СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ»

Лектор курсу			**Довженко Надія Михайлівна**, кандидат технічних наук, доцент		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** nadezhdadovzhenko@gmail.com; **сторінка курсу в Moodle –** http://dl.dut.edu.ua/course/view.php?id=64	
Галузь знань			12 «Інформаційні технології»		**Рівень вищої освіти**	Другий (магістр)	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	10	
Освітня програма			Інформаційна та кібернетична безпека		**Тип дисципліни**	Професійної та практичної підготовки	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	6	180	18	-	18	18	126

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Технології виявлення уразливостей мережевих ресурсів, Прикладна загальна теорія систем ІК
Освітні компоненти для яких є базовою	Управління проектами інформаційної безпеки

Мета курсу:	опанування основних положень щодо організації та реалізації захисту інформації телекомунікаційних систем та мереж, комплексного забезпечення інформаційної безпеки систем та мереж, вивчення принципів та одержання практичних навичок створення безпечної мережевої інфраструктури.

Компетентності відповідно до освітньої програми

Компетентність (КФ)

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

Результати навчання (РН)

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1. Технології організації та забезпечення безпеки мережевої інфраструктури			
Тема 1. Інформаційні технології організації безпеки мережевої інфраструктури **Лекція 1. Моделі управління мережевими ресурсами.** ***Знати***: принципи створення надійної та безпечної мережевої інфраструктури; ***Вміти:*** застосовувати системний підхід для запобігання загроз безпеці мережевої інфраструктури; ***Компетенції:*** КЗ-1, КЗ-4, КФ-1 ***Результати навчання:*** РН-4, РН-5 ***Рекомендовані джерела:*** 1-5	Лекція 1 2 год		**Лекція №1. Моделі управління мережевими ресурсами.** 1. Модель робочої групи (модель розподіленого управління) 2. Модель домена (модель централізованого управління)
	Практичне заняття 1 2 год		**Практична робота №1. Профіль безпеки стандарту ISO/OSI.** 1.Профіль безпеки для заданих сервісів безпеки їх комбінацій і додатків 2.Обґрунтувати запропонованого профілю
	Лабораторна робота 1 2 год		**Лабораторна робота №1. Основні команди комутаторів. Управління комутаторами.** 1. Налаштування DES - 3200-28 2. Управління обліковими записами користувачів 3. Налаштування параметрів ідентифікації комутатора

Тема 1. Інформаційні технології та принципи організації інформаційної безпеки. Тема 2. Моделі управління мережевими ресурсами. Тема 3. Програмні та апаратні засоби захисту в інформаційних системах Тема 4. Технології захисту інформації при міжмережевій взаємодії Тема 5. Технології захисту у мережах на основі протоколів TCP/IP.	Самостійна робота		
Тема 1. Інформаційні технології організації безпеки мережевої інфраструктури. **Лекція 2. Програмні та апаратні засоби захисту в інформаційних системах.** ***Знати***: основи застосування інформаційних технологій та систем безпеки мережевої інфраструктури; ***Вміти***: здійснювати аналіз та оцінку загроз безпеці мережевої інфраструктури; ***Компетенції:*** КЗ-1, КЗ-4, КФ-1, КФ-3 ***Результати навчання:*** РН-5, РН-6 ***Рекомендовані джерела:*** 1–5	Лекція 2 2 год		**Лекція №2. Програмні та апаратні засоби захисту в інформаційних системах.** 1. Програмні засоби забезпечення захисту інформації 2. Технічні (апаратні) засоби забезпечення захисту інформації
	Практичне заняття 2 2 год		**Практична робота №2. Виявлення мережевих атак шляхом аналізу трафіка.** 1. Основи захвату та аналізу мережевого трафіка 2. Виявлення мережевих атак шляхом аналізу трафіка
	Лабораторна робота 2 2 год		**Лабораторна робота №2. Команди оновлення програмного забезпечення комутатора і збереження відновлення конфігураційних файлів.** 1. Підготовка до режиму оновлення і збереження програмного забезпечення комутатора 2. Управління обліковими записами користувачів 3. Налаштування порядку загрузки программного забезпечення комутатора 4. Вивантаження Log -файлов
Тема 6. Виявлення мережевих атак шляхом аналізу трафіка. Тема 7. Тенденції розвитку і застосування методів і засобів захисту інформації в телекомунікаційних системах. Тема 8. Захист інформації в корпоративних мережах.	Самостійна робота		
Тема 2. Методи і засоби забезпечення безпеки мережевої інфраструктури. **Лекція 3. Захист інформації в корпоративних мережах..**	Лекція 3 2 год		**Лекція №3. Захист інформації в корпоративних мережах.** 1. Основи і мета політики безпеки в корпоративних мережах 2. Багаторівневий захист корпоративних мереж

