СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ»

Лектор курсу			**Мужанова Тетяна Михайлівна**, кандидат наук з держ.упр., доц., доцент кафедри управління кібербезпекою та захистом інформації		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:** muzanovat@gmail.com; **сторінка курсу в GWE –** https://classroom.google.com/u/0/c/NzA3Mjc5MTk1MTY4	
Галузь знань			12 «Інформаційні технології»		**Рівень вищої освіти**	бакалавр	
Спеціальність			125 «Кібербезпека та захист інформації»		**Семестр**	4	
Освітня програма			«Управління інформаційною та кібернетичною безпекою»		**Тип дисципліни**	Основна	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36	-	54

АНОТАЦІЯ КУРСУ

Взаємозв'язок у структурно-логічній схемі

Освітні компоненти, які передують вивченню	Нормативно-правове забезпечення інформаційної безпеки, Стандарти інформаційної та кібербезпеки, Основи національної безпеки
Освітні компоненти для яких є базовою	Системний аналіз інформаційної безпеки, Організація конфіденційного діловодства, Управління інформаційною безпекою банків

Мета курсу:	набуття студентами компетенцій, знань, умінь і навичок у галузі забезпечення інформаційної безпеки держави, суспільства та особи, зокрема його нормативно-правових та організаційних засад, напрямів виявлення та протидії загрозам в інформаційній сфері з метою подальшого використання зазначених знань та навиків у подальшій практичній діяльності.

Компетентності відповідно до освітньої програми

Загальні компетентності (ЗК)	**Фахові компетентності (ПП)**
ЗК 2. Здатність застосовувати отримані знання в практичних ситуаціях. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації.	**ПП 2**. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки.

Результати навчання (РН)

РН 6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН 12. Розробляти моделі загроз та порушника.
РН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН 29. Виконувати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН 31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

РН 32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН 48. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
МОДУЛЬ 1 «ОСНОВНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ»			
Тема 1. ***Теоретичні засади інформаційної безпеки держави*** ***Знати***: теоретичні засади забезпечення ІБ держави, суспільства, особи, сутність основних понять за темою, отримати уявлення про історію розвитку ІБ держави. ***Вміти:*** використовувати теоретичні знання у практичних ситуаціях, оцінювати й прогнозувати загрози ІБ держави, суспільства відповідно до різних методів, в т.ч. за паспортом загрози. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 1,5,7.	Лекція 1	5,5*	Лекція-візуалізація, встановлення зв'язку з попередніми дисциплінами
	Практичне заняття 1		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення матеріалів про загрози інформаційній безпеці.
	Практичне заняття 2		Коротке повторення матеріалу попередніх занять, робота в малих групах щодо оцінювання й прогнозування розвитку потенційних загроз ІБ (за паспортом загрози). Підготовка презентацій за результатами роботи групи.
Тема 2. ***Система забезпечення інформаційної безпеки України*** ***Знати***: структуру системи ЗІБ України, сутність і напрями політики ЗІБ, положення нормативно-правових актів із питань ЗІБ України, повноваження суб'єктів системи ЗІБ та принципами їх взаємодії, роль неурядових організацій у ЗІБ України ***Вміти***: застосовувати норми законодавства України щодо ЗІБ у практичних ситуаціях, оцінити повноваження органів державної влади у системі ЗІБ, встановити роль неурядових організацій у ЗІБ України. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 1,5,7.	Лекція 2	5,5*	Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача)
	Практичне заняття 3		Усне експрес-опитування за матеріалами попередніх занять, індивідуальні виступи за результатами самостійного вивчення положень законодавства України з питань ІБ. Представлення узагальненої схеми нормативно-правового ЗІБ України.
	Практичне заняття 4		
	Лекція 3		Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 5		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення повноважень суб'єктів ЗІБ України. Представлення узагальненої схеми суб'єктів ЗІБ України.
	Практичне заняття 6		Усне експрес-опитування за темами попередніх занять. Індивідуальні виступи за результатами самостійного вивчення повноважень суб'єктів ЗІБ України. Проведення контрольної роботи № 1 «Основні аспекти забезпечення інформаційної безпеки України»
Тема 1. Зміна підходів до класифікації національних інтересів та загроз ІБ відповідно до законодавства України. **Тема 2**. Зарубіжний досвід кадрового забезпечення у сфері	Самостійна робота 14 год		1. Класифікації національних інтересів в інформаційній сфері відповідно до ЗУ «Про основи нац.безпеки» 2003 р. та «Про національну безпеку» 2018 р.

