СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«УПРАВЛІННЯ БЕЗПЕКОЮ ІНФОРМАЦІЙНИХ МЕРЕЖ»

Лектор курсу			**Мужанова Тетяна Михайлівна**, кандидат наук з держ.упр., доц., доцент кафедри управління інформаційною та кібербезпекою		**Контактна інформація лектора (e-mail), сторінка курсу в Moodle**	**e-mail:** muzanovat@gmail.com; **сторінка курсу в Moodle –** https://dn.dut.edu.ua/course/view.php?id=408	
Галузь знань			12 «Інформаційні технології»		**Рівень вищої освіти**	магістр	
Спеціальність			125 «Кібербезпека»		**Семестр**	10	
Освітня програма			«Управління інформаційною безпекою»		**Тип дисципліни**	Вибіркова	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	36	-	36

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Менеджмент інформаційної безпеки Організаційне забезпечення захисту інформації
Освітні компоненти для яких є базовою	Аудит інформаційної безпеки Ефективність управління інформаційною безпекою
Мета курсу:	набуття студентами компетенцій, знань, умінь і навичок з питань організації та забезпечення безпеки інформаційних мереж, розглядаючи їх як комплекс технічних, інформаційних та програмних засобів, що призначені для вирішення широкого кола завдань забезпечення безпеки інформаційних процесів; формування необхідних теоретичних знань та практичних навичок у галузі побудови та функціонування систем інформаційної безпеки і комп'ютерних технологій та можливостей їх використання.

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності спеціальності (КФ)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях **КЗ6.** Здатність використовувати інформаційні і комунікаційні технології для впровадження проектів в інформаційній та безпековій сферах.	**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.

Програмні результати навчання (ПРН)

РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного

захисту інформації у кіберпросторі.
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.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1 Інформаційна мережа, базові поняття та проблеми функціонування			
Тема 1. Базові поняття в області безпеки інформаційних мереж. SIEM-системи, як технології управління інформаційною безпекою мережі. Технології управління інформаційними мережами. ***Знати***: 1. Базові поняття в області безпеки інформаційних мереж. 2. Системи моніторингу та управління безпекою інформаційної мережі. 3. Походження SIEM-систем та принципи їх роботи. 4. Перелік світових компаній, лідерів-розробників SIEM–систем 5. Системи управління інформаційними мережами. ***Вміти:*** використовувати теоретичні знання у практичних ситуаціях, оцінювати системи управління інформаційними мережами відповідно до різних методів управління безпекою і відповідністю. ***Формування компетенцій:*** К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 1	5,5*	Лекція-візуалізація, встановлення зв'язку з попередніми дисциплінами
	Практичне заняття 1		Коротке повторення матеріалу попередніх лекцій, робота в малих групах за темою «Технології управління інформаційними мережами». Підготовка презентацій за результатами роботи групи.
Тема 2. Методичний апарат оцінки рівня ІБ на основі стандарту COBIT. Систематизація операційних ризиків, пов'язаних з ІБ мереж. Інформаційні технології в банківській системі. Аналіз загроз ІБ мереж. ***Знати***: 1. Загальні положення стандарту COBIT. 2. Управління та аудит ІТ-процесів забезпечення ІБ відповідно до COBIT. 3. Види ризиків інформаційній безпеці мереж. 4. Банківські інформаційні системи. 5. Технології управління ІБ банківських інформаційних мереж. ***Вміти***: Систематизувати операційні ризики, пов'язані з ІБ мереж, аналізувати загрози ІБ мереж, в т.ч. банківських ІС, застосовувати на практиці знання принципів управління й аудиту ІТ-процесів забезпечення ІБ відповідно до стандарту COBIT. ***Формування компетенцій:*** К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 2	5,5*	Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача)
	Практичне заняття 2		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Систематизація операційних ризиків, пов'язаних з інформаційною безпекою мереж»
	Практичне заняття 3		Індивідуальні виступи за результатами самостійного вивчення теми «Технології управління ІБ банківських інформаційних мереж».
	Практичне заняття 4		Усне експрес-опитування за матеріалами попередньої лекції, Індивідуальні виступи за результатами самостійного вивчення теми «Хмарні технології».

