СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«Управління безпекою інформаційних мереж»

Лектор курсу			**Савченко Віталій Анатолійович**, д.т.н., професор, професор кафедри управління інформаційною та кібербезпекою		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** savitan@ukr.net; **сторінка курсу в GWE –** https://classroom.google.com/c/NzA4Mjk5OTI4ODQ2	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	магістр	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	2	
Освітньо-професійна програма			Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	Вибіркова компонента освітньо-професійної програми	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36	-	96

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

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 **КЗ3.** Здатність до абстрактного мислення, аналізу та синтезу.	**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.

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.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.

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. Комплексний та процесний підходи до управління безпекою мереж. Системи управління інформаційними мережами Підходи до управління безпекою і відповідністю мережі (FCAPS, COBIT, ISO 27001). Ризик, загроза, вразливість. Систематизація операційних ризиків, пов'язаних з безпекою мереж. ***Знати:*** 1. Базові поняття в області безпеки інформаційних мереж. 2. Комплексний та процесний підходи до управління безпекою мережі. 3. Системи управління інформаційними мережами. 4. FCAPS, COBIT, ISO 27001. 4. Сутність понять: ризик, загроза, вразливість, класифікації ризиків безпеці мережі. ***Вміти:*** використовувати теоретичні знання у практичних ситуаціях, оцінювати системи управління інформаційними мережами відповідно до різних підходів до управління безпекою і відповідністю, класифікувати й оцінювати ризики безпеці мережі. ***Формування компетенцій:*** КЗ1, КФ3 ***Результати навчання:*** РН2, РН3 ***Рекомендовані джерела:*** 1-7.	Лекція 1	2*	Лекція-візуалізація, встановлення зв'язку з попередніми дисциплінами
	Практичне заняття 1		Коротке повторення матеріалу попередніх лекцій, робота в малих групах за темою «Підходи до управління безпекою і відповідністю мережі. FCAPS, COBIT, ISO 27001». Підготовка презентацій за результатами роботи групи.
	Практичне заняття 2		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Систематизація операційних ризиків, пов'язаних з інформаційною безпекою мереж»
Тема 2. Класифікація загроз безпеки інформаційних мереж. Аналіз та моделювання мережевих загроз. Стандарти серії ISO 27000. ISO 27001. Аналіз загроз ІБ корпоративних мереж.. ***Знати***: 1. Сутність поняття «загроза безпеці мережі» та види загроз. 2. Загальні відомості про стандарти серії 27000, основні положення ISO	Лекція 2	2*	Лекція-візуалізація, експрес-опитування студентів

27001:2022. 3. Засади проведення аналізу (розвідки) загроз безпеці мережі, в т.ч. моделювання загроз, джерела загроз. 4. Види загроз корпоративним мережам різного типу. ***Вміти***: Систематизувати, аналізувати й моделювати загрози безпеці мереж згідно з алгоритмом, використовувати наявні джерела інформації про загрози, застосовувати на практиці отримані знання засад аналізу загроз безпеці мережі. ***Формування компетенцій:*** КЗ1, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН10 ***Рекомендовані джерела:*** 1-7.	Практичне заняття 3		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Стандарти серії ISO 27000. ISO 27001 як основа для сертифікації СУІБ»
	Практичне заняття 4		Індивідуальні виступи за результатами самостійного вивчення теми «Аналіз загроз безпеці локальних корпоративних мереж».
Тема 3. Забезпечення інформаційної безпеки мереж. Методологія управління IT COBIT. Політика безпеки інформаційних мереж. Основні поняття політики безпеки. Структура політики безпеки мереж організації. ***Знати***: 1. Методи забезпечення інформаційної безпеки мереж. 2. Загальні положення стандарту COBIT. 3. Основні поняття і структуру політики безпеки організації. 4. Засади формування політик і процедур ІБ мережі. ***Вміти***: аналізувати й використовувати методи вирішення проблем безпеки мереж, застосовувати підходи до управління IT COBIT для розробки і впровадження заходів безпеки мереж, розробляти проекти політики і процедур безпеки інформаційних мереж. ***Формування компетенцій:*** КЗ1, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН10 ***Рекомендовані джерела:*** 1-7.	Лекція 3	2*	Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача)
	Практичне заняття 5		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення теми «Методичний апарат оцінки рівня ІБ на основі стандарту COBIT».
	Практичне заняття 6		Робота в малих групах за темою «Політика безпеки інформаційних мереж». Підготовка проектів політики ІБ мереж і їх презентація.
Тема 4. Концепція поглибленого захисту (Defence-in-Depth). Технології виявлення загроз інформаційним мережам. Мережеві сканери. IDS/IPS. ***Знати***: 1. Рівні, структуру та заходи поглибленого захисту мереж. 2. Види технологій виявлення загроз інформаційним мережам. 3. Класифікації та сутність функціонування систем виявлення і запобігання мережевим атакам IDS/IPS. ***Вміти***: використовувати заходи поглибленого захисту мереж на практиці, обирати засоби виявлення загроз відповідно до завдань, застосовувати набуті знання для виявлення атак на інформаційні мережі, аналізувати мережеву інформацію. ***Формування компетенцій:*** КЗ1, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН10 ***Рекомендовані джерела:*** 1-7.	Лекція 4	2*	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 «Технології виявлення загроз інформаційним мережам. Мережеві сканери». Розробка узагальнених рекомендацій.
	Практичне заняття 8		Практичне опрацювання матеріалів за темою «Технології виявлення атак на інформаційні мережі. IDS/IPS». Формування вказівок щодо їх використання у захисті мереж. **Проведення контрольної роботи № 1**

Тема 1. Підходи до управління безпекою і відповідністю мережі (NIST, ITIL, ISO 27032). **Тема 2.** Управління інформаційною безпекою на стратегічному рівні. **Тема 3.** Засоби моніторингу й аналізу мереж. **Тема 4.** SCADA-системи як засіб контролю і збору інформації. Переваги і недоліки.	Самостійна робота 18 год	6*	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. Засоби моніторингу й аналізу мереж. Системи управління мережею (NMS). 4. Архітектура SCADA-систем. Призначення, структура і основні функції SCADA-систем.
Змістовий модуль 2 Технології управління безпекою інформаційних мереж			
Тема 5. Методи ідентифікації й автентифікації користувачів інформаційної мережі. ЕЦП і функція хешування. Біометричні методи управління безпекою мереж. ***Знати***: 1. Основні методи ідентифікації й автентифікації користувачів інформаційної мережі. 2. Процедури цифрового підпису й сутність функції хешування. 3. Основні види й засади використання біометричних методів. 4. Переваги і недоліки систем біометричної ідентифікації й автентифікації. ***Вміти***: застосовувати практично знання щодо методів ідентифікації й автентифікації користувачів мережі, засад використання й забезпечення безпеки ЕЦП, обирати методи біометричної ідентифікації й автентифікації для проектування заходів безпеки мереж, зокрема систем управління доступом. ***Формування компетенцій:*** КЗ1, КЗ3, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН5, РН10 ***Рекомендовані джерела:*** 1-7.	Лекція 5	2*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Електронний цифровий підпис і функція хешування». Формування висновків з теми.
	Практичне заняття 10		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення питань щодо біометричних методів управління безпекою інформаційних мереж. Дискусія. Визначення основних переваг і недоліків різних біометричних методів.
Тема 6. Технології захисту мережі (файєрволи, антивірусний захист, VPN, NAC, безпека е-пошти). Технології запобігання й протидії загрозам кінцевих точок. Використання технологій обману DT. ***Знати***: 1. Класифікація технологій захисту мережі. 2. Принципи роботи засобів захисту мереж (файєрволів, антивірусів, VPN, NAC, захисту е-пошти). 3. Сутність роботи технологій запобігання й протидії загрозам кінцевих точок (EDR, UBA, UEBA, DLP). 4. Сутність і види технологій введення в оману (honeypot, honeytoken, honeynet, honeywall, DT) і безпечного виконання програм (Sandbox). ***Вміти:*** застосовувати на практиці набуті знання щодо оцінювання, вибору й використання технологій захисту мереж, протидії загрозам	Лекція 6	2*	Лекція-візуалізація, експрес-опитування студентів, письмова перевірка знань (за рішенням викладача)
	Практичне заняття 11		Практичне опрацювання матеріалів за темою «Технології запобігання й протидії загрозам кінцевих точок (EDR, UBA, UEBA, DLP)» з прикладами рішень від провідних виробників.

кінцевих точок, введення в оману і безпечного виконання програм. ***Формування компетенцій:*** К31, К33, КФ5 ***Результати навчання:*** РН2, РН3, РН5, РН10 ***Рекомендовані джерела:*** 1-7.	Практичне заняття 12		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення теми «Сутність і види технологій введення в оману (honeypot, honeytoken, honeynet, honeywall, DT) і безпечного виконання програм (Sandbox). Підготовка і представлення презентацій про кращі продукти (за бажанням).
Тема 7. Модель OSI. Технології захисту на канальному, транспортному й мережевому рівнях. Технології захисту на прикладному, представницькому й сеансовому рівнях. Протокол Kerberos. ***Знати***: 1. Рівні моделі OSI та їх функції. 2. Переваги й недоліки моделі OSI. 3. Протоколи формування захисту на канальному, транспортному й мережевому рівні. 4. Функції прикладного, представницького й сеансового рівнів OSI. 5. Специфіка роботи мережевого протоколу взаємної автентифікації Kerberos. ***Вміти***: застосовувати отримані знання про рівні моделі OSI та засоби захисту на кожному з них для формування власної моделі безпеки мережі конкретної організації, аналізувати й обирати варіанти реалізації мережевого захисту відповідно до моделі OSI. ***Формування компетенцій:*** К31, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН5, РН10 ***Рекомендовані джерела:*** 1-7.	Лекція 7	2*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 13		Усне експрес-опитування за матеріалами попередньої лекції, практичне опрацювання матеріалів за темою «Технології захисту на канальному, транспортному й мережевому рівнях», 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 технологій захисту на прикладному, представницькому й сеансовому рівнях. Аналіз специфіки мережевого протоколу взаємної автентифікації Kerberos.
Тема 8. Технологія аналізу захищеності інформаційних мереж. Безпека мобільних технологій в корпоративному середовищі. Безпека хмарних технологій. ***Знати***: 1. Засади аналізу захищеності мережевих протоколів, сервісів та операційних систем. 2. Методика аналізу захищеності систем і мереж. 3. Основні напрями забезпечення безпеки мобільних технологій в корпоративному середовищі. 4. Підхід NIST до класифікації загроз мобільним пристроям та методів їх протидії. 5. Загрози і вразливості хмарних технологій. 6. Напрями й засоби забезпечення хмарної безпеки. Методи забезпечення ІБ мереж, створених на базі хмарних технологій. ***Вміти:*** аналізувати стан захищеності мережевих протоколів, сервісів та операційних систем відповідно до розглянутої методики, оцінювати й обирати напрями й методи захисту мобільних і хмарних технологій в корпоративному мережевому середовищі. ***Формування компетенцій:*** К31, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН5, РН10 ***Рекомендовані джерела:*** 1-7.	Лекція 8	2*	Лекція-візуалізація, експрес-опитування студентів, письмова перевірка знань (за рішенням викладача)
	Практичне заняття 15		Індивідуальні виступи за результатами самостійного вивчення теми «Безпека мобільних технологій в корпоративному середовищі». Дискусія та вироблення рекомендацій щодо основних напрямів захисту корпоративних мобільних технологій».
	Практичне заняття 16		Опрацювання матеріалів за темою «Безпека хмарних технологій». Формування таблиці загроз хмарним технологіям та заходів їх запобігання і протидії. Представлення результатів і обговорення..

Тема 9. Системи управління інформацією та подіями інформаційної безпеки (SIEM). Організаційні та фізичні заходи управління безпекою мережі. Центр операцій безпеки (SOC). Центр мережевих операцій NOC. ***Знати***: 1. Функції та завдання SIEM-систем. 2. Джерела інформації та приклади сучасних SIEM-систем. 3 Засади управління персоналом і фізичною безпекою інформаційних мереж. 4. Роль SOC і NOC в управлінні безпекою інформаційних мереж організації. 5. Відмінності між функціональними можливостями NOC і SOC. ***Вміти***: використовувати на практиці знання щодо оцінювання, вибору й використання продуктів SIEM, інструментів управління безпекою інформаційних мереж у рамках SOC і NOC. ***Формування компетенцій:*** КЗ1, КФ3, КФ5 ***Результати навчання:*** РН2, РН3, РН5, РН10 ***Рекомендовані джерела:*** 1-7.	Лекція 9	2*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 17		Індивідуальні виступи за результатами самостійного вивчення питань організаційного та фізичного забезпечення безпеки мережі.
	Практичне заняття 18		Робота у малих групах. Практичне опрацювання матеріалів за темою «Роль SOC і NOC в управлінні безпекою інформаційних мереж організації». Підготовка узагальнених схем за темою. **Проведення контрольної роботи № 2**
Тема 5. Методи мультифакторної автентифікації користувачів інформаційної мережі. **Тема 6.** Протокол мережевої автентифікації 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 18 год	6*	5. Двофакторна автентифікація. Логічні, ідентифікаційні та біометричні методи автентифікації користувачів інформаційної мережі. 6. Протокол Kerberos. Автентифікатори. Управління ключами та сеансові мандати. 7. Загрози та вразливості у захисті мобільних пристроїв. Системи DLP, MDM, MAM та EEM у захисті мобільних пристроїв, даних та додатків. 8. Види загроз інформаційній безпеці в режимі віддаленого доступу. Методи підвищення інформаційної безпеки мереж, пристроїв і даних. 9. 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. Мужанова Т. М., Щавінський Ю. В., Рабчун Д. І. Управління безпекою інформаційних мереж : навч. посіб. Київ : ДУТ, 2023. 170 с.
2. Ахрамович В.М. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур». К.:ДУТ, 2019. 163 с.
3. Бурячок В.Л., Аносов А.О., Семко В.В., Соколов В.Ю., Складанний П. М. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, К.: КУБГ, 2019. 218 с.
4. 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.
5. Жилін А.В., Шаповал О.М., Успенський О.А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. ІСЗЗІ КПІ. Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. 213 с.
6. Легомінова С. В., Мужанова Т. М., Щавінський Ю. В., Якименко Ю. М., Запорожченко М. М., Рабчун Д. І. Аудит інформаційної безпеки : навч. посіб. Київ : ДУТ, 2023. 125 с.
7. Полторак В.П. Інформаційна безпека та захист даних в комп'ютерних технологіях і мережах : навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології». Київ : КПІ ім. Ігоря Сікорського, 2020. 78 с. URL: https://ela.kpi.ua/bitstream/123456789/38326/1/Information_security_NP.pdf
7. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А. Інформаційна безпека в комп'ютерних мережах : навч. посіб. /; 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
8. Соколов В.Ю., Бурячок В.Л., Таджділні М.М. Безпека безпроводових і мобільних мереж : навч. посіб. ред. перекл. О. П. Райтер. 2 вид., доп. К. : КУБГ, 2019. 130 с.
Додаткові джерела:
1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements. 80 p.
2. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls. 164 p.
3. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. Офіційний вісник України. 26.01.2021. № 6, стор. 10, стаття 306
4. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 31.05.2005 р. № 80/94-ВР. Відомості Верховної Ради України. 1994. № 31, Ст. 286
5. Про основні засади забезпечення кібербезпеки : Закон України від 05.10.2017 р. № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст.403.
6. 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.
Електронні ресурси:
1. Законодавство України. URL: https://zakon.rada.gov.ua
2. Сторінка ДССЗЗІ України. URL: https://cip.gov.ua/ua
3. Сторінка ISACA. URL: https://www.isaca.org/
4. Сторінка SANS. URL: https://www.sans.org/

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.:*	
	• 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.	Додаткові бали 5-10
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік 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	**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)

	незначними прогалинами у володінні практичними навичками.		
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. Студент знає основні положення матеріалу, що мають визначальне значення при виконанні індивідуальних/контрольних завдань та поясненні представлених думок в межах дисципліни, що вивчається.	**Достатній** На достатньому рівні забезпечує вимоги до знань, умінь і навичок вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
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 заліковку 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 заліковку книжку не проставляється*