інформаційної та кібербезпеки: досвід для України.			2. Види загроз ІБ відповідно до Доктрин ІБ України 2009 та 2017 рр., Стратегій нац.безпеки України 2007 та 2020 рр. 3. Досвід підготовки фахівців у сфері ІКБ США. 4. Європейська практика кадрового забезпечення ІКБ.
МОДУЛЬ 2 «ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ ДЕРЖАВИ»			
Тема 3. ***Безпека інформаційного простору держави*** ***Знати***: основні засади забезпечення інформаційної безпеки інформаційних ресурсів, інфраструктури держави та національного інформаційного простору, види інформації обмеженого доступу проблеми національного інформаційного простору України та напрями забезпечення його ІБ, засади стратегічних комунікацій. ***Вміти***: застосовувати отримані знання для аналізу й прогнозування тенденцій у забезпеченні безпеки національного інформаційного простору, інформаційної інфраструктури та ресурсів України, класифікувати види інформації обмеженого доступу відповідно до вимог вітчизняного законодавства. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 1-4.	Лекція 4	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 7		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення питань щодо видів інформації обмеженого доступу відповідно до законодавства України. Формування висновків з теми.
	Практичне заняття 8		Усне експрес-опитування за матеріалами попередніх занять, індивідуальні виступи за результатами самостійного вивчення питань щодо засад стратегічних комунікацій в Україні. Дискусія.
Тема 4. ***Основи кібербезпеки держави*** ***Знати***: сутність ключових понять у сфері кібербезпеки, основні засади забезпечення кібербезпеки держави, класифікації кіберзлочинів, особливості політики кібербезпеки провідних держав світу. ***Вміти***: застосовувати отримані знання для аналізу й прогнозування тенденцій у забезпеченні кібербезпеки України, впровадження заходів забезпечення кібербезпеки на рівні держави та організації. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 1-4.	Лекція 5	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 9		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення підходів до класифікації кіберзлочинів. Формування висновків з теми.
	Практичне заняття 10		Усне експрес-опитування за матеріалами попередніх занять, індивідуальні виступи за результатами самостійного вивчення питань щодо впровадження політики кібербезпеки провідних держав світу (США, КНР), а також ЄС. Дискусія. Проведення контрольної роботи № 2 «Забезпечення безпеки інформаційного простору держави»
Тема 3. Підходи до встановлення та класифікації об'єктів критичної інформаційної інфраструктури держави в Україні та ЄС. **Тема 4.** Законодавство ЄС з кібербезпеки та кіберстійкості.	Самостійна робота 14 год		1. Класифікація об'єктів критичної інфраструктури відповідно до нормативної бази ЄС. 2. Нормативно-правові засади забезпечення безпеки критичної інфраструктури в Україні (ЗУ «Про основні засади забезпечення кібербезпеки України», Постанова КМУ від 09.10.2020 р. № 943 «Деякі питання об'єктів критичної інформаційної інфраструктури», Постанова КМУ від 19.06.2019

			р. № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури». 3. Положення ЗУ «Про критичну інфраструктуру та її захист». 4. Стратегії кібербезпеки 2016, 2020 років. Акти про кіберстійкість і кіберсолідарність 2022 р. 5. Європейський досвід протидії кіберзлочинності з початку 2000-х років.
МОДУЛЬ 3 «ІНФОРМАЦІЙНЕ ПРОТИБОРСТВО»			
Тема 5. ***Інформаційний простір як середовище інформаційного протиборства*** ***Знати***: сутність основних понять у сфері інформаційного протиборство, вимоги до структури системи ІП держави як складової системи ЗІБ, форми і методи ІП тощо. ***Вміти:*** на основі отриманих знань виявити й проаналізувати факти, що свідчать про використання ІП у вітчизняному та світовому інформаційному просторі, встановити форми і методи ІП, застосувати теоретичні знання для оцінювання й прогнозування ситуації у сфері ІП в Україні, розробити план АІВ\СІО. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 1-4,7,9.	Лекція 6	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 11		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення форм і методів ІП з обов'язковим наведенням і оцінкою конкретних прикладів ІП з української та світової практики.
	Практичне заняття 12		Усне експрес-опитування за матеріалами попередніх занять, робота в малих групах над розробкою планів АІВ\СІО відповідно до обраної тематики. Представлення результатів.
Тема 6. ***Особливості сучасного етапу інформаційного протиборства*** ***Знати***: сутність основних гібридних характеристик і мережевих принципів сучасного інформаційного протиборства, види інформаційної зброї. ***Вміти:*** на основі отриманих знань виявити й проаналізувати факти, що свідчать про використання ІП у вітчизняному та світовому інформаційному просторі, встановити форми і методи ІП, застосувати теоретичні знання для оцінювання й прогнозування ситуації у сфері ІП в Україні, розробити план АІВ\СІО. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 1-4,7,9.	Лекція 7	5,5*	Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача)
	Практичне заняття 13		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення матеріалів про мережеві принципи ІП з обов'язковим наведенням конкретних прикладів. Обговорення і підведення підсумків.
	Практичне заняття 14		Усне експрес-опитування за матеріалами попередніх занять, індивідуальні виступи за результатами самостійного вивчення матеріалів про види інформаційної зброї з обов'язковим наведенням і оцінкою конкретних фактів її використання. Обговорення і підведення підсумків. Проведення контрольної роботи № 3 «Інформаційне протиборство»

