Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Інститут спеціального зв'язку та захисту інформації КПІ ім. Ігоря Сікорського
Спеціальна кафедра № 4

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Робоча програма навчальної дисципліни (силабус)

Рівень вищої освіти	*Другий (магістерський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*125 Кібербезпека та захист інформації*
Освітньо-професійна програма	*Безпека державних інформаційних ресурсів*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*І рік підготовки, весняний семестр*
Обсяг дисципліни	*5 кредитів*
Семестровий контроль / контрольні заходи	*Залік / модульна контрольна робота / реферат*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	
Розміщення курсу	*Google Classroom*

Київ 2023

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Силабус освітнього компонента "Менеджмент інформаційної безпеки держави" складено відповідно до освітньої-наукової програми підготовки магістрів з кібербезпеки за спеціальності 125 – Кібербезпека та захист інформації.

Метою навчальної дисципліни є формування у курсантів наступних компетентностей: (КЗ-1) Здатність застосувати знання у практичних ситуаціях; (КЗ-2) Здатність проводити дослідження на відповідному рівні. (КЗ-3) Здатність до абстрактного мислення, аналізу і синтезу.

Предметом навчальної дисципліни є інформаційної безпеки держави що функціонує, а також система форм і методів організації захисту особового складу від негативного інформаційно-психологічного впливу.

Програмні результати навчання, на формування та покращення яких спрямована дисципліна: (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 інноваційну діяльність в сфері інформаційної безпеки або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі; (РН9) Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та кібербезпекою організації на базі стратегії і політики інформаційної безпеки; (РН14) Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, операційних процесів у сфері інформаційної та кібербезпеки в цілому; (РН15) Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та кібербезпеки, а також знання та пояснення , що їх обгрунтовують до персоналу, партнерів та інших осіб.

2. Пререквізити та постреквізити навчальної дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою).

Успішне вирішення завдань навчальної дисципліни базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін першого (бакалаврського) рівня вищої освіти.

Навчальна дисципліна, яка забезпечується цією навчальною дисципліною – "Військове стажування"

3. Зміст навчальної дисципліни

Семестр 1-й

Розділ (змістовий модуль) І. Безпека в умовах глобальних трансформацій сучасного світу.

Тема 1. Предмет та завдання навчальної дисципліни "Менеджмент інформаційної безпеки держави".

Тема 2. Національна безпека держави як соціальна проблема.

Розділ (змістовий модуль) ІІ. Інформаційна безпека держави.

Тема 3. Інформаційна безпека як складова національної безпеки держави.

Тема 4. Гендерні аспекти інформаційної безпеки.

Розділ (змістовий модуль) ІІІ. Загрози безпеки держави, суспільства, людини в інформаційної сфері.

Тема 5. Загрози національної безпеки держави в інформаційної сфері.

Тема 6. Загрози людині та суспільству в інформаційної сфері.

Розділ (змістовий модуль) ІV. Менеджмент по захисту інформаційної безпеки України.

Тема 7. Сутність та завдання менеджменту інформаційної безпеки.

Тема 8. Актуальні питання підготовка фахівців у сфері інформаційної безпеки та кібербезпеки.

4. Навчальні матеріали та ресурси

Основна література:

1. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник. /В. В. Петрик, С. О. Гнатюк, М. М. Присяжнюк та ін. Полтава, 2022. 328 с.
2. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене / В. М. Петрик, М. М. Присяжнюк, Я. М. Жарков та ін.]; за заг. ред. В. М. Петрика. Київ: Вид-во ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 388 с.
3. Богданов О. М., Петрик В. М. Соціальна інженерія (сучасні технології та шляхи захисту): навч. посіб. Київ: ІСЗЗІ КПІ імені Ігоря Сікорського, 2018. 80 с.
4. Ананьїн В. О., Горлинський В. В., Пучков О. О. Міжнародна безпека та євроатлантична інтеграція України: навч. посіб. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2020. 231 с.

Додаткова література:

1. Інформаційна безпека: підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін; під. ред. В. В. Остроухова. Київ: Вид-во Лира-К, 2021. 412 С.
2. Бакалинський О. О., Кожедуб Ю. В., Цуркан В. В. Менеджмент інформаційної безпеки: конспект лекцій. Київ: Україна: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2017. 90 с.
3. Менеджмент інформаційної безпеки: навчальний посібник для студентів спеціальності 125 "Кібербезпека" / О. Г. Корченко, М. Є. Шелест, С. В. Казмірчук, Ю. М. Ткач, Є. В. Іванченко. Ніжин: ФОП Лук'яненко В. В. ТПК "Орхідея", 2019. 408 с.
4. Інформаційна безпека держави: підручник / В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; в 2 т. Київ: Вид-во ІСЗЗІ НТУУ "КПІ", 2016. Т. 1. 264 с.
5. Інформаційна безпека держави: підручник / В. М. Петрик, М. М. Присяжнюк, Д. С. Мельник та ін.; в 2 т. Київ: Вид-во ІСЗЗІ НТУУ "КПІ", 2016. Т. 2. 328 с.
6. Золотар О.О. Інформаційна безпека людини: теорія і практика: монографія. Київ : ТОВ Видавничий дім "АртЕк", 2018. 446 с. URL: http://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf. (дата звернення: 29.06.2022).
7. Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ, 2017. 104 с. URL: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf. (дата звернення: 29.06.2022).
8. Мужанова Т. М. Інформаційна безпека держави: навч. посіб. Київ: ДУТ, 2019. 131 с. URL: https://nubip.edu.ua/sites/default/files/u34/posibnik_ibd_muzhanova_2019.pdf. (дата звернення: 04.01.2022).
9. Світова гібридна війна: український фронт / За заг. ред. В. П. Горбуліна. Київ: НІСД, 2017. 496 с. URL: https://shron1.chtyvo.org.ua/Horbulin_Volodymyr/Svitova_hibrydna_viina_ukrainskyi_front.pdf. (дата звернення: 04.01.2022).
10. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення: 29.06.2022).
11. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації": Указ Президента України від 19 березня 2021 року № 106/2021. URL: https://www.president.gov.ua/documents/1062021-37421. (дата звернення: 29.06.2022).
12. Алещенко В. Інформаційно-психологічна складова безпеки особистості в умовах війни. Вісник Національного університету оборони України, № 2 (66) 2022. С. 5–17. URL: http://visnyk.nuou.org.ua/article/view/255150. (дата звернення: 04.01.2022).
13. Рішення Ради національної безпеки і оборони України «Про План реалізації Стратегії кібербезпеки» від 30 грудня 2021 року. Указ Президента України від 1 лютого 2022 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text (дата звернення: 14.02.2022).
14. Рішення Ради національної безпеки і оборони України « Про Стратегію національної безпеки України» від 14 вересня 2020 року. Указ Президента України від 14 вересня 2020 року № 37/2022. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 14.02.2022).