Тема 3. Забезпечення інформаційної безпеки мереж. Політика безпеки інформаційних мереж. Основні поняття політики безпеки. Структура політики безпеки організації. Технологія побудови і використання VPN-мереж ***Знати***: 1. Методи забезпечення інформаційної безпеки мереж. 2. Шляхи вирішення проблем захисту інформації в мережах. 3. Основні поняття і структура політики безпеки організації. 4. Методи забезпечення ІБ мереж, створених на базі VPN-технологій ***Вміти***: розробляти проекти політики ІБ мереж, аналізувати шляхи вирішення проблем захисту інформації в мережах, застосовувати інформаційно-аналітичні методи для їх аналізу, оцінювати й обирати методи забезпечення ІБ мереж, створених на базі VPN-технологій. ***Формування компетенцій:*** К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 3	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення теми «Використання VPN-технології в процесі побудови інформаційних мереж». Розробка узагальнених рекомендацій.
	Практичне заняття 6		Робота в малих групах за темою «Політика безпеки інформаційних мереж». Підготовка проектів політики ІБ мереж і їх презентація.
Тема 4. Аналіз загроз мережевої безпеки інформаційних систем. Інформаційна безпека SCADA систем. Технології виявлення атак на інформаційні мережі. ***Знати***: 1. Методи забезпечення інформаційної безпеки мереж та шляхи вирішення проблем захисту інформації в мережах. 2. Загрози та вразливості дротових і бездротових корпоративних мереж. 3. Поняття, загальні принципи побудови і безпеки SCADA-систем. 4. Класифікація систем виявлення атак IDS. ***Вміти***: використовувати методи забезпечення ІБ мереж на практиці, виявляти й аналізувати загрози та вразливості дротових та бездротових корпоративних мереж, аналізувати мережеву інформацію, класифікувати системи виявлення атак IDS ***Формування компетенцій:*** К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 4	5,5*	Лекція-візуалізація, експрес-опитування студентів, письмова перевірка знань (за рішенням викладача)
	Практичне заняття 7		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення теми «Інформаційна безпека SCADA систем». Розробка узагальнених рекомендацій.
	Практичне заняття 8		Практичне опрацювання матеріалів за темою «Технології виявлення атак на інформаційні мережі. IDS-атаки» **Проведення контрольної роботи № 1**
Тема 1. Системи моніторингу та управління безпекою інформаційної мережі (DLP, SIEM). **Тема 2.** Управління інформаційною безпекою на стратегічному рівні. **Тема 3.** VPN-технології як засіб забезпечення ІБ мереж. Переваги і недоліки. **Тема 4.** SCADA-системи як засіб контролю і збору інформації. Переваги і недоліки.	Самостійна робота		1. Можливості, принципи побудови та особливості використання DLP і SIEM- систем. 2. Принципи організації ІБ на стратегічному рівні підприємства. Розробка стратегій та концепцій управління інформаційною безпекою інформаційних мереж. 3. Види VPN-технологій та їх функції. Порівняльна характеристика продуктів різних виробників. 4. Архітектура SCADA-систем. Призначення, структура і основні функції SCADA-систем. 5.