Знати: принципи створення надійної та безпечної мережевої інфраструктури; ***Вміти***: знаходити основні шляхи щодо реалізації методів та заходів забезпечення безпеки мережевої інфраструктури; ***Компетенції:*** КФ-5, КЗ-4, КФ-7 ***Результати навчання:*** РН-8, РН-11 ***Рекомендовані джерела:*** 1-5	Практичне заняття 3 2 год		**Практична робота №3. Команди протоколу IEEE 802.1X**. 1. Вивчення команд протоколу 802.1X 2. Налаштування аутентификации 802.1X на основі портів 3. Налаштування аутентификации 802.1X на основі MAC-Адрес
	Лабораторна робота 3 2 год		**Лабораторна робота №3. Команди моніторингу працездатності комп'ютерної мережі.** 1. Вивчення команд перегляду утилізації (завантаження) портів і CPU комутатора 2. Вивчення команд перегляду статистики/помилок переданих пакетів на порту комутатора 3. Вивчення команд перегляду сесій підключених до комутатора користувачів і Log-Файлу комутатора
Тема 9. Принципи та методи надання доступу до інформаційних ресурсів. Тема 10. Профіль безпеки стандарту ISO/OSI. Тема 11. Передача потоку даних. Багатоадресна розсилка Тема 12. Команди агрегування каналів. Тема 13. Аутентифікація користувачів за стандартом IEEE Std 802.ÏX. Тема 14.Команди протоколу IEEE 802.1X. Тема 15. Створення гостьової VLAN з обмеженими правами для користувачів (802.1X Guest VLAN). Тема 16. Команди моніторингу працездатності комп'ютерної мережі.	Самостійна робота		
Тема 2. Методи і засоби забезпечення безпеки мережевої інфраструктури. **Лекція 4. Принципи та методи надання доступу до інформаційних ресурсів.** ***Знати***: основні програмні та апаратні засоби забезпечення захисту інформації у мережевої інфраструктури; ***Вміти***: знаходити основні шляхи щодо реалізації методів та заходів забезпечення безпеки мережевої інфраструктури; ***Компетенції:*** КЗ-1, КЗ-4, КФ-1, КФ-3, КФ-8 ***Результати навчання:*** РН-8, РН-1, РН-13 ***Рекомендовані джерела:*** 1–5	Лекція 4 2 год		**Лекція №4. Принципи та методи надання доступу до інформаційних ресурсів.** 1. Принципи забезпечення доступу до інформаційних ресурсів. 2. Методи ідентифікації і аутентифікації користувачів 3. Методи контролю доступу
	Практичне заняття 4 2 год		**Практична робота №4. Команди настроювання протоколів єднального дерева STP, RSTP, MSTP.** 1. Налаштування протоколу RSTP (IEEE 802.1w) 2. Налаштування протоколу MSTP (IEEE 802.1s) для кожної VLAN

			3. Налаштування протоколу MSTP (IEEE 802.1s) для балансування навантаження
	Лабораторна робота 4 2 год		**Лабораторна робота №4. Функція запобігання петлеутворення (Loopback Detection).** 1. Налаштування Loopback Detection Independent STP у режимі Port-Based 2. Налаштування функції Loopback Detection Independent STP у режимі Vlan-based (для версії LBD 4.0).
Тема 17. Аутентифікація користувачів за стандартом IEEE Std 802.ÏX. Тема 18. Команди протоколу IEEE 802.1X. Тема 19. Створення гостьової VLAN з обмеженими правами для користувачів (802.1X Guest VLAN). Тема 20. Команди моніторингу працездатності комп'ютерної мережі.	Самостійна робота		
Тема 2. Методи і засоби забезпечення безпеки мережевої інфраструктури. **Лекція 5.** Системи виявлення вторгнень. ***Знати***: основні програмні та апаратні засоби забезпечення захисту інформації у мережевої інфраструктури; ***Вміти***: знаходити підходи щодо оцінки рівня безпеки мережевої інфраструктури ***Компетенції:*** КФ-5, КФ-7, КФ-8 ***Результати навчання:*** РН-11, РН-17, РН-21 ***Рекомендовані джерела:*** 1–5	Лекція 5 2 год		**Лекція №5. Системи виявлення вторгнень.** 1. Загальні відомості про системи виявлення вторгнень. 2. Визначення типів систем виявлення вторгнень 3. Створення політики виявлення вторгнень. 4. Визначення цілей застосування та об'єкти моніторингу IDS 5. Види обробки подій, встановлення порогів.
Тема 21. Системи виявлення вторгнень. Тема 22. Створення політики виявлення вторгнень. Тема 23. Практика застосування політики IDS. Тема 24. Команди управління таблицями MAC, IP, ARP. Тема 25. Контроль над підключенням вузлів до портів комутатора. Тема 26. Функція Port Security.	Самостійна робота		

Тема 27. Функція запобігання петлеутворення (Loopback Detection). Тема 28. Команди настроювання протоколів єднального дерева STP, RSTP, MSTP.			
Змістовий модуль 2. Побудова захищеної мережевої інфраструктури			
Тема 3. Функції забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI **Лекція 6. Методи і засоби аналізу безпеки програмного забезпечення.** ***Знати***: основні програмні та апаратні засоби забезпечення захисту інформації у мережевої інфраструктури; ***Вміти***: розробляти рекомендацій та застосовувати заходи із забезпечення захисту інформаційних систем та мереж. ***Компетенції:*** КФ-3, КФ-5, КФ-8 ***Результати навчання:*** РН-8, РН-11, РН-17, РН-21 ***Рекомендовані джерела:*** 1–5	Лекція 6 2 год		**Лекція №6. Методи і засоби аналізу безпеки програмного забезпечення.** 1. Контрольно-випробні методи аналізу безпеки програмного забезпечення 2. Логіко-аналітичні методи контролю безпеки програм
	Практичне заняття 5 2 год		**Практична робота №5. Команди VLAN на основі портів і стандарту IEEE 802.1Q** 1. Налаштування VLAN на основі портів 2. Налаштування VLAN на основі стандарту IEEE 802.1Q Оптимізація налаштування комутаторів з великою кількістю VLAN
	Лабораторна робота 5 2 год		**Лабораторна робота №5. Команди управління таблицями MAC, IP, ARP**. 1. Вивчення команд перегляду таблиць MAC-адрес. 2. Вивчення команд перегляду таблиць комутації IP-адрес 3. Вивчення команд перегляду ARP-таблиць.
Тема 29. Методи і засоби аналізу безпеки програмного забезпечення Тема 30. Планування захищеної мережі. Тема 31. Методика створення списків управління доступом (ACL). Тема 32. Основні команди комутаторів. Управління комутаторами. Тема 33. Команди оновлення програмного забезпечення комутатора і збереження відновлення конфігураційних файлів. Тема 34. Списки керування доступом (Access Control List).	Самостійна робота		
Тема 3. Функції забезпечення безпеки мережевої інфраструктури відповідно рівнів моделі OSI **Лекція 7. Забезпечення безпеки на фізичному рівні моделі OSI.** ***Знати***: основи застосування інформаційних технологій та систем безпеки мережевої інфраструктури; ***Вміти***: розробляти рекомендацій та застосовувати заходи із забезпечення захисту інформаційних систем та мереж	Лекція 7 2 год		**Лекція №7. Забезпечення безпеки на фізичному рівні моделі OSI.** 1. Комунікаційні сигнали та кодування. 2. Забезпечення безпеки на фізичному рівні
	Практичне заняття 6 2 год		**Практична робота №6. Команди налаштування функції Q-in-Q (Double VLAN)** 1. Налаштування функції Port-based Q-in-Q 2. Налаштування функції Q-in-Q qinq ports all

Компетенції: КФ-5, КФ-7, КФ-8 ***Результати навчання:*** РН-11, РН-17, РН-21 ***Рекомендовані джерела:*** 1–5	Лабораторна робота 6 2 год		**Лабораторна робота №6. Контроль над підключенням вузлів до портів комутатора. Функція Port Security.** 1. Налаштування керування кількістю користувачів, що підключаються до портів комутатора, шляхом обмеження максимальної кількості досліджуваних MAC-Адрес 2. Налаштування порядку загрузки программного забезпечення комутатора 3. Налаштування захисту від підключення до портів, заснованої на статичній таблиці MAC-Адрес
	Лабораторна робота 7 2 год		**Лабораторна робота №7. Команди агрегування каналів.** 1. Налаштування статичного агрегування каналів 2. Налаштування динамічного агрегування каналів (LACP) 3. Налаштування динамічного агрегування каналів (LACP) при розподілі каналів між трьома комутаторами.
Тема 35. Забезпечення безпеки на фізичному рівні моделі OSI. Тема 36. Забезпечення безпеки на транспортному рівні моделі OSI. Тема 37. Забезпечення безпеки на канальному рівні моделі OSI. Тема 38. Забезпечення безпеки на рівні додатків моделі OSI. Тема 39. Забезпечення безпеки на мережному рівні моделі OSI. Тема 40. Особливості реалізації VLAN стандарту 802.1Q. Тема 41. Команди VLAN на основі портів і стандарту IEEE 802.1Q Тема 42. Особливості реалізації VLAN з розширеннями стандарту IEEE 802.1Q. Тема 43. Команди налаштування функції Q-in-Q (Double VLAN)	Самостійна робота		
Тема 4. Побудова захищеної мережевої інфраструктури **Лекція 8. Планування захищеної мережі.** ***Знати***: основні програмні та апаратні засоби забезпечення захисту інформації у мережевої інфраструктури; ***Вміти***: знаходити основні шляхи щодо реалізації методів та заходів забезпечення безпеки мережевої інфраструктури; ***Компетенції:*** КЗ-1, КЗ-4, КФ-5, КФ-8 ***Результати навчання:*** РН-6, РН-13, РН-71 ***Рекомендовані джерела:*** 1-5	Лекція 8 2 год		**Лекція №8. Планування захищеної мережі.** 1. Організація захищеного підключення 2. Розробка схеми адресації
	Практичне заняття 7 2 год		**Практична робота №7. Контроль над підключенням вузлів до портів комутатора. Функція IP-MAC-port** 1. Налаштування роботи функції IP-MAC-port Binding у режимі ARP 2. Налаштування роботи функції IP-MAC-port Binding у режимі ACL
	Лабораторна робота 8 2 год		**Лабораторна робота №8. Команди налаштування асиметричних VLAN і сегментації трафіку. Застосування асиметричних VLAN (Asymmetric VLAN).** 1. Налаштування асиметричних VLAN 2. Налаштування сегментації трафіку
	Практичне заняття 8		**Практична робота №8. Настроювання QoS. Пріоритезація трафіка**

	2 год		1. Налаштування пріоритету за замовчуванням на портах комутаторів 2. Механізм обслуговування черг пріоритетів Weighted Round Robin
Тема 44. Принципи забезпечення доступу до інформаційних ресурсів Тема 45. Технології захисту у мережах на основі протоколів TCP/IP Тема 46. Канальний рівень. Механізми доступу до середовища Тема 47. Функції контролю підключення вузлів до портів комутатора. Тема 48. Технології побудови віртуальних локальних мереж (VLAN). Тема 49. Команди налаштування асиметричних VLAN і сегментації трафіку. Тема 50. Застосування асиметричних VLAN (Asymmetric VLAN). Тема 51. Контроль над підключенням вузлів до портів комутатора. Функція IP-MAC-port	Самостійна робота		
Тема 4. Побудова захищеної мережевої інфраструктури **Лекція 9. Технології побудови віртуальних локальних мереж (VLAN).** ***Знати***: основні програмні та апаратні засоби забезпечення захисту інформації у мережевої інфраструктури; ***Вміти***: розробляти рекомендацій та застосовувати заходи із забезпечення захисту інформаційних систем та мереж. ***Компетенції:*** КЗ-4, КФ-5, КФ-6, КФ-7 ***Результати навчання:*** РН-6, РН-8, РН-17 ***Рекомендовані джерела:*** 1-5	Лекція 9 2 год		**Лекція №9. Технології побудови віртуальних локальних мереж (VLAN).** 1. Логічна сегментація мереж за допомогою технології VLAN. 2. Типи побудови віртуальних локальних мереж (VLAN).
	Практичне заняття 9 2 год		**Практична робота №9. Команди протоколу GVRP (просування інформації про VLAN в мережі)** 1. Опанування роботи протоколу GVRP 2. Налаштування динамічної передачі інформації про VLAN через магістральні комутатори
	Лабораторна робота 9 2 год		**Лабораторна робота №9. Обмеження адміністративного доступу до керування комутатором.** 1. Налаштування «довіреного вузла» (Trusted Host) 2. Включення режиму шифрування паролів облікових записів у конфігураційних формах 3. Налаштування Web-Консолі (по протоколу SSL)
Тема 52. Настроювання QoS. Пріоритезація трафіка Тема 53. Особливості реалізації статичних і динамічних VLAN Тема 54. Команди протоколу GVRP (просування інформації про VLAN в мережі) Тема 55. Обмеження адміністративного доступу до керування комутатором	Самостійна робота		

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Комп‘ютерне обладнання, Cisco Packet Tracer, GNS3, мережа Інтернет ауд. 419.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Бурячок В. Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. Київ. ДУТ. 2015. 449 с.
2. Chris Carthern, William Wilson, Noel Rivera. Cisco Networks. Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA. Apress, 2018.1117p.
3. Карпенко М. Ю., Макогон Н. В. Конспект лекцій з курсу «Комп’ютерні мережі». Харків. ХНУМГ ім. О. М. Бекетова. 2019. 99 с.
4. Жураковський Б. Ю. Комп’ютерні мережі. Частина 1. Навчальний посібник. Київ. КПІ ім. Ігоря Сікорського. 2020. 336 с.
5. Enterprise Networking, Security, and Automation Companion Guide (CCNAv7). Cisco Networking Academy. Cisco Press. 2020.
6. Joseph Muniz, Gary McIntyre, Nadhem AlFardan. Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press. 2020. 448 p.
7. Omar Santos, Panos Kampanakis, Aaron Woland. Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP. Cisco Press. 2016. 368 p.

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 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

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 0,5 бала
	• звіт про виконання практичного завдання	за кожен звіт максимум 1 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання подальшої роботи. 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	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)

	кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .		
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*