15. Загородня Ю. В. Кібербезпека як інноваційний захист у політичному просторі України. Вісник Національного технічного університету України «Київський політехнічний інститут». Політологія. Соціологія. Право. 2021. №. 4 (52). С. 33–38. DOI: doi.org/10.20535/2308-5053.2021.4(52).248130
16. Кулеба Д. Війна за реальність: як перемагати у світі фейків, правд і спільнот. Київ : Книголав, 2022. 384 с.
17. Закон України «Про основні засади забезпечення кібербезпеки України». 05 жовтня 2017 року № 2163-VII. URL: https:// https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2022).
18. Конституція України [Електронний ресурс]: Закон України від 28.06.1996 № 254к/96-ВР // Верховна Рада України. URL: http://zakon2.rada.gov.uaЛaws/show/254к/96-вр

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Навчальний процес за даною дисципліною складається з лекцій, семінарських занять, що проводяться за розкладом, підготовки реферату (ІСЗ), системної самостійної роботи, модульної контрольної роботи, рубіжного контролю, залікової письмової контрольної роботи, а також проведення індивідуальних і групових консультацій за графіком консультацій.

Якість навчання забезпечується шляхом постановки і розв'язання проблемних питань на семінарських заняттях, застосуванням активних форм навчання. Керівництво самостійною роботою відбувається шляхом визначення завдань і рекомендацій для самостійного відпрацювання навчального матеріалу та систематичним контролем викладача за ходом відпрацювання навчальних завдань.

У випадку запровадження обмежувальних заходів, що унеможливлюють організацію і здійснення освітнього процесу в навчальних приміщеннях у складі груп, проведення навчальних занять з даного кредитного модуля можна здійснювати віддалено з використанням технологій дистанційного навчання.

Навчальна література, зазначена в пункті 4 цієї робочої програми кредитного модуля, є відкритою, не містить відомостей з обмеженим доступом і може бути оприлюднена з використанням технологій дистанційного навчання, а сама програма не потребує коригування у випадку проведення навчальних занять у дистанційному режимі.

Структура кредитного модуля

Номери, назви розділів, тем і питання навчальних занять, посилання на літературу		Кількість годин				
		Всього	у тому числі			
			Лекції	Практичні (семінарські) заняття	Лабораторні заняття (комп`ютерний практикум)	СР
Розділ (змістовий модуль) І. ***Безпека в умовах глобальних трансформацій сучасного світу.***						
Тема 1	**Предмет та завдання навчальної дисципліни "Менеджмент інформаційної безпеки держави."**	**2.5**	**2**	**-**	**-**	**0.5**
Заняття 1/1	Вступ до дисципліни "Менеджмент інформаційної безпеки держави." 1. Рейтингова система оцінювання результатів навчання курсантів. 2. Мета, завдання, значення і місце навчальної дисципліни у підготовці	2.5	2	-	-	0.5

	фахівців. 3. Перелік компетентностей які формуються у курсантів навчальної дисципліною. Основана література: [1–3].					
Тема 2	**Національна безпека держави як соціальна проблема.**	**14**	**4**	**6**	**-**	**4**
Заняття 2/1	Еволюція соціуму і соціального насильства, його сутність і типи. 1. Соціальне насильство і війна; світоглядний та методологічний зміст. 2. Сутність, походження та класифікації війн. Основана література: [4].	2.5	2	-	-	0.5
Заняття 2/2	Соціальне насильство і війна: історія та сучасність. 1. Природа соціального насильства. 2. Війна як соціальне явище. 3. Концепції походження війн. 4. Геополітичні інтерпретації війни. 5. Класифікація війн збройних конфліктів.. 6. Війна та збройні конфлікти в сучасних умовах. Основана література: [4].	3	-	2	-	1
Заняття 2/3	Національна безпека України у системі сучасних геополітичних координат. 1. Сутність та задачі національної безпеки. 2. Види національної безпеки. Основна література: [4].	2.5	2	-	-	0.5
Заняття 2/4	Національна безпека як соціальна система. 1. Сутність та задачі національної безпеки. 2. Підсистеми безпеки. 3. Об’єкти національної безпеки. 4. Види безпеки у сучасному суспільстві. 5. Рівні безпеки за їхньою масштабністю. 6. Значення знання концептуальних засад національної безпеки для фахівців Держспецзв’язку. Основна література: [4].	3	-	2	-	1
Заняття 2/5	Національна безпека України: сутність, структура. 1. Задачі національної безпеки України. 2. Основні принципи забезпечення національної безпеки. 3. Пріоритети національних інтересів	3	-	2	-	1

	України. 4. Об'єкти національної безпеки України. 5. Суб'єкти національної безпеки України. 6. Умови достатнього рівня оборонної могутності України. 7. Воєнна організація України. Основна література: [4].					
	Разом за розділом І.	**16.5**	**6**	**6**	**-**	**4.5**
Розділ (змістовий модуль) ІІ. *Інформаційна безпека держави.*						
Тема 3	**Інформаційна безпека як складова національної безпеки держави.**	**17**	**4**	**8**	**-**	**5**
Заняття 3/1	Інформаційна безпека в системі національної безпеки України. 1. Інформаційна безпека: сутність, структура. та об'єкти захисту. 2. Суб'єкти та об'єкти інформаційного впливу. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 3/2	Інформаційна безпека держави: сутність, структура. 1. Інформаційна безпека в системі національної безпеки держави. 2. Інформаційна безпека держави: сутність, задачі. 3. Стан інформаційна безпека держави. 4. Структура інформаційної безпеки держави. 5. Об'єкти інформаційна безпека держави. 6. Суб'єкти забезпечення інформаційної безпеки держави. Основна література: [1–3].	3	-	2	-	1
Заняття 3/3	Інформаційна безпека України (ІБУ). 1. Основні задачі забезпечення інформаційної безпеки України. 2. Життєвє важливі інтереси в інформаційної сфері України. 3. Об'єкти захисту інформаційної безпеки України. 4. Основні групи загроз ІБУ. 5. Основні принципи забезпечення ІБУ. 6. Система функції забезпечення ІБУ. 7. Діяльність спецслужб України у сфері забезпечення ІБД. Основна література: [1–3].	3	-	2	-	1
Заняття 3/4	Інтереси держави у сфері інформаційної безпеки. 1. Загальні інтереси держави у сфері інформаційної безпеки.	2.5	2	-	-	0.5

