СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ТЕОРІЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ОБМЕЖЕНОГО ДОСТУПУ»

Лектор курсу	Ахрамович Володимир Миколайович, доктор технічних наук, професор, кафедри систем інформаційного та кібернетичного захисту	**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**12z**@ukr.net; **сторінка курсу в Moodle –** http://dn.dut.edu.ua/course/view.php?id=424
Галузь знань	12 Інформаційні технології	**Рівень вищої освіти**	Магістр
Спеціальність	Кібербезпека	**Семестр**	1
Освітня програма	Магістра	**Тип дисципліни**	Вибіркова

Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	28	-	30	22	70

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Методологія наукових досліджень кібербезпеці
Освітні компоненти для яких є базовою	

Мета курсу:	Формування системи теоретичних знань щодо організаційного забезпечення захисту інформації обмеженого доступу; концептуальні засади із вжиття організаційних та технічних заходів для забезпечення інформаційної безпеки; вибір, залежно від загроз, сучасних системи захисту інформації; освоєння сучасних засобів технічного захисту інформації; побудова сучасного захисту інформації на об'єктах інформаційної діяльності; створення комплексу технічного захисту інформації на об'єктах інформаційної діяльності з обмеженим доступом

Компетентності відповідно до освітньої програми

Soft- skills / Загальні компетентності (ЗК)	**Hard-skills / Спеціальні компетентності (СК)**
ЗК 1 Уміння критичної самооцінки – здатність визначати та задовольняти потреби особистого та наукового розвитку, бути критичним і самокритичним **ЗК-3. Знання інформаційних технологій – здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.**	**ФК-1. Інтегративна компетентність** **ФК-3. Організаційно-комунікативна компетентність** **ФК-4. Професійна компетентність** **ФК-5. Загальнонаукова компетентність** **ФК-6. Політехнічна компетентність**

ЗК-4. Навички керування проектами – здатність демонструвати своєчасність та спланованість у дослідженні, здатність до адаптації та дії в новій ситуації, здатність розробляти та управляти проектами.	**ФК-7. Інженерна компетентність** **ФК-8. Ділова компетентність**

Програмні результати навчання (ПРН)

ПРН 9. Уміти здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності.
ПРН-15. Уміти орієнтуватися у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної безпеки**.**
ПРН-17. Уміти підтримувати комплексні системи інформаційної та кібербезпеки в стані, необхідному для вирішення завдань захисту інформації.
ПРН-18. Уміти аналізувати існуючі технології, методи і засоби застосування шкідливого програмного забезпечення, нівелювання уразливостей мережевих та Web-ресурсів.
ПРН-21. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки.
ПРН-24. Уміти здійснювати науково-технічне супроводження заходів з формування і коригування програмних комплексів забезпечення безпеки та захисту інформації на об'єктах інформаційної діяльності.
ПРН-25. Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об'єктів інформаційної діяльності.
ПРН-28. Бути здатним до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації.
ПРН-30. Бути здатним до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.
ПРН-32. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об'єктах інформаційної діяльності та інформації, що циркулює в ІТ системах та мережах.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1. Організаційне забезпечення та системи захисту інформації обмеженого доступу			
Тема 1. ***Організаційне забезпечення захисту інформації обмеженого доступу.*** ***Знати***: Допуск посадових осіб та порядок оформлення допуску до державної таємниці. Організація секретного діловодства. Ознаками комерційної таємниці. Законодавство України про державну таємницю Захист конфіденційної інформації. Захист професійної таємниці. Захист персональних даних (інформації про особу) в Україні. Принципи впровадження політики безпеки.	Лекція 1 2 год.	15	Лекція-візуалізація
	Лекція 2 2 год..		Лекція-візуалізація
	Лекція 3 4 год.		Лекція-візуалізація

Організація допуску та доступу персоналу до конфіденційної інформації. Організація доступу до таємної інформації. Захист службової інформації. Основні напрями захисту електронної інформації. Довідник кваліфікаційних характеристик професій працівників. Безпека господарської діяльності підприємства, установи, організації. Перелік відомостей, що становлять службову інформацію і яким присвоюється гриф з обмеженим доступом «для службового користування» Злочини проти конфіденційності, цілісності і доступності комп'юте-рних даних та систем. Злочини, пов'язані з використанням комп'ютерів. Злочини, пов'язані з порушенням авторських і суміжних прав з використанням комп'ютерних даних і систем. Злочин, пов'язані зі змістом даних. Нормативні документи системи ТЗІ. ***Вміти:*** обгрунтовувати та реалізовувати на об'єктах інформаційної діяльності з обмеженим доступом захист інформації, здійснювати оцінку систем захисту інформації автоматизованої системи відповідно до вимог діючих стандартів та нормативних документів, володіти вмінням формувати технології розроблення комплексів захисту інформації з обмеженим доступом та охорони об'єктів інформаційної діяльності, розробляти проекти комплексів засобів захисту інформаційної діяльності. ***Формування компетенцій:***ЗК1, ЗК3, ФК-1, ФК-5. ***Результати навчання:***ПРН-15, ПРН-21, ПРН-25. ***Рекомендовані джерела:*** 1-7, 12,20.	Практичне заняття 1 3 год		Організація секретного діловодства
	Практичне заняття 2 4 год		Довідник кваліфікаційних характеристик професій працівників. Безпека господарської діяльності підприємства, установи, організації
	Практичне заняття 3 3 год		Перелік відомостей, що становлять службову інформацію і яким присвоюється гриф з обмеженим доступом «для службового користування»
	Лабораторне заняття 1 2 год		Правові аспекти безпеки інформаційної діяльності в Україні
	Самостійна робота		Указ президента України №685/2021 .Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року. Принципи впровадження політики безпеки. Організація допуску та доступу персоналу до конфіденційної інформації. Організація доступу до т. .аємної інформації. Захист службової інформації. Основні напрями захисту електронної інформації. Допуск посадових осіб та порядок оформлення допуску до державної таємниці. Організація секретного діловодства. Ознаками комерційної таємниці. Законодавство України про державну таємницю. Злочини, пов'язані з використанням комп'ютерів.
Тема 2. ***Технічні канали витоку інформації.*** ***Знати***: Поняття технічного каналу витоку інформації ТЗІ призначений для її захисту від витоку по технічних каналах витоку інформації. Побічні електромагнітні випромінювання.	Лекція 4 2 год	15	Лекція-візуалізація

Класифікація, причини та джерела створення технічних каналів витоку інформації. Узагальнена модель технічного каналу витоку інформації. Випромінювачі електромагнітних коливань. Загальні відомості про закладні устрої. Класифікація закладних устроїв. Характеристики та принцип дії ЗП. Акустичні ЗП. Мікрофони. Телефонні закладні устрої. Закладні устрої в засобах обчислювальної техніки. Лазерний з'єм акустичної інформації з вікон. Методичні вказівки з розробки методики виявлення закладних пристроїв. .***Вміти:*** обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності. ***Формування компетенцій:ЗК1, ЗК3, ЗК4,ФК-1, ФК-3, ФК-4, ФК-5, ФК-6, ФК-7, ФК-8.*** ***Результати навчання: РН-9, ПРН-17, ПРН-18, ПРН-21, ПРН-22, ПРН-24 ПРН-25, ПРН-28, ПРН-30 .*** ***Рекомендовані джерела: 1 -4,18,19,21-26.***	Лекція 5 4 год		Лекція-візуалізація
	Практичне заняття 4 2 год		Методичні вказівки з розробки методики виявлення закладних пристроїв
	Практичне заняття 5 2 год		Державний стандарт України ДСТУ 3396.0-96
	Самостійна робота		Технічні канали витоку інформації. Класифікація, причини та джерела створення. Узагальнена модель технічного каналу витоку інформації. Випромінювачі електромагнітних коливань Методичні вказівки з розробки методики виявлення закладних пристроїв..
Змістовий модуль 2 «Сучасні системи захисту інформації обмеженого доступу»			
Тема 3. ***Захист інформації обмеженого доступу*** ***Знати***: Загрози безпеці інформації. Класифікація атак. Методика класифікації загроз STRIDE. Порушники. Наслідки дій порушників. Стратегію та архітектуру захисту інформації. Політику безпеки інформації. Види забезпечення безпеки інформації. Захист програмного забезпечення від реасемблерів та налагоджувачів. Системний підхід до захисту ПЗ. Безпека інформаційних ресурсів у ІКСМ.	Лекція 6 4 год	25	Лекція-візуалізація
	Лекція 7 3 год		Лекція-візуалізація
	Лекція 8 3 год		Лекція-візуалізація
	Практичне заняття 6 2 год		Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС
	Практичне заняття 7		Вивчення міжнародного стандарту з оцінювання безпеки інформаційних технологій (ISO/IEC 15408)

Комплексні система захисту інформації. Об'єкти захисту та їхні властивості. Розроблення й оцінювання захищених систем. Адміністративний рівень інформаційної безпеки. Ідентифікація й аутентифікація, керування доступом. Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації. Формування вимог до КСЗІ. Технічне завдання на комплексну систему захисту інформації типового робочого місця зовнішнього користувача. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Методику оцінки захищеності інформації. .***<u>Вміти</u>***: обгрунтовувати та реалізовувати системи захисту інформаційних ресурсів з обмеженим доступом на об'єктах інформаційної діяльності; досліджувати загрози безпеці інформації. Проводити захист програмного забезпечення від реасемблерів та налагоджувачів, системний підхід до захисту ПЗ. Забезпечувати безпеку: інформаційних ресурсів у ІКСМ. адміністративний рівень інформаційної безпеки, ідентифікацію й аутентифікацію, керування доступом, правила проведення робіт із сертифікації засобів захисту інформації. ***<u>Формування компетенцій:ЗК1, ЗК3, ЗК4,ФК-1, ФК-4, ФК-5, , ФК-7. .</u>*** ***<u>Результати навчання: ПРН-9, ПРН-15, ПРН-17, ПРН-18, , ПРН-21, ПРН-24, ПРН-25, ПРН-30, ПРН-32.</u>*** ***<u>Рекомендовані джерела: 1-6,8-15,18,19,21-23,26.</u>***	2 год		
	Практичне заняття 8 2 год		Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації
	Практичне заняття 9 2 год		Формування вимог до КСЗІ
	Практичне заняття 10 2 год		Технічне завдання на комплексну систему захисту інформації типового робочого місця зовнішнього користувача
	Практичне заняття 11 2 год		Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах
	Практичне заняття 12 2 год		Методика оцінки захищеності інформації
	Лабораторне заняття 2 2 год		Створення конфіденційних документів
	Лабораторне заняття 3 4 год		Аудит в Windows
	Лабораторне заняття 4 4 год		Кількісна оцінка стійкості парольного захисту
	Лабораторне заняття 5 4 год		Захист від копіювання. Прив'язка до апаратного забезпечення. Використання реєстру
	Лабораторне заняття 6 4 год		Сканування мереж
	Лабораторне заняття 7		Ризики безпеки Інтернет-додатків

	2 год		
	Самостійна робота		Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації Технічне завдання на комплексну систему захисту інформації типового робочого місця зовнішнього користувача.
Тема 4. Моделі та способи захисту інформації з обмеженим доступом Знати: моделі захисту інформації, інформаційної безпеки. Рівні захисту інформації. Реалізацію ядра безпеки. Модель захисту інформації в межах держави. Модель довільного керування доступом. примусового керування доступом, Bell-LaPadula, Діона. MRDB з категоріями у складі міток безпеки, СЗІ реляційних СУБД, СЗІ MRDB, безпечної БД. Вимоги до моделей. Опис підходу до формування моделі ІБ. Програму оцінки ефективності систем захисту інформації"Оцінка СЗІ". Електронний цифровий підпис. Нормативні документи ТЗІ та етапи створення КСЗІ в ІТС. Аспекти захисту мовної інформації у корпоративній мережі зв'язку. Вимоги до ключових даних в середовищі хмарних обчислень. Модель порушника ІТС хмарних обчислень. Модель загроз відносно хмарних сервісів. Вміти: обгрунтовувати та реалізовувати системи захисту СКУД на об'єктах інформаційної діяльності, здійснювати вибір методів і засобів захисту інформації з обмеженим доступом на об'єктах інформаційної діяльності, розробляти проекти комплексів засобів	Лекція 9 2 год	5	Лекція-візуалізація
	Лекція 10 2 год		Лекція-візуалізація
	Самостійна робота		Рівні захисту інформації Реалізація ядра безпеки Модель захисту інформації в межах держави Експертиза в галузі технічного захисту інформації

захисту та охорони об'єктів інформаційної діяльності, здійснювати системний підхід. Проводити експертизу в галузі технічного захисту інформації. Створювати дієву структуру системи захисту інформації від НСД, концептуальну модель захисту інформації для технологій стаціонарного зв'язку, стільникового зв'язку. Обробляти результати досліджень моделі загроз та порушника відносно ключів. Формувати вимоги до КСЗІ. Розробляти технічне завдання на комплексну систему захисту інформації типового робочого місця зовнішнього користувача, методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Проводити сканування мереж. Налаштовувати параметри безпеки сучасних браузерів. Director ***Формування компетенцій:ЗК1, ЗК3, ЗК4,ФК-1, ФК-4, ФК-5, , ФК-7. .*** ***Результати навчання: ПРН-17, ПРН-18, ПРН-24, ПРН-25.*** ***Рекомендовані джерела: 5,-7,14-17,21-26***.			

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерне обладнання, мережа Інтернет ауд. 423.
- Навчальна лабораторія засобів контролю доступу «HIKVISION»
- Навчальна лабораторія технічного захисту інформації «PIAC»
- Програмне забезпечення. Windows XP, 8,10, Microsoft Office, Simple Passwords, Network Skanner, Comodo Firewall.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Закони України:

1. Закон України «Про інформацію» від 02.10.1992 № 2657-XII
2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
3. Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-ДСТУ 3396.0-96

5. ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ ДСТУ 33961-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт. http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?artid=38911&cat_id=3 8836.
6. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.

Укази президента:

7. № 685/2021Указ президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».
8. Указ президента України №685/2021. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". від 28 грудня 2021 року

Постанова Кабінету Міністрів України

9. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
10. Постанова Кабінету міністрів України «Про затвердження Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію» від 19 жовтня 2016 р. № 736[1]
11. Постанова Кабінету Міністрів України "Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури" від 19.06.2010 № 518.

Нормативні документи

12. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
13. НД 1.6-005-2013 Захист інформації на об'єктах інформаційної діяльності. Положення про категоріювання об'єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці. https://zakon.rada.gov.ua/rada/show/v0215519-13.
14. Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок. (ТР ТЗІ ПЕМВН-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id =101798&cat_id-89734&ctime=1344500065981
15. Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок (ТР ЕОТ-95). http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art id=120206&cat id=89769&ctime=1421836194327.
16. НД ТЗІ 1.5-001-2000 Радіовиявлювачі. Класифікація. Загальні технічні вимоги.
17. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. http://dstszi.kmu.gov.ua/dstszi/doccatalog/document?id=106342.

Основна

18. Technical Guide to Information Security Testing and Assessment. Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Murugiah Souppaya. Amanda Cody. Angela Orebaugh. NIST Special Publication 800-115. (Sep. 2008). 80 p. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf.
19. Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. Paul Cichonski. Tom Millar. Tim Grance. Karen Scarfone. Special Publication 800-61 Revision 2 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

20. Артемов В. Ю. Нормативно-правовий довідник з охорони інформації в Україні. У 4-х томах / Артемов В. Ю., Лєнков О. С., Пашков А. С., Стаднік О. М., Хорошко В. О. – К.: Вид. ДУІКТ, 2018.
21. Бабак В. П. Теоретические основы защиты информации / Бабак В. П., Ключников А. А. – НАН Украины, Ин-т проблем безопасности АЭС.– Чернобыль (Киев.обл.): Ин-т проблем безопасности АЭС, 2018.– с.776
22. Богуш В.М. Інформаційна безпека держави / В.М. Богуш, О.К. Юдін. – К. : "МК-Прес", 2018. – 432 с.
23. Ленков С. В. Методы и средства защиты информации. В 2-х томах /Ленков С. В., Перегудов Д. А., Хорошко В. А.– К.: Арий,2018.
24. Максименко Г.А., Хорошко В.А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. К: ПолиграфКонсал-тинг, 2020. 317 с.
25. Пащенко Р.Е. Красношапка І.В. Максюта Д.В. Генерування та формування сигналів. Харків: ХУПС. 2019. 200 с.
26. Хорев А.А. Техническая защита информации/ учеб. пособие для студентов вузов/ в 3-х томах. − т. 1: Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2018. - 436 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 встановлений термін.
- Якщо пошукувач 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 пошукувач повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Пошукувач, 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 пошукувач 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	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,5 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 бал
	•	

Додаткова оцінка	• Участь у наукових конференціях, підготовка наукових публікацій, отримання міжнародного сертифікату за напрямом.	Звільняється від екзамену
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	• Модульний контроль № 1 «Організаційне забезпечення та системи захисту інформації обмеженого доступу»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «Сучасні системи захисту інформації обмеженого доступу»	максимальна оцінка – 15 балів
	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від іспиту
	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій формі.	30 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 залікуу
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***екзамен***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання наукової роботи. Залік проходить у письмовій формі.	40 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	Критерії оцінювання	Рівень компетентності	Оцінка /*запис в екзаменаційній відомості*
90-100	**Аспірант 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 аспірант 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 аспіранта 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	**Аспірант демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналізможливих 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 аспіранту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / **Зараховано (В)**
75-81	**Аспірант 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/**	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання	Добре / **Зараховано (С)**

	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.	теоретичних положень для практичного використання викликають утруднення.	
64-74	**Аспірант** 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	Аспірант 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, аспірант 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	Аспірант може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни аспірант виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у аспіранта 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	Аспірант повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Аспірант не допущений до здачі заліку.	**Незадовільний** Аспірант не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / **Не допущений (F)** *В заліковку книжку не проставляється*