Тема 5. Історія розвитку інформаційного протиборства. **Тема 6.** Особливості сучасного етапу ІП.	Самостійна робота 14 год		1. Етапи розвитку ІП. Еволюція форм і методів ІП. 2. 36 стратагем Сунь-Цзи. 3. Гібридний характер ІП. 4. Мережеві принципи ІП. 5. Особливості інформаційного тероризму.
МОДУЛЬ 4 «ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОЇ БЕЗПЕКИ СУСПІЛЬСТВА І ОСОБИ»			
Тема 7. ***Особливості забезпечення ІБ суспільства й особи. Забезпечення інформаційно-психологічної безпеки*** ***Знати***: основні засади забезпечення інформаційної та інформаційно-психологічної безпеки особи, виявлення та протидії загрозам інформаційно-психологічного характеру, види психологічного впливу та їх характеристики. ***Вміти***: аналізувати і прогнозувати загрози, а також тенденції забезпечення ІБ суспільства та особи в умовах глобалізації і цифровізації, застосовувати отримані знання для захисту інформаційних прав і свобод людини і громадянина. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 6,7.	Лекція 8	5,5*	Лекція-візуалізація, експрес-опитування студентів
	Практичне заняття 15		Усне експрес-опитування за матеріалами попередньої лекції. Індивідуальні виступи за результатами самостійного вивчення матеріалів про види психологічного впливу з наведення конкретних прикладів з практики на рівні особи і суспільства. Дискусія.
	Практичне заняття 16		Усне експрес-опитування за матеріалами попередніх занять. Індивідуальні виступи за результатами самостійного вивчення матеріалів про особливості інформаційно-психологічного впливу. Формування класифікації форм і методів ІПВ.
Тема 8. ***Технології маніпулятивного інформаційно-психологічного впливу. Методи виявлення і протидії технологіям маніпулятивного ІПВ. Медіаосвіта й медіаграмотність*** ***Знати***: сутність і риси маніпулятивного ІПВ, засоби запобігання і протидії маніпуляціям на рівні особи і держави, маніпулятивні технології у ЗМІ й міжособистісному спілкуванні, роль медіаосвіти та медіаграмотності у протидії манупілятивним технологіям. ***Вміти:*** виявляти й аналізувати факти маніпулятивного ІПВ на психіку людини (в т.ч. через ЗМІ), його мотиви та цілі, запобігати і протидіяти маніпулятивним технологіям на рівні особи, організації, держави. ***Формування компетенцій:*** ЗК2, ЗК5, ПП2 ***Результати навчання:*** РН6, РН12, РН19, РН29, РН31, РН32, РН48 ***Рекомендовані джерела:*** 6,7,8,9.	Лекція 9	5,5*	Лекція-візуалізація, експрес-опитування студентів, термінологічний диктант (за рішенням викладача)
	Практичне заняття 17		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення маніпулятивних технологій у ЗМІ з обов'язковим наведенням і оцінкою конкретних фактів їх застосування. Обговорення і підведення підсумків.
	Практичне заняття 18		Усне експрес-опитування за матеріалами попередньої лекції, індивідуальні виступи за результатами самостійного вивчення матеріалів про медіаосвіту й медіаграмотність. Проведення контрольної роботи № 4 «Забезпечення інформаційно-психологічної безпеки суспільства і особи»
Тема 7. Інформаційно-психологічна безпека особи та засоби її забезпечення. **Тема 8.** Маніпулятивні технології в політичній та економічній сфері.	Самостійна робота 12 год		1. Засоби забезпечення інформаційно-психологічної безпеки особи та суспільства на рівні держави. 2. Ментальність, суспільна мораль як об'єкти забезпечення інформаційно-психологічної безпеки. 3. Соціально-вікові, освітні, гендерні, національні особливості

			забезпечення інформаційно-психологічної безпеки. 4. Виборчі маніпулятивні технології. 5. Методи маніпулювання свідомістю в рекламі.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

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

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Мужанова Т.М. Інформаційна безпека держави : посібник. Київ: ДУТ, 2019. 131 с. URL: http://www.dut.edu.ua/uploads/l_1856_97597210.pdf
2. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : Підручник. К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.
3. Бурячок В. Л., Толюпа С.В., Семко В.В., Складанний П.М., Лукова-Чуйко Н.В. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник. К. : ДУТ-КНУ, 2016. 178 с. URL: http://www.dut.edu.ua/uploads/p_303_92597962.pdf
4. Бурячок, В.Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : Підручник; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с. URL: http://www.dut.edu.ua/uploads/l_1209_69915296.pdf
5. Биченок Н.Н., Савченко В.А., Дзюба Т.М. Основи забезпечення інформаційної безпеки держави у воєнній сфері : Підручник. 2017. URL: http://www.dut.edu.ua/ua/lib/1/category/742/view/2011
6. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. К.: Вид-во Ліра-К, 2021. 412 с. URL: https://duikt.edu.ua/uploads/l_1352_84114000.pdf
7. Інформаційно-психологічне протиборство: підручник / В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін. ; за заг. ред. В. М. Петрика ; Ін-т спец. зв'язку та захисту інформації НТУ України «КПІ ім. І. Сікорського». Київ : ІСЗЗІ КПІ ім. І. Сікорського, 2018. 387 с. URL: https://mil.univ.kiev.ua/files/8_367228400.pdf
8. Забезпечення інформаційної безпеки держави : Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки, 2017. 204 с. URL: http://vlp.com.ua/files/170227_zmist.pdf
9. Бібліотека Центру практичної психології «Псі-фактор». URL: https://psyfactor.org/lybr.htm
10. Мужанова Т.М., Якименко Ю.М. Досвід Європейського Союзу з протидії деструктивній інформаційній діяльності в мережі Інтернет. Сучасний захист інформації. 2019. № 2. С.37-41. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2314

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 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, есе, 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 «Основні аспекти забезпечення інформаційної безпеки України»	максимальна оцінка – 10 балів
	Модульний контроль № 2 «Забезпечення безпеки інформаційного простору держави»	максимальна оцінка – 10 балів
	Модульний контроль № 3 ««Інформаційне протиборство»»	максимальна оцінка – 10 балів
	Модульний контроль № 4 «Забезпечення інформаційно-психологічної безпеки суспільства і особи»	максимальна оцінка – 10 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 заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Іспит проходить у письмовій або усній формі (на вибір викладача).	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 аналітичного характеру, що свідчить про високий рівень засвоєння навчального матеріалу, показує здатність застосовувати знання із суміжних дисциплін. Знає сучасні напрями, методи і тенденції забезпечення інформаційної та кібербезпеки держави, 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 забезпечення інформаційної безпеки держави 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 оцінювання й аналізу ситуацій у сфері інформаційної безпеки, 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 аналітичними методами та вміє застосовувати їх для оцінки ситуацій у сфері інформаційної безпеки. 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 (B)
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 аналітичного характеру з питань забезпечення інформаційної безпеки держави, 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 і поясненні представлених думок в межах дисципліни, що вивчається.	**Достатній** На достатньому рівні забезпечує вимоги до знань, умінь і навичок згідно з робочою програмою 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 оцінювання й аналізу ситуацій у сфері інформаційної безпеки**,** 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 у сфері інформаційної безпеки**.** У ході виконання практичних/індивідуальних/контрольних завдань показує формальне ставлення, відсутність глибокого розуміння предмету і 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, показати слабкі аналітичні 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 заліку.	**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*