	2. Стратегія формування єдиного інформаційного простору держави. Основна література: [1–3].					
Заняття 3/5	Сфера інформаційної безпеки держави: (СІБД) її інтереси та формування єдиного інформаційного простору. 1. Загальні інтереси держави у сфері інформаційної безпеки. 2. Інформаційна політика держави. 3. Геополітичні особливості сучасного інформаційного простору. 4. Структура інформаційного впливу. 5. Об'єкти інформаційного впливу. 6. Діяльність спецслужб України у сфері забезпечення ІБД. Основна література: [1–3].	3	-	2	-	1
Заняття 3/6	Стратегія формування та розвитку єдиного інформаційного простору України. 1. Єдиний інформаційний простір України: сутність, значення. 2. Стратегія формування єдиного інформаційного простору держави. 3. Засоби масової інформації як засіб впливу на інформаційний простір. 4. Протидія діяльності зарубіжних державних та недержавних організацій інформаційному впливу. Основна література: [1–3].	3	-	2	-	1
Тема 4	**Гендерні аспекти інформаційної безпеки.**	**5.5**	**2**	**2**	-	**1.5**
Заняття 4/1	Гендерні аспекти інформаційної безпеки. 1. Гендерні стереотипи та комунікативні моделі у сучасному суспільстві. 2. Гендерні особливості інформаційного впливу. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 4/2	Гендер в епоху інформаційного суспільства. 1. Гендер: становлення наукової галузі в сучасному суспільстві. 2. Гендерні стереотипи та комунікативні моделі. 3. Гендерні особливості інформаційного впливу. 4. Роль інтернет -ресурсів у популяризації гендерної проблематики. 5. Питання гармонізації гендерних відносин у сучасному українському	3	-	2	-	1

	суспільстві. 6. Гендерна культура особистості фахівця: сутнісні аспекти. 7. Особливості соціалізації жінок у воєнної сфері суспільства. Основна література: [1–3].					
	Разом за розділом ІІ.	**22.5**	**6**	**10**	**-**	**6.5**
Розділ (змістовий модуль) ІІІ. ***Загрози безпеки держави, суспільства, людини в інформаційній сфері***						
Тема 5	**Загрози національної безпеки держави в інформаційній сфері.**	**15.5**	**4**	**6**	**-**	**5.5**
Заняття 5/1	Поняття та види загроз безпеки держави в інформаційній сфері. 1. Загальна характеристика зовнішніх та внутрішніх загроз в інформаційній сфері 2. Інформаційна зброя. 3. Спеціальні інформаційні операції (СІО). Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 5/2	Загрози безпеки держави в інформаційній сфері. 1. Загальна характеристика зовнішніх загроз держави. 2. Загальна характеристика внутрішніх загроз держави. 3. Спеціальні інформаційні операції в інформаційній політиці. 4. Класифікація психологічних операцій. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 5/3	Інформаційна зброя особливості та класифікація. 1. Інформаційний простір як театр сучасних воєнних дій. 2. Класифікація сучасної інформаційної зброї. 3. Основні показники та особливості інформаційної зброї. 4. Види інформаційної зброї. 5. Основні способи й методи застосування інформаційної зброї. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 5/4	Інформаційна війна як форма інформаційного протиборства. 1. Інформаційне протиборство: сутність, задачі, форми. 2. Інформаційна війна: об’єкти посягань. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття	Інформаційна війна: сутність і зміст.	3.5	-	2	-	1.5

5/5	1. Сутність та задачі інформаційної війни. 2. Об'єкти посягань інформаційної війни. 3. Сучасні теоретичні підходи до використовування понять «інформаційна боротьба» та «інформаційна війна». 4. Види інформаційної боротьби. 5. Форми інформаційної війни. Основна література: [1–3].					
Тема 6	**Загрози людині та суспільству в інформаційної сфері.**	**53**	**10**	**20**	**-**	**23**
Заняття 6/1	Загрози особистісній безпеці від деструктивних інформаційних впливів. 1. Інформаційно-психологічна безпека особи. 2. Характеристика інформаційно психологічного впливу. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 6/2	Поняття та сутність інформаційного впливу на суспільство та особистість 1. Сутність інформаційно-психологічної безпеки особи. 2. Загрози особистості від деструктивних інформаційних впливів. 3. Інформаційне середовище та його вплив на людину. 4. Види інформаційно-психологічного впливу. 5. Роль ЗМІ в маніпулюванні свідомістю людини. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 6/3	Інформаційний вплив на суспільство та особистість. 1. Інформаційно-психологічна безпека особи. 2. Види загроз особистості від деструктивних інформаційних впливів. 3. Інформаційне середовище та його вплив на людину. 4. Види інформаційно-психологічного впливу. 5. Роль ЗМІ в маніпулюванні свідомістю людини. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 6/4	Сутність та зміст сугестивних технологій маніпулятивного впливу. 1. Наукові особливості сугестивних явищ. 2. Поняття та напрями реалізаці	2.5	2	-	-	0.5

	сугестивних технологій. Основна література: [1–3].					
Заняття 6/5	Інформаційно-комунікативне суспільство як новий об'єкт сугестивного впливу. 1. Наукові концепції інформаційного суспільства. 2. Україна в умовах формування інформаційно-комунікативного суспільства. 3. Сутність сугестивних технологій маніпулятивного впливу. 4. Наукові особливості сугестивних технологій. 5. Напрями реалізації сугестивних технологій. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 6/6	Чорний піар як сугестивна технологія. 1. Чорний піар: підходи, зміст, принципи. 2. Сугестія як психолінгвістична основа чорного піару. 3. Піартехніки реалізації сугестії. 4. Чорна риторика як маніпулятивна технологія чорного піару. 5. Принципи й правила чорної риторики: сугестивний підхід. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 6/7	Інтернет як середовище сугестивного впливу. 1. Сугестія в Інтернеті. 2. Принципи сугестивної лінгвістики в інтернетній комунікації. 3. Сугестія в жанрах Інтернету (медіавіруси, блоги, комп'ютерні ігри тощо). Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 6/8	Маніпулятивні технології в засобах масової інформації. 1. Сутність та походження феномену "маніпуляція". 2. Види маніпулювання суспільної свідомістю. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 6/9	Технології маніпулювання свідомістю людини. 1. Методи маніпулювання свідомістю людини. 2. Дезінформація як засіб впливу на людину. 3. Пропаганда.	3.5	-	2	-	1,5

	4. Сугестивні технології маніпулятивного впливу. Основна література: [1–3].					
Заняття 6/10	Маніпулятивні технології в засобах масової інформації (ЗМІ). 1. Фактори впливу на діяльність ЗМІ. 2. Базові захисні установки захисту від маніпулювання. 3. Характеристика впливу радіо інформаційних агентств. 4. «Вікна Овертона» у маніпулятивн технологіях. 5. Засоби розпізнавання загрози маніпулятивного впливу. Основна література: [1–3].	3.5	-	2	-	1.5
Заняття 6/11	Загрози інформаційної безпеки інформаційно-комунікаційних мережах. 1. Інтернет як арена сугестивного маніпулятивного впливу. 2. Соціальна інженерія в аспекті маніпулятивного впливу. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 6/12	Захист від загроз маніпулятивного впливу. 1. Соціальна інженерія: сутність, сучасне застосування. 2. Основні методи соціальної інженерії. 3. Види атак із використанням соціальної інженерії. 4. Кібертероризм як загроза інформаційної безпеки. 5. Комп'ютерна злочинність як загроза інформаційної безпеки. Основна література: [1–3].	4	-	2	-	2
Заняття 6/13	Захист інформації від соціальної інженерії. 1. Базові методи захисту. 2. Модель захисту від соціальної інженерії. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 6/14	Проблеми захисту інформації від соціальної інженерії. 1. Методика протидії соціальної інженерії. 2. Основні теорії створення методики протидії 3. Соціотехнічне тестування та створення профілів персоналу. 4. Підвищення захищеності системи. 5. Біометрія як механізм захисту від соціальної інженерії.	4	-	2	-	2

	6. Модель захисту від соціальної інженерії. Основна література: [1–3].					
Заняття 6/15	МКР з тем 1 – 6. Основна література: [1–3].	8	-	2	-	6
Разом за розділом ІІІ.		**68.5**	**14**	**26**	**-**	**28.5**
Розділ (змістовий модуль) IV. ***Менеджмент по захисту інформаційної безпеки України.***						
Тема 7	**Сутність та завдання менеджменту інформаційної безпеки.**	**16.5**	**4**	**6**	**-**	**6.5**
Заняття 7/1	Менеджмент в інформаційної безпеці. 1. Базове поняття менеджменту. 2. Спеціалізовані міжнародні організації у сфері інформаційної безпеці. 3. Стандарти ISD /IEC 27000. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 7/2	Менеджмент в інформаційної безпеці: поняття та його роль 1. Базове поняття менеджменту. 2. Системи менеджменту інформаційної безпеки. 3. Спеціалізовані міжнародні організації у сфері інформаційної безпеці. 4. Стандарти ISD /IEC 27000. Основна література: [1–3].	3.5	-	2	-	1,5
Заняття 7/3	Складові системи менеджменту інформаційної безпеки (СМІБ). 1. Переваги впровадження та сфери дії СМІБ. 2. СМІБ: забезпечення, функціонування, вдосконалення. Основна література: [1–3].	2.5	2	-	-	0.5
Заняття 7/4	Характеристика СМІБ. 1. Сфери дії СМІБ. 2. Цілі СМІБ. 3. Забезпечення СМІБ. 4. Функціонування СМІБ. 5. Оцінка ефективності СМІБ. 6. Вдосконалення СМІБ. Основна література: [1–3].	4	-	2	-	2
Заняття 7/5	Засоби підтримки функціонування СМІБ. 1. Організаційне забезпечення інформаційної безпеки. 2. Безпека персоналу. 3. Криптографічне забезпечення. 4. Управління доступом. 5. Безпека комунікацій. 6. Впровадження та експлуатація інформаційних систем.	4	-	2	-	2

	7. Аудит системи менеджменту інформаційної безпеки. Основна література: [1–3]					
Тема 8	**Актуальні питання підготовка фахівців у сфері інформаційної безпеки та кібербезпеки.**	**12**	**2**	**6**	**-**	**4**
Заняття 8/1	Напрями підготовки та удосконалення професіоналізму фахівців інформаційної безпеки та кібербезпеки України. 1. Підготовка фахівців у сфері інформаційної безпеки у сучасному суспільстві. 2. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки. 3. Підготовка фахівців інформаційної безпеки та кібербезпеки в Україні. Основна література: [1–3].	3	2	-	-	1
Заняття 8/2	Підготовка фахівців у сфері інформаційної безпеки. 1. Актуальність проблеми підготовка фахівців у сфері інформаційної безпеки. 2. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки (США, КНР, ФРН та ін.). 3. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні. 4. Напрями удосконалення системи підготовки фахівців у сфері інформаційної безпеки та кібербезпеки в Україні. 5. Інформаційна культура фахівця Держспецзв'язку. 6. Інформаційна культура населення України та роль фахівців в її формування. Основна література: [1–3].	3	-	2	-	1
Заняття 8/3	Захист рефератів.	3	-	2	-	1
Заняття 8/4	Захист рефератів.	3	-	2	-	1
Разом за розділом 4		**28.5**	**6**	**12**	**-**	**10.5**
Реферат		**6**	**-**	**-**	**-**	**6**
Залік		**8**	**-**	**2**	**-**	**6**
Всього годин		**150**	**32**	**56**	**-**	**62**

6. Самостійна робота курсантів

Головними видами самостійної роботи курсантів є: самостійна підготовка до аудиторних занять та самостійна підготовка до заліку.

Доцільно час самостійної підготовки для поглибленого вивчення та закріплення навчального матеріалу розподілити наступним чином:

№ з/п	Назва теми та перелік основних питань (перелік дидактичного забезпечення, посилання на літературу)	Кількість годин СР
1.	***Розділ (Змістовий модуль) І. Безпека в умовах глобальних трансформацій сучасного світу.*** ***Тема 1. Предмет та завдання навчальної дисципліни «Менеджмент інформаційної безпеки держави».*** *1. Об'єкт, предмет та мета навчальної дисципліни «Менеджмент інформаційної безпеки держави».* *2. Методологічні засади навчальної дисципліни «Менеджмент інформаційної безпеки держави».* *Основна література: [1–3].*	**4.5** 0.5
2.	***Тема 2. Національна безпека держави як соціальна проблема.*** *1. Сутність, задачі національної безпеки.* *3. Об'єкти національної безпеки.* *2. Види національної безпеки.* *4. Значення знання концептуальних засад національної безпеки для фахівців Держспецзв'язку.* *Основна література: [1–3].*	4
3.	***Розділ (змістовий модуль) ІІ. Інформаційна безпека держави.*** ***Тема 3. Інформаційна безпека як складова національної безпеки держави.*** *1. Стратегія формування єдиного інформаційного простору держави.* *2. Інформаційна політика держави.* *3. Геополітичні особливості* сучасного інформаційного простору. *4. Стратегія розвитку єдиного інформаційного простору України* *Основна література: [1–3].*	**6.5** 5
4.	***Тема 4. Гендерні аспекти інформаційної безпеки.*** *1. Гендерні особливості інформаційного впливу.* *2. Роль інтернет -ресурсів у популяризації гендерної проблематики.* *Основна література: [1–3].*	1.5
5.	***Розділ (змістовий модуль) ІІІ.Загрози безпеки держави, суспільства, людини в інформаційної сфері.*** *Тема 5. Загрози національної безпеки держави в інформаційної сфері.* *1. Інформаційна зброя особливості та класифікація.* *2. Інформаційна війна.* *3. Спеціальні інформаційні операції в інформаційній політиці.* *Основна література: [1–3].*	**28.5** 5.5
6.	***Тема 6. Загрози людині та суспільству в інформаційної сфері.*** *1. Роль ЗМІ в маніпулюванні свідомістю людини.* *2. Методи маніпулювання свідомістю людини.* *3. Дезінформація як засіб впливу на людину.* *Основна література: [1–3].*	23

7.	***Розділ (змістовий модуль) IV. Менеджмент по захисту інформаційної безпеки України.*** ***Тема 7. Сутність та завдання менеджменту інформаційної безпеки.*** *1. Системи менеджменту інформаційної безпеки.* *2. Спеціалізовані міжнародні організації у сфері інформаційної безпеці.* *3. Характеристика СМІБ.* *4. Стандарти ISD /IEC 27000.* *5. Аудит: сутність та цілі.* *Основна література: [1–3].*	**10.5** 6.5
8.	***Тема 8. Актуальні питання підготовка фахівців у сфері інформаційної безпеки та кібербезпеки.*** *1. Проблеми підготовка фахівців у сфері інформаційної безпеки.* *2. Міжнародний досвід підготовки фахівців інформаційної безпеки та кібербезпеки.* *3. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні.* *4. Напрями удосконалення системи підготовки фахівців Україні у сфері інформаційної безпеки та кібербезпеки.* *Основна література: [1–3].*	4
9.	***Реферат***	**6**
10.	***Підготовка до заліку***	**6**
Всього годин		**62**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила відвідування занять

Відвідування курсантами лекційних і семінарських занять є обов'язковим. Відсутність курсанта на занятті можлива за поважною причиною, про що робиться помітка в журналі відвідування занять.

Правила поведінки на заняттях

Під час аудиторної роботи курсанта на лекції необхідно уважно слухати викладача, осмислювати, узагальнювати теоретичні положення лекції і конспектувати матеріал у власному конспекті з навчальної дисципліни, не порушуючи етичних норм і вимог дисципліни поведінки на заняттях. Всі питання, стосовно змісту матеріалу і методики лекції, можна задавати викладачеві наприкінці заняття. При застосуванні дистанційної форми навчання лекції і семінарські заняття можуть проводитись з використанням платформ Google classroom, Google meet, Zoom, Cisco Webex Meetings. Під час роботи над матеріалами тексту і презентації лекції у віртуальному середовищі, курсант повинен ознайомиться з темою, метою і планом лекції, рекомендованою літературою, основними поняттями і категоріальним апаратом і змістом теми та законспектувати навчальний матеріал.

Під час самостійної роботи необхідно доповнювати конспекти та розкривати складні питання, що не були з'ясовані протягом лекції, використовуючи рекомендовані по темі навчальні посібники та словники. Для успішного самостійного опрацювання та засвоєння навчального матеріалу, курсантам пропонуються такі види роботи: читати та конспектувати рекомендовані першоджерела, тексти та статті за професійно-орієнтованою тематикою; складати конспекти та ставити творчі запитання до прочитаних текстів; писати короткі анотації до наукових джерел; готовити презентації до семінарських занять;

писати і захищати реферати та виконувати завдання з формування навичок творчої та дослідницької діяльності.

Семінарське заняття, незалежно від форми проведення і середовища, передбачає розгорнуте обговорення питань плану семінару методами дискусії або конференції і містить виступи курсантів з підготовленими короткими доповідями і рефератами з послідуючим обговоренням. На кожному семінарському занятті викладачем оцінюються підготовлені курсантами реферати і виступи, активність в дискусії, вміння формулювати та відстоювати свою позицію, а також проводиться письмовий експрес-контроль засвоєння теми.

Мультимедійна презентація виступу на семінарському занятті дозволяє передавати інформацію у візуалізованому, схематичному вигляді, що підвищує її цінність, можливості розуміння і засвоєння начального матеріалу, особливо при змішаному або віддаленому режимі навчання. Навчальна презентація розробляється згідно з підпитанням теми семінарського заняття, бути інтерактивною, передбачати зворотній зв'язок з аудиторією.

Презентації для підтримки виступу на семінарському занятті мають бути спрямованими на розкриття основних теоретичних положень теми виступу, містити оптимум наукового тексту у структурованому вигляді, що містить на одному слайді від 3 до 7 окремих положень та мінімум візуалізованих матеріалів. Доповнююча текстова інформація, що спрямована на обґрунтування, презентованих теоретичних положень, має бути озвучена доповідачем, протягом від7 до 10 хв.

Правила захисту індивідуальних завдань

Опанування навчальною дисципліною передбачає, виконання індивідуального семестрового завдання (ІСЗ) – підготовку кожним курсантом реферату на обрану та узгоджену з викладачем тему. Результати виконання ІСЗ курсантів оцінюються під час їх виступу на семінарських заняттях або в процесі співбесіди з викладачем.

Реферат – це дослідження, огляд наукових і правових джерел, спрямований на вивчення, аналіз і узагальнення ідеї, викладених у наукових працях з визначеної проблеми. Загальний обсяг реферату має становити 25–30 рукописних (надрукованих) аркушів, оформлених як наукова робота. Структурно реферат складається з титульного аркушу, змісту, вступу, двох, трьох питань, висновків, списку використаної літератури.

Автор реферату має підготуватися до виступу на семінарі, щоб на вимогу викладача протягом 5–10 хвилин викласти суть проблеми, що розглядається в рефераті. Для кращого захисту реферату пропонується застосовувати наукову мультимедійну презентацію. Оформлений згідно з вимогами, які пред’являються до наукових робіт, реферат оцінюється викладачем.

Загальними вимогами до реферату є:

- чіткість та логічна послідовність викладення матеріалу;
- переконливість аргументації;
- стислість і точність формулювань, які виключають можливість неоднозначного тлумачення;
- конкретність викладення результатів дослідження;
- наукова обґрунтованість висновків;
- академічна доброчесність
- зв’язок з майбутньою професійною діяльністю.

Підготовка до написання рефератів починається зі складання бібліографії – списку використаної літератури (не менш десяті назв першоджерел, монографій, наукових статей, законодавчих актів) та її опрацювання.

У вступі розкривається важливість та актуальність проблеми, стан її висвітлення у літературі, обов’язково визначаються мета та завдання реферату.

В основній частині, що складається з 2–3 питань, потрібно зробити огляд літератури за темою, у логічній послідовності, аргументовано, з посиланнями на джерела,

розкрити зміст кожного питання з відповідними висновками, що узагальнюють результати аналізу його опрацювання в наукових джерелах.

У загальних висновках наводять узагальнюючу оцінку одержаних результатів дослідження стосовно суті питань, що розглядались у роботі, визначається наукова та практична цінність виконаної роботи. Наприкінці, потрібно підкреслити значущість отриманого знання для формування громадянської свідомості військовослужбовця, професійній діяльності фахівця Держспецзв'язку.

Викладати матеріал слід сучасною українською мовою, короткими чіткими фразами, правильно оформлюючи науковий апарат.

Наприкінці реферату подається список використаної літератури (джерел). Список використаних джерел – елемент бібліографічного апарату, котрий містить бібліографічні описи використаних джерел згідно з державним стандартом: вказується прізвище автора, його ініціали, повна назва книги, місце видання та рік видання, загальна кількість сторінок; для наукових статей додається номер журналу та номери сторінок публікації.

Загальні правила цитування. Цитування повинно бути повним, допускається пропуск слів, речень, абзаців без перекручення авторського тексту. Випущений текст замінюється трьома крапками. При непрямому цитуванні (переказі) слід бути гранично точним у викладанні думок автора і давати відповідні посилання на джерело. Посилання у тексті реферату на джерело слід зазначати порядковим номером за переліком джерел, виділеним двома квадратними дужками, наприклад: "... у працях [1-3]...". Якщо використовують відомості, матеріали з джерел із великою кількістю сторінок, то у посиланні необхідно точно вказати номери сторінок, наприклад: [1, с.3].

До оформлення реферату висуваються наступні вимоги – робота має бути надрукована з одного боку паперу формату А4. Робота набираються 14 шрифтом із полуторним інтервалом. Аркуш реферату повинен мати наступні рамки поля: ліве – 25 мм., праве – 15 мм., верхнє – 20 мм. та нижнє – 20 мм. Нумеруються всі сторінки реферату, починаючи з титулу, але на ньому номер сторінки не проставляють. Абзацний відступ повинен бути однаковим упродовж усього тексту роботи і дорівнювати п'яти знакам (1,25 см.).

На титульному аркуші реферату зазначаються: назва інституту, кафедра, назва дисципліни, тема, прізвище, ім'я по батькові виконавця, курс, група, науковий ступень, вчене звання прізвище, ім'я, по батькові особи, що має провірити реферат, місто та рік.

Друга сторінка має містити план реферату, що складається із вступу, двох або трьох питань та висновки. Остання сторінка містить перелік використаної літератури.

Правила призначення заохочувальних та штрафних балів

Курсанту за роботу в семестрі можуть бути виставлені додаткові заохочувальні rЗ (зі знаком плюс) або штрафні rШ (зі знаком мінус) бали – до 10 балів. Заохочувальні бали rЗ виставляються за: наявності конспекту всіх лекцій, тем самостійного вивчення і семінарських занять; роботу у науковому товаристві за тематикою дисципліни; участь у інститутській або університетській конференціях (конкурсах, семінарах).

Штрафні бали rШ нараховуються за: не відпрацювання у конспекті тем пропущених лекційних і самостійних занять; спробу використання недозволених джерел під час проведення експрес-контролю; затримку подання ІСЗ.

Політика дедлайнів та перескладань

Терміни виконання навчальних завдань і контрольні заходи пов'язані з проходженням навчальної програми з дисципліни і розкладом занять. Крайній термін виконання ІСЗ (реферату) – останнє семінарське заняття. Якщо контрольні заходи пропущені з поважних причин (хвороба або вагомі життєві обставини), курсанту надається можливість додатково скласти контрольне завдання протягом найближчого тижня. Тематичне завдання, яке подається на перевірку з порушенням терміну виконання, оцінюється з врахуванням штрафних балів.

Умови перескладання заліку. У разі отримання курсантом незадовільної оцінки або наявності заборгованості, перескладання заліку з дисципліни допускається не більше двох разів. При другому перескладанні заліку у курсанта може приймати комісія, яка створюється завідувачем спеціальної кафедри. Оцінка, отримана курсантом у результаті другого перескладання заліку, є остаточною. Курсант, який був не допущений до складання заліку, або був допущений, але не з'явився без поважної причини на залік (коли присутність курсанта обов'язкова), або був усунений від заліку, вважається таким, що використав відповідну спробу скласти залік з дисципліни і має заборгованість.

Політика щодо академічної доброчесності

Відповідно до Закону України "Про освіту" – викладання навчальної дисципліни ґрунтується на засадах академічної доброчесності – сукупності етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень. Порушеннями академічної доброчесності вважаються: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання. За порушення академічної доброчесності здобувачі освіти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит, залік тощо); повторне проходження відповідного освітнього компонента освітньої програми. Списування під час контрольних (модульних) робіт та заліку заборонено (в тому числі із використанням мобільних девайсів).

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". **Норми етичної академічної поведінки** студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського". Детальніше: https://kpi.ua/code

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: здійснюється в формі письмового або усного експрес-опитування та виступів за темою семінарського заняття.

Рубіжний контроль: проводиться для уточнення рейтингу курсантів, за результатами вивчення І – ІІІ модулів, шляхом виконання модульної контрольної роботи (МКР).

Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Семестровий контроль: залік, який проводиться в формі залікової контрольної роботи.

Умови допуску до семестрового контролю:

1) зарахування виконання семестрового індивідуального завдання – реферату;

2) позитивна оцінка за МКР;

Оцінювання результатів навчання курсантів здійснюється у відповідності до Методичних рекомендацій до розроблення і застосування рейтингових систем оцінювання курсантів в ІСЗЗІ КПІ ім. Ігоря Сікорського.

Рейтингова система оцінювання результатів навчання (РСО) з навчальної дисципліни

1. Рейтинг курсанта а з дисципліни складається з балів, що він отримує за:

– виконання 5 письмових експрес-контролів;

– поточний контроль на семінарських заняттях (8 усних відповіді);

– виконання модульної контрольної роботи (далі – МКР);

– виконання індивідуального семестрового завдання (далі – ІСЗ) у формі реферату.

2. Критерії нарахування балів.

2.1. **Експрес-контрольна робота оцінюються максимум в 3 балів**:

– “відмінно” – повна, глибока, логічно стрункa і обґрунтована відповідь (не менше 90% потрібної інформації) – 3 бала;

– “добре” – достатньо повна і аргументована відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 2 бала;

– “задовільно” – неповна і недостатньо аргументована відповідь (не менше 60% потрібної інформації) з незначними помилками – 1 бал;

– “незадовільно” – відповідь не відповідає вимогам на “задовільно” – 0 балів.

2.2. **Максимальний бал за усну відповідь на семінарському занятті оцінюються в 5 балів**:

– “відмінно” – повна, глибока, логічно стрункa і обґрунтована відповідь (не менше 90% потрібної інформації) – 5 балів;

– “добре” – достатньо повна і аргументована відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 4 балів;

– “задовільно” – неповна і недостатньо аргументована відповідь (не менше 60% потрібної інформації) з незначними помилками – 2 балів;

– “незадовільно” – відповідь не відповідає вимогам на “задовільно” – 0 балів.

2.3. **Максимальний бал за МКР оцінюється в 10 балів** за такими критеріями:

– “відмінно” – повна, глибока, обґрунтована і логічна відповідь (не менше 90% потрібної інформації) – 10 балів;

– “добре” – достатньо повна, аргументована відповідь (не менше 75% потрібної інформації), або повна відповідь з незначними неточностями – 7-8 балів;

– “задовільно” – неповна, неаргументована відповідь (не менше 60% потрібної інформації) з незначними помилками – 3-5 балів;

– “незадовільно” – відповідь не відповідає вимогам на “задовільно” – 0 балів.

2.4. **Максимальний бал за ІСЗ (реферат) оцінюється в 15 балів** за такими критеріями:

– “відмінно” – творчий підхід, всебічне, глибоке, логічне, аргументоване розкриття проблеми з посиленням на наукові джерела, обґрунтуванням її значущості для майбутньої соціальної і професійної діяльності и розвитку світогляду – 14-15 балів;

– “добре” – повне, науково обґрунтоване, логічне розкриття проблеми з відображенням власної позиції – 10 – 12 балів;

– “задовільно” – неповне і недостатньо аргументоване розкриття проблеми з певними недоліками – 5 – 8 балів;

– “незадовільно” – ІСЗ не виконане, тобто ІСЗ не зараховано – 0 балів.

Наявність позитивної оцінки за ІСЗ є однією з умов допуску до залікової контрольної роботи.

2.5. Курсанту за роботу в семестрі можуть бути виставлені додаткові заохочувальні rЗ (зі знаком плюс) або штрафні rШ (зі знаком мінус) бали – до 10 балів. Заохочувальні бали rЗ виставляються за: наявності конспекту всіх лекцій, тем самостійного вивчення і семінарських занять; роботу у науковому товаристві за тематикою дисципліни; участь у інститутській або університетській конференціях (конкурсах, семінарах). Штрафні бали rШ нараховуються за: не відпрацювання у конспекті тем пропущених лекційних і самостійних занять; спробу використання недозволених джерел під час проведення експрес-контролю; затримку подання ІСЗ.

RD з кредитного модуля формується як сума всіх рейтингових балів rК, а також заохочувальних rЗ та штрафних балів rШ

$$\mathbf{R_D = (5_{пек}\ x3)+(12_{допов.}x5)+\ 10_{МКР}+15_{Реф} = 100\ балів}$$

2.6. **Залікова контрольна робота оцінюється в 100 балів** Її оцінка визначається як сума балів із залікової контрольної роботи rЗКР та балів із індивідуального семестрового завдання rІСЗ.

Контрольне завдання ЗКР складається з п’яті питань, із переліку, що наданий у Сілабусі, на які, курсанту потрібно дати письмові відповіді. Максимальний бал за виконання контрольного завдання ЗКР, що складається з трьох теоретичних питань по 15 балів, оцінюється в 75 балів за такими критеріями:

– “відмінно” – повна, глибока, логічно стрункa і науково обґрунтована відповідь (не менше 95% потрібної інформації) – 85 балів;

– “дуже добре” – повна і аргументована відповідь (не менше 85% потрібної інформації), або незначні неточності) – 70-80 балів;

– “добре” – достатньо повна і аргументована відповідь (не менше 75% потрібної інформації, або незначні неточності) – 65-70 балів;

– “задовільно” – неповна і недостатньо аргументована відповідь (не менше 65% потрібної інформації та деякі помилки) – 55-60 балів;

– “достатньо” – неповна відповідь (не менше 60% потрібної інформації та деякі помилки) – 50 балів;

– “незадовільно”, відповідь не відповідає умовам на “достатньо” – 0 балів.

Максимальна сума вагових балів, набраних за залікову контрольну роботу, з умовою зарахування балів, отриманих за виконання реферату, складає 100 балів.

3. Умовою атестації є отримання не менш ніж 50% від кількості балів, яку курсант може отримати на час проведення атестації.

4. Рейтингова оцінка трансформується до університетської системи оцінювання згідно з таблицею 1.

Таблиця 1. Переведення рейтингових балів до оцінок за університетською шкалою

Рейтингові бали, RD. Оцінка за університетською шкалою

Кількість балів	Оцінка
95-100	Відмінно
85-94	Дуже добре
75-84	Добре
65-74	Задовільно
60-64	Достатньо
Менше ніж 60	Незадовільно

5. Якщо сума набраних, протягом семестру, балів менш ніж 60, курсант виконує залікову контрольну роботу. У цьому разі сума балів за виконання ІСЗ та залікову контрольну роботу переводиться до підсумкової оцінки згідно з таблицею 1.

6. Курсант, який у семестрі отримав RD>60 балів, може прийняти участь у заліковій контрольній роботі.

7. Якщо здобувач виконав умови допуску до семестрового контролю у формі заліку, але набрав менше 60 балів, то результуюча оцінка виставляється за результатами залікової контрольної роботи, з урахуванням “жорсткої РСО”. При жорсткій РСО – попередній рейтинг здобувача з відповідної навчальної дисципліни (за винятком рейтингу семестрового завдання) скасовується і він отримує оцінку з урахуванням результатів залікової контрольної роботи. Жорстка РСО формує відповідальне ставлення здобувача до виконання залікової контрольної роботи, змушує його критично оцінити рівень своєї підготовки та ретельно готуватися до заліку.

9. Додаткова інформація з навчальної дисципліни

Перелік питань, які виносяться на модульну контрольну роботу та семестровий контроль.

1. Сутність, задачі національної безпеки.
2. Об’єкти національної безпеки.
3. Види національної безпеки.
4. Значення знання концептуальних засад національної безпеки для фахівців Держспецзв’язку.
5. Інформаційна безпека держави: сутність, структура.
6. Об’єкти інформаційна безпека держави.
7. Структура інформаційного впливу.
8. Об’єкти інформаційного впливу
9. Загальні інтереси держави у сфері інформаційної безпеки.
10. Інформаційна політика держави.
11. Геополітичні особливості сучасного інформаційного простору.
12. Стратегія формування єдиного інформаційного простору держави.
13. Стратегія розвитку єдиного інформаційного простору України
14. Гендерні стереотипи та комунікативні моделі.
15. Гендерні особливості інформаційного впливу.
16. Роль інтернет-ресурсів у популяризації гендерної проблематики.
17. Загальна характеристика зовнішніх загроз держави у сфері інформаційної безпеки.
18. Загальна характеристика внутрішніх загроз держави у сфері інформаційної безпеки.
19. Інформаційна зброя особливості та класифікація.
20. Інформаційна війна.
21. Спеціальні інформаційні операції в інформаційній політиці
22. Зробіть порівняльний аналіз визначень щодо інформації.
23. Принципи, суб’єкти та об’єкти інформаційних відносин.
24. Визначення понять “інформаційна сфера”, “безпека інформаційної сфери”, “інформаційна діяльність”, “інформаційні ресурси”, “інформаційна структура”, “інформаційний суверенітет”.
25. Співвідношення понять “безпека інформації”, “безпека інформаційної сфери” та “інформаційна безпека”.
26. Визначить поняття “інформаційна безпека”, “інформаційна безпека”, “інформаційна безпека особи”, “інформаційна безпека суспільства”, “інформаційна безпека держави”.
27. Реальні та потенційні загрози інформаційній безпеці України.
28. Форми та види інформаційного протиборства?
29. Розкрийте співвідношення понять “інформаційне протиборство”, “інформаційна війна”, “спеціальна інформаційна операція”, “акція інформаційного впливу”.
30. Форми та види інформаційного протиборства? Розкрийте співвідношення понять “інформаційне протиборство”, “інформаційна війна”, “спеціальна інформаційна операція”, “акція інформаційного впливу”.
31. Дайте визначення та розкрийте завдання інформаційної війни (ІВ)?
32. Назвіть об’єкти посягань, об’єкти деструктивного інформаційного впливу та форми ІВ.
33. Назвіть сім складових ІВ та основні компоненти ІВ у військовій сфері.
34. Охарактеризуйте етапи, ознаки та суб’єктів проведення спеціальних інформаційних операцій (СІО).
35. Методи СІО, дайте визначення та розкрийте форми дезінформування і пропаганди.
36. Форми диверсифікації громадської думки, психологічного тиску й поширення чуток.
37. Джерела загроз інформаційний безпеці особи та суспільства.
38. Рівень ефективності проведення інформаційно-психологічного впливу (ІПсВ).
39. Зміни в індивідуальній свідомості, до яких можуть призвести небезпечні ІПсВ.
40. Види ІПсВ.
41. Дайте визначення таким поняттям як “маніпулювання”, “маніпулювання”, “об’єкт маніпулювання”, “суб’єкт маніпулювання”, “жертва маніпулювання”, “інструмент

маніпулювання”, “мішені маніпулювання”.
42. Визначення і базові методи ІПсВ. Розкрийте алгоритми здійснення переконання та навіювання.
43. Розкрийте п’ять груп “мішеній маніпулювання”.
44. Опишіть вектори нападу методами соціальної інженерії при використанні мережі Інтернет.
45. Розкрийте засоби і методи соціального інженера спрямовані на якості людської природи.
46. Охарактеризуйте базові методи захисту від атак за допомогою соціальної інженерії.
47. Розкрийте основні фази активного захисту від соціальної інженерії.
48. Базове поняття менеджменту.
49. Системи менеджменту інформаційної безпеки.
50. Спеціалізовані міжнародні організації у сфері інформаційної безпеці.
51. Сфери дії СМІБ.
52. Цілі СМІБ.
53. Забезпечення СМІБ.
54. Функціонування СМІБ.
55. Оцінка ефективності СМІБ.
56. Вдосконалення СМІБ
57. Організація підготовки фахівців інформаційної безпеки та кібербезпеки в Україні.
58. Напрями удосконалення системи підготовки фахівців у сфері інформаційної безпеки та кібербезпеки в Україні.
59. Розкрийте природу й основні види ризику у сфері кібербезпеки.
60. Визначити основні терміни стосовно менеджменту ризиками.
61. Охарактеризувати призначення, мету, принципи менеджменту ризиків.
62. Проаналізуйте чинники прояву ризиків.
63. Охарактеризувати впровадження стилю менеджменту ризиків.
64. Охарактеризувати впровадження процесу менеджменту ризиків.
65. Охарактеризувати контролювання стилю менеджменту ризиків.
66. Охарактеризувати процесну модель менеджменту ризиків.
67. Розкрийте етапи (стадії) менеджменту ризиків.
68. Охарактеризувати встановлення контексту менеджменту ризиків.
69. Охарактеризувати оцінювання ризиків.
70. Охарактеризувати ідентифікування ризиків.
71. Охарактеризувати аналізування ризиків.
72. Охарактеризувати атестування ризиків.
73. Охарактеризувати обробляння ризиків.
74. Охарактеризувати шляхи зменшення ризиків.
75. Визначити основні терміни за стандартом ISO/IEC 27000.
76. Охарактеризувати вимоги стандарту ISO/IEC 27001 до побудови СМІБ.
77. Розкрийте загальну характеристику кіберзлочинності.
78. Зробіть системний аналіз соціальної інженерії.
79. Проаналізуйте заходи з протидії атакам за допомогою соціальної інженерії.
80. Розкрийте принципи дії та особливості застосування інформаційної та сейсмічної зброї.
81. Організаційне забезпечення інформаційної безпеки.
82. Безпека персоналу.
83. Криптографічне забезпечення.
84. Управління доступом.
85. Безпека комунікацій.
86. Впровадження та експлуатація інформаційних систем.
87. Аудит системи менеджменту інформаційної безпеки: сутність та цілі.
88. Внутрішній аудит. системи менеджменту інформаційної безпеки.
89. Зовнішній аудит. системи менеджменту інформаційної безпеки.

Рекомендована тематика рефератів (ІСЗ)

1. Теоретичні погляди на безпеку, її сутність, зміст і класифікацію.
2. Державна безпека України: місце в системі національної безпеки.
3. Інформаційна безпека України, її сутність і характеристика.
4. Загальна характеристика видів національної безпеки.
5. Основи, цілі та принципи національної безпеки і оборони України.
6. Пріоритети і правові засади забезпечення кібербезпеки і безпеки інформаційних ресурсів.
7. Інформаційна безпека: сутність, структура, загальна характеристика.
8. Воєнна безпека: сутність, зміст і призначення.
9. Сектор безпеки і оборони і національна політика держави.
10. Місце і завдання Держспецзв'язку в секторі безпеки і оборони України.
11. Воєнна безпека держави як складова національної безпеки.
12. Стратегія сталого розвитку і національна безпека України.
13. Кіберпростір і кібербезпека у міжнародних відносинах.
14. Міжнародні стандарти прав і свобод людини у світовому і національному кіберпросторі.
15. Інформаційне суспільство, інформаційний простір та інформаційна безпека.
16. Інформаційна безпека, як чинник і передумова сталого розвитку суспільства.
17. Міжнародні документи про права людини та їх захист у кіберпросторі.
18. Гендерні аспекти організації інформаційної та інформаційно-психологічної безпеки.
19. Сутність, мета, форми і технології інформаційно-психологічного протиборства.
20. Спеціальні інформаційні операції: цілі, ознаки, суб'єкти та етапи.
21. Сутність, цілі, засоби і компоненти ведення інформаційних і кібервоєн.
22. Теорія вікон Овертона в аспекті маніпулювання свідомістю.
23. Сугестивні технології маніпулятивного впливу в Інтернеті.
24. Проксі- та нелінійні війни сучасності.
25. Роль інформаційної складової у сучасних гібридних війнах.
26. Інформаційний тероризм та інформаційна безпека в сучасних умовах.
27. Засоби масової комунікації як інструмент інформаційних війн.
28. Маніпулятивні технології сучасних соціальних мереж.
29. Соціальна інженерія в аспекті інформаційної безпеки людини.
30. Методи профілактика наслідків негативного інформаційно-психологічного впливу на військовослужбовців.
31. Методики протидії негативному інформаційно-психологічному впливу на військовослужбовців під час виконання службово-бойових завдань
32. Основні методи, що застосовуються у технологіях соціальної інженерії та способи захисту.
33. Психологічні війни та операції як складові морально-психологічного впливу в сучасному світі.
34. Теорія нейролінгвістичного програмування як модель програмування людської поведінки та комунікацій.
35. Цілі, форми, методи і особливості здійснення сугестивного впливу через Інтернет і засобами комунікації та способи захисту.
36. Засоби масової інформації як інструмент впливу на інформаційний простір в умовах гібридної війни.
37. Інформаційна безпека держави в умовах глобалізації.
38. Система забезпечення інформаційної безпеки України.
39. Перспективи та проблеми інтеграції України у світовий інформаційний процес.
40. Нейролінгвістичне програмування як інструмент сугестивного маніпулятивного впливу.
41. Сучасні маніпулятивні технології в засобах масової інформації.
42. Комп'ютерна злочинність та кібертероризм як загрози інформаційній безпