u>Вміти</u>: розумітися на правах і обов’язках працівників банків; пропонувати процедуру організації системи захисту комерційної таємниці банків. Формувати основні задачі та вимоги до захисту банківської; запобігати використанню в злочинних цілях інформації в банківських установах;</td><td>Лекція 3</td><td rowspan="3">4,45*(+15 МК1)</td><td>Лекція-візуалізація</td></tr>
<tr><td>Практичне заняття 3</td><td>Розв’язок ситуаційних завдань, вирішення практичних завдань</td></tr>
<tr><td>Лабораторне заняття 3</td><td>Проведення контролю знань №1</td></tr>
</table>

впровадувати політик та процедур захисту даних для дотримання регуляторних вимог; поводити оцінку впливу на захист даних та управління запитами ***Формування компетенцій:*** **ЗК1, ЗК2**, **ПП4** ***Результати навчання:*** **ПРН12**, **ПРН22.** ***Рекомендовані джерела:*** 12-16			
Змістовний модуль2. Управління інформаційною безпекою банківських установ			
Тема 4. **Інформаційна розвідка. Поширені кіберзагрози. Соціоінженерний підхід.** ***Знати***: задачі інформативної, бізнес-розвідки, неправомірні методи збору інформації; інформаційно-аналітичний супровід процесу прийняття управлінських рішень як напрям ЗІБ сучасного підприємства; шкідливе програмне забезпечення, фішинг, програми-вимагачі, інсайдерські загрози; дії та кроки соціального інженера. ***Вміти***: проводити аналіз та оцінку оточення для виявлення потенційного соціального інженера; проводити аналітичну, інформаційну розвідку за відкритими джерелами у глобальній мережі. ***Формування компетенцій:*** **ЗК1, ЗК4**, **ПП12**. ***Результати навчання:*** **ПРН41**. ***Рекомендовані джерела:*** 1, 5, 6, 8, 20	Лекція 4	4,45*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 4		Доповіді з презентацією за темою та їх обговорення.
	Лабораторне заняття 4		Виконання завдань
Тема 5. **Управління мобільними пристроями (захист кінцевих точок) у банках** ***Знати***: захист кінцевих точок і мобільних пристроїв, що використовуються співробітниками і клієнтами банку; розгортання рішень для захисту кінцевих точок, управління мобільними пристроями (MDM) та управління мобільними додатками (MAM); впровадження політик безпеки та засобів контролю для захисту від загроз на кінцевих точках програмні продукти аналізу ризиків, що використовуються у світі для банківського сектору ***Вміти***: розрізняти програмні продукти аналізу ризиків у банківській сфері, здійснювати захист кінцевих точок і мобільних пристроїв, що використовуються співробітниками і клієнтами банку ***Формування компетенцій:*** **ЗК1, ЗК4**, **ПП 4.** ***Результати навчання:*** **ПРН22**, **ПРН44**. ***Рекомендовані джерела:*** 16	Лекція 5	4,45*	Лекція-візуалізація
	Практичне заняття 5		Розв’язок задач. Кейси.
	Лабораторне заняття 5		Виконання завдань
Тема 6. **Управління інформаційною безпекою банківських установ** ***Знати***: принципи управління ІББ (розімкнутого управління, компенсації, зворотного зв’язку); властивості управління ІББ; зобов’язання керівництва щодо управління інформаційною безпекою; критичні бізнес-процеси/ банківські продукти, які відносять до інформації з обмеженим доступом; політика інформаційної безпеки банку ***Вміти***: нести відповідальність та виконувати функції керівника управління інформаційною безпекою; приймати участь у розробці політики інформаційної безпеки банку, розумітися на основних аспектах, що має включати політика інформаційної безпеки банків..	Лекція 6	4,45* (+15 МК2)	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 6		Розв’язок задач. Ситуаційні завдання.
	Лабораторне заняття 6		Виконання завдань

Формування компетенцій: **ЗК1, ЗК2**, **ПП8**, **ПП4, ПП12.** ***Результати навчання:*** **ПРН5**, **ПРН22**, **ПРН33** ***Рекомендовані джерела:*** 7-13, 19, 21			
Тема 7. **Захист хмарного середовища банку** ***Знати***: суть хмарних обчислень, їх переваг та ризиків для банків; кращі практики захисту хмарних систем та сервісів; впровадження засобів контролю безпеки та заходів для захисту конфіденційних даних, що зберігаються в хмарі AWS; особливості управління ідентифікацією та доступом (IAM) для хмарних сервісів; інтеграція IAM з рішеннями єдиного входу (SSO) та багатофакторної автентифікації (MFA); принципи проєктування хмарних середовищ ***Вміти***: керуватися принципами IAM для управління доступом користувачів до хмарних ресурсів; вміти керувати ідентифікацією та доступом в AWS; впроваджувати політики і ролі IAM для забезпечення мінімальних привілеїв і гранульованого контролю доступу ***Формування компетенцій:*** **ЗК1, ПП1** ***Результати навчання:*** **ПРН22**	Лекція 7	4,45*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 7		Ситуаційні завдання. Розв'язок задач
	Лабораторне заняття 7		Виконання завдань. Обговорення за результатами виконаних робіт
Тема 8. **Моніторинг хмарної безпеки та реагування на інциденти** ***Знати*:** як збирати дані про активність та події у мережі; інструменти і сервіси моніторингу хмарної безпеки для виявлення і реагування на загрози безпеки. AWS Cloud Watch, Cloud Trail, Security Hub, AWS Config, Lambda ***Вміти***: розробляти плани і процедури реагування на інциденти, специфічних для хмарних середовищ: вміти визначати, які AWS-сервіси можна використовувати для моніторингу, вміти визначати, які AWS-сервіси можна використовувати для реагування на інциденти *Формування компетенцій:* ЗК1, ПП1 ***Результати навчання:*** **ПРН22**	Лекція 8	4,45*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 8		Виконання вправ і симуляцій для перевірки ефективності можливостей реагування на інциденти
	Лабораторне заняття 8		Виконання завдання
Тема 9. **Вимоги до кібербезпеки в банківській системі (врахування вимог до захисту банку як об'єкта критичної інфраструктури)** ***Знати***: вимоги до інформаційної безпеки в банківській системі України, принципи забезпечення інформаційної безпеки; вимоги щодо впровадження СУІБ; вимоги, що висуваються до банків щодо забезпечення їх інформаційної безпеки. Стратегічні орієнтири управління інформаційною безпекою банків на період воєнного стану та післявоєнного відновлення економіки ***Вміти***: формувати безпечне середовище для функціонування банків; забезпечувати інформаційний захист з урахуванням сучасних вимог до банківських структур; розумітися на кращих практиках захисту інформаційної безпеки банків та приймати стратегічні рішення щодо захисту інформаційної інфраструктури банку у повоєнний час ***Формування компетенцій:*** **ЗК1, ПП1** ***Результати навчання:*** **ПРН22** ***Рекомендовані джерела:*** 7-13, 22	Лекція 9	4,45* (+15 МК2)	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9		Ситуаційні завдання. Презентації за темою та їх обговорення.
	Лабораторне заняття 9		Проведення контролю знань №2
Залік	Проведення заліку	30*	Підсумковий контроль - залік
Самостійна робота		*	Завдання із переліку запропонованих проблемних питань для дослідження

		за тематикою наукових інтересів здобувача освіти у межах опанування даної освітньої компоненти

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕНН ДИСЦИПЛІНИ

Комп'ютери с програмним забезпеченням для виконання практичних робіт: комп'ютери Asus, комп'ютерний клас для проведення занять
Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».
Мультимедійний проєктор, мультимедійна система Acer X113 DLP
Програмний продукт Object Control.
Система дистанційного навчання і контролю Moodle –http://dl.dut.edu.ua

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Навчально-методичний косплекс з дисципліни «Управління інформаційною безпекою банків»
2. Kapeliushna T., Kryshtal H. Synergy of the banking sector and socio-economic under the influence of the state regulator. Підприємництво та інновації. 2019. Вип. 9, 2019 С.147-152 URL: http://www.ei-journal.in.ua/index.php/journal/article/view/219/208
3. Конспект лекцій з дисципліни «Управління інформаційною безпекою банків»
4. Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур» /В.М.Ахрамович. Державний університет телекомунікацій. – К.:ДУТ, 2019. – 163 с. іл. – Бібліограф.: 166 с.
5. Розпорядження Кабінету Міністрів України № 356-р «Про схвалення основних (стратегічних) напрямів діяльності банків державного сектору на період воєнного стану та післявоєнного відновлення економіки»
6. Мужанова Т.М. Конкурентна розвідка як інструмент інформаційно-аналітичного супроводу забезпечення інформаційної безпеки підприємства. *Економіка та суспільство*. Випуск # 16 / 2018 С.425-431.
7. Постанова Кабінету Міністрів України від 9 жовтня 2020 р. N 1109 «Деякі питання об'єктів критичної інфраструктури»
8. Про затвердження Змін до Правил зберігання, захисту, використання та розкриття банківської таємниці. https://zakon.rada.gov.ua/laws/show/v0098500-21#Text
9. Постанова НБУ «Про затвердження Положення про здійснення контролю за дотриманням банками вимог законодавства з питань інформаційної безпеки, кіберзахисту та електронних довірчих послуг» від 16.01.2021 р. №4. URL: https://bank.gov.ua/admin_uploads/law/16012021_4.pdf
10. Політика інформаційної безпеки Приватбанку. URL: https://static.privatbank.ua/files/file.pdf
11. Політика інформаційної безпеки "Укрсіббанк". URL: https://ukrsibbank.com/wp-content/uploads/2021/12/information_security_policy.pdf
12. Політика інформаційної безпеки. URL: "БАНК УКРАЇНСЬКИЙ КАПІТАЛ"
13. https://ukrcapital.com.ua/uk/licenses/polozhennia/572-polityka-informatsiinoi-bezpeky-at-bank-ukrayinskyy-kapital/file.html
14. Політика інформаційної безпеки"Райфайзен банк аваль". URL: https://raiffeisen.ua/storage/files/politika-informatsiynoi-bezpeki.pdf
15. Браіловський М.М. Захист інформації у банківській діяльності / М.М. Браіловський, Г.П. Лазарєв, В.О. Хорошко – К.: ТОВ «ПоліграфКонсалтинг», 2016. – 216 с.
16. Єрьоміна Н.В. Банківські інформаційні системи: Навч. посібник / Н.В. Єрьоміна. – К.: КНЕУ, 2015. — 220 с.
17. Зубок М.І. Інформаційна безпека в підприємницькій діяльності: Підручник / М.І. Зубок. – К.: ГНОЗІС, 2015. – 225 с.
18. Побережний С.М. Організація діяльності підрозділів банківської безпеки в сучасному комерційному банку / С.М. Побережний. – Суми: ВВП "Мрія-1" ЛТД, 2016. – 53 с.
19. Стрельбицька Л.М. Банківське безпекознавство: Навч. посібник / Л.М. Стрельбицька, М.П. Стрельбицький, В.К. Гіжевський. – К.: Кондор, 2017. – 602 с.
20. Вступ до банківської справи: Навч. посібник / М.І. Савлук, Мороз , А.М. Коряк; Під ред. М. І. Савлука. – К.: Лібра, 2016. – 344 с.
21. Зубок М.І. Безпека банківської діяльності / М.І. Зубок. – К.: КНЕУ, 2015. – 156 с.
22. Тедов О.О. Електронні банківські послуги та Інтернет-банкінг: правове регулювання / О.О. Тедов. – К.: Новий індекс, 2015. – 320 с.

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 зазначений 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

Форми контролю	Види навчальної роботи	* Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на лекціях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,25 бала
	• ведення конспекту	за кожну лекцію 1,5 бали
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	Робота на практичних заняттях*, у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 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)	за кожну презентацію максимум 10 балів
	• 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 3 бали
РУБІЖНЕ ОЦІНЮВАННЯ (контроль знань)	Контроль знань № 1	за кожне правильно виконане завдання максимальна оцінка – 15 балів
	Контроль знань № 2	за кожне правильно виконане завдання максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Згідно рішення кафедри
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***залік***	Метою екзамену є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у формі тестування	Критерії оцінювання зазначено у таблиці

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об 'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки,	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли	Добре / Зараховано (В)

	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.	вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	
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 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*