Змістовий модуль 2 Технології управління безпекою інформаційних мереж			
Тема 5. Електронний цифровий підпис і функція хешування. Біометричні методи управління безпекою інформаційних мереж. Методи аутентифікації користувачів інформаційної мережі. ***Знати***: 1. Основні процедури цифрового підпису та функція хешування. 2. Засади використання біометричних методів. Дактилоскопічні системи аутентифікації. 3. Технології аутентифікації. 4. Основні недоліки систем аутентифікації. ***Вміти***: застосовувати практично знання щодо засад використання й забезпечення безпеки ЕЦП, основних систем аутентифікації, в тому числа біометричних методів встановлення ідентичності. ***Формування компетенцій:*** К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 5	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Біометричні методи управління безпекою інформаційних мереж». Формування висновків з теми.
	Практичне заняття 10		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення питань щодо методів аутентифікації користувачів інформаційної мережі. Дискусія. Визначення основних недоліків різних систем аутентифікації.
Тема 6. Алгоритми шифрування. Технології захисту на канальному, сеансовому та прикладному рівнях. Протокол Kerberos. ***Знати***: 1. Класифікація алгоритмів шифрування. 2. Принципи роботи симетричних та асиметричних алгоритмів шифрування, їх недоліки систем. 3. Протоколи формування захищених каналів на канальному та сеансовому рівнях. 4. Захист мережевого рівня. 5. Протокол Kerberos, функціонування та недоліки. 6. Організація захищеного віддаленого доступу, принцип дії, протоколи, недоліки. 3. Управління ідентифікацією та доступом. ***Вміти:*** застосовувати на практиці вимоги до формування захищених каналів на канальному, сеансовому та мережевому рівнях, принципи організації захищеного віддаленого доступу, управління ідентифікацією та доступом користувача. ***Формування компетенцій:*** К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 6	5,5*	Лекція-візуалізація, експрес-опитування студентів, письмова перевірка знань (за рішенням викладача)
	Практичне заняття 11		Практичне опрацювання матеріалів за темою «Технології захисту на канальному та сеансовому рівнях».
	Практичне заняття 12		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення теми «Технології захисту на прикладному рівні. Протокол Kerberos. Організація захищеного видаленого доступу. Управління ідентифікацією та доступом».
Тема 7. Архітектура підсистем захисту операційної системи. Використання технології міжмережевих екранів. Основні недоліки. Мобільні пристрої в корпоративних інформаційних мережах.	Лекція 7	5,5*	Лекція-візуалізація, експрес-опитування студентів

Знати: 1. Основні функції підсистем захисту операційної системи. 2. Проблеми забезпечення ІБ операційних систем. 3. Основні функції міжмережевих екранів. 4. Варіанти реалізації мережевого захисту на базі між мережевих екранів. 5. Використання мобільних пристроїв в інформаційних мережах (системах). 6. Загрози використання й методи захисту мобільних пристроїв в корпоративних мережах. ***Вміти***: застосовувати отримані знання для вирішення проблем безпеки ОС, аналізувати й обирати варіанти реалізації мережевого захисту на базі міжмережевих екранів, виявляти й оцінювати ризики й загрози ІБ мобільних пристроїв у корпоративних мережах. ***Формування компетенцій:*** КЗ1, КЗ6, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Практичне заняття 13		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Технології міжмережевих екранів», підготовка рекомендацій щодо переваг і недоліків різних варіантів реалізації мережевого захисту на базі міжмережевих екранів.
	Практичне заняття 14		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення питань щодо безпеки мобільних пристроїв у корпоративних інформаційних мережах». Аналіз загроз використання мобільних пристроїв в корпоративних мережах.
Тема 8. Технологія аналізу захищеності інформаційних мереж. Технологія та засоби захисту корпоративних інформаційних мереж. Базові налаштування політики SRP на робочих станціях інформаційної мережі. ***Знати***: 1. Аналіз захищеності мережевих протоколів, сервісів та операційних систем. 2. Методика аналізу захищеності інформаційних систем. 3. Основні напрями захисту корпоративних мереж. 4. Види сканерів безпеки корпоративних ІТ-систем. 5. Механізм SRP та його налаштування. ***Вміти:*** аналізувати стан захищеності мережевих протоколів, сервісів та операційних систем відповідно до розглянутої методики, оцінювати й обирати напрями й методи захисту корпоративних мереж, виявляти й усувати проблеми у системі захисту мереж. ***Формування компетенцій:*** КЗ1, КЗ6, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Лекція 8	5,5*	Лекція-візуалізація, експрес-опитування студентів, письмова перевірка знань (за рішенням викладача)
	Практичне заняття 15		Індивідуальні виступи за результатами самостійного вивчення теми «Технологія та засоби захисту корпоративних інформаційних мереж». Дискусія та вироблення рекомендацій щодо основних напрямів захисту корпоративних мереж».
	Практичне заняття 16		Практичне опрацювання матеріалів за темою «Базові налаштування політики SRP на робочих станціях інформаційної мережі та усунення можливих проблем».
Тема 9. Програмні методи адміністрування та аналізу інформаційної мережі. Хмарні технології. ***Знати***: 1. Можливості програмних засобів адміністрування інформаційної мережі. 2. Налаштування та робота програм сканування інформаційної мережі. 6. Принципи побудови ІС на базі хмарних технологій. 7. Проблемні питання впровадження хмарних технологій. 8. Методи забезпечення ІБ мереж, створених на базі хмарних технологій. ***Вміти***: використовувати на практиці знання щодо налаштування та роботи програм сканування інформаційної мережі, методів забезпечення ІБ мереж, створених на базі хмарних технологій.	Лекція 9	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 17		Індивідуальні виступи за результатами самостійного вивчення питань налаштування та робота програм сканування інформаційної мережі.

Формування компетенцій: К31, К36, КФ3, КФ8 ***Результати навчання:*** РН2, РН3, РН5, РН13 ***Рекомендовані джерела:*** 1-7.	Практичне заняття 18		Робота у малих групах. Практичне опрацювання матеріалів за темою «Методи забезпечення ІБ мереж, створених на базі хмарних технологій». Підготовка узагальненої схеми за темою. **Проведення контрольної роботи № 2**
Тема 5. Методи аутентифікації користувачів інформаційної мережі. **Тема 6.** Протокол мережевої аутентифікації Kerberos: засади функціонування та недоліки. **Тема 7.** Новітні підходи до захисту мобільних пристроїв у корпоративних інформаційних мережах. **Тема 8.** Проблеми управління безпекою інформаційних мереж в умовах зростання обсягів віддаленої роботи. **Тема 9.** Управління безпекою хмарних технологій.	Самостійна робота		1. Двохфакторна аутентифікація. Логічні, ідентифікаційні та біометричні методи аутентифікації користувачів інформаційної мережі. 2. Протокол Kerberos. Аутентифікатори. Управління ключами та сеансові мандати. 3. Загрози та вразливості у захисті мобільних пристроїв. Системи DLP, MDM, MAM та EEM у захисті мобільних пристроїв, даних та додатків. 4. Види загроз інформаційній безпеці в режимі віддаленого доступу. Методи підвищення інформаційної безпеки мереж, пристроїв і даних. 5. Управління безпекою хмарних технологій. Стримуюче управління. Профілактичне управління. Детективне управління. Коригуюче управління.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- Мультимедійний проектор;
- Комп'ютерний клас для проведення практичних занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

Навчальні посібники:

1. Інформаційна безпека в комп'ютерних мережах : навч. посіб. / О.А. Смірнов, О.К. Конопліцька-Слободенюк, С.А. Смірнов [та ін.] ; М-во освіти і науки України, Центральноукраїн. нац. техн. ун-т. - Кропивницький : Лисенко В.Ф., 2020. 295 с. URL:http://dspace.kntu.kr.ua/jspui/bitstream/123456789/9799/1/Inform_bezp_komp_mer.pdf
2. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак ; КПІ ім. Ігоря Сікорського. Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с. URL: https://ela.kpi.ua/bitstream/123456789/38326/1/Information_security_NP.pdf
3. Соколов В.Ю. Безпека безпроводових і мобільних мереж : Навчальний посібник / В.Ю. Соколов, В.Л. Бурячок, М.М. Тадждіні / ред. перекл. О. П. Райтер. 2 вид., доп. К. : КУБГ, 2019. 130 с.
4. Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур». Державний університет телекомунікацій. К.:ДУТ, 2019. 163 с. 166 с.
5. Домарєв, В.В., Домарєв Д.В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k). Донецьк: «Велстар», 2012. 146 с.
6. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І.. Телекомунікаційні та інформаційні мережі. URL: http://www.dut.edu.ua/ua/lib/2/category/742/view/472
7. Захарченко М.В., Вараксін О.О., Кононович В.Г., Вараксін С.О. Протоколи, термінальне обладнання та інформаційна безпека у мережах наступного покоління. 2013. URL: http://www.dut.edu.ua/ua/lib/1/category/1222/view/499

Додаткові джерела:

1.Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах : Постанова КМУ від 16.11.2002, № 1772. URL: https://zakon.rada.gov.ua/laws/show/1772-2002-%D0%BF#Text
2.Деякі питання забезпечення функціонування державних інформаційних ресурсів : Постанова КМУ від 30 грудня 2022 р. № 1500. URL: https://zakon.rada.gov.ua /laws/show/1500-2022-%D0%BF#Text

3.НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 24.04.1999 р. № 22 Чинний від 01.07.1999 р.
4.НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 28.04.1999 р. № 22 Чинний від 01.07.1999 р.
5.НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53 Чинний від 15.12.2000 р.
Електронні ресурси:
1. Законодавство України. URL: https://zakon.rada.gov.ua
2. Сторінка ДССЗЗІ України. URL: https://cip.gov.ua/ua
3. Журнал "Информационные технологии. Аналитические материалы". URL: http://it.ridne.net
4. Історія розвитку інформаційних технологій в Україні. URL: http://www.icfcst.kiev.ua/MUSEUM/ITu.html
5. Системи безпеки і відеонагляду. URL: http://bezopasnost.biz
6. OpenPGP. URL: www.pgpi.org.
7. Computer security vulnerabilities. URL: www.securityfocus.com

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу індивідуально і в групах.
- Середовище в аудиторії є інтерактивним, творчим, відкритим до дискусії та взаємодопомоги.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій, семінарських та практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем, які не ввійшли в теоретичний курс, або були розглянуті коротко, їх поглиблене опрацювання на основі рекомендованої літератури, практичне оволодіння навичками аналітичного характеру, методами роботи з літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він надає викладачу виконані завдання в індивідуальному порядку.
- Під час роботи над завданнями не допустимо порушення вимог академічної доброчесності: при використанні Інтернет-ресурсів та інших джерел інформації студент має посилатися на використане джерело. Не допускається підказування й допомога студенту з боку одногрупників під час виконання індивідуальних завдань. У разі виявлення факту плагіату студент отримує за завдання 0 балів, аналогічну оцінку отримують автори тотожних робіт.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- Використання телефонів і комп'ютерних засобів без дозволу викладача забороняється.

***КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ**

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 бала
	• опитування за результатами вивчення теми, перевірка знання термінології	за кожну правильну відповідь 0,25 бала
	• індивідуальний виступ за результатами самостійного вивчення навчального матеріалу	за кожен виступ максимум 2 бали
	• доповідь з презентацією за темою, в тому числі вивченою самостійно (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності презентації і доповіді)	за кожну доповідь максимум 3 бали
	• підготовка повідомлення, ессе, порівняльної характеристики, аналіз положень законодавства, публікації тощо	за кожну правильну відповідь 2 бали
	• участь у дискусії, обговоренні положень нормативних актів, положень законодавства тощо	за кожну участь 1 бал

РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1	максимальна оцінка – 20 балів
	Модульний контроль № 2	максимальна оцінка – 20 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у всеукраїнських та міжнародних конкурсах наукових студентських робіт за спеціальністю тощо.	Звільняється від іспиту
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Іспит***	Метою іспиту є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у формі тестування.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис у заліковій відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу, що відповідає робочій програмі дисципліни, правильно й обґрунтовано відповідає на поставлені запитання за темою. Студент уміє реалізувати теоретичні положення дисципліни у ході виконання практичних завдань, що свідчить про високий рівень засвоєння навчального матеріалу, показує здатність застосовувати знання із суміжних дисциплін. Знає сучасні напрями, методи і тенденції забезпечення безпеки інформаційних мереж, набуті в рамках даної дисципліни. За час навчання при проведенні практичних занять та виконанні індивідуальних/ контрольних завдань студент проявляє вміння самостійно опрацьовувати наукову літературу та нормативні документи, активно долучатися до обговорення проблем управління інформаційною безпекою мереж та шляхів їх вирішення. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки обсягів матеріалу, передбаченого робочою програмою, або невпевненістю у тлумаченні окремих теоретичних положень.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента щодо виконання практичних завдань підвищують його вміння використання знань, отриманих при вивченні інших дисциплін, а також знань, набутих при самостійному поглибленому вивченні питань у межах дисципліни, яка вивчається.	Відмінно / Зараховано (А)
82-89	Студент демонструє гарні знання змісту навчальних матеріалів, підходів до управління безпекою інформаційних мереж, що відповідає робочій програмі дисципліни, вміє застосовувати набуті знання та вміння для самостійної роботи, але допускає одиничні неточності. Вміє самостійно виправляти допущені помилки, число яких є незначним. Показує володіння практичними методами та вміє застосовувати їх для усунення проблем безпеки інформаційних мереж на достатньому рівні. За час навчання при проведенні практичних занять, виконанні індивідуальних/ контрольних завдань студент проявляє хорошу здатність самостійно виконувати поставлені завдання, долучатися до обговорення шляхів вирішення проблем за напрямом із незначними прогалинами у володінні практичними навичками.	**Достатній** На достатньо високому рівні забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Забезпечує студенту самостійне виконання практичних завдань у разі незначної зміни умов, порівняно з наданими у матеріалах дисципліни	Добре / Зараховано (В)
75-81	Студент загалом добре володіє навчальним матеріалом, знає основні теоретичні положення відповідно до робочої програми дисципліни, вміє застосовувати набуті вміння для виконання практичних завдань з питань управління інформаційною безпекою мереж, але допускає окремі неточності, вміє пояснити основні положення виконаних завдань та дати правильні відповіді у ході опитування. Помилки у відповідях не є системними.	**Достатній** На достатньому рівні забезпечує вимоги до знань, умінь і навичок вивченим матеріалом робочої програми дисципліни.	Добре / Зараховано (С)

	Студент знає основні положення матеріалу, що мають визначальне значення при виконанні індивідуальних/контрольних завдань та поясненні представлених думок в межах дисципліни, що вивчається.	Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	
64-74	Студент засвоїв більшу частину теоретичного матеріалу та в основному вивчив підходи до управління інформаційною безпекою мереж**,** передбачених робочою програмою дисципліни, розуміє постановку стандартних завдань, має уявлення щодо способів їх виконання. У ході виконання завдань допускає значну кількість неточностей і грубих помилок, які може усунути з допомогою викладача.	**Середній** Забезпечує помірний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент володіє певними неґрунтовними знаннями, передбаченими в робочій програмі дисципліни, на мінімально допустимому рівні. З використанням основних теоретичних положень студент з труднощами виконує поставлені завдання щодо опрацювання літератури, оцінювання й аналізу ситуацій, пов'язаних зі сферою безпеки інформаційних мереж**.** У ході виконання практичних/ індивідуальних/ контрольних завдань демонструє формальне ставлення, відсутність глибокого розуміння роботи та взаємозв'язків з іншими темами.	**Середній** Забезпечує мінімально допустимий рівень у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти матеріалів курсу, показує слабкі практичні навички**.** Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, якість виконання практичних завдань в більшості є низькою, відповіді невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни та володіння необхідними вміннями у студента відсутні.	**Низький** Не забезпечує практичної реалізації завдань, що формуються при вивченні дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі іспиту.	**Незадовільний** Студент не підготовлений до самостійного вирішення завдань, які встановляє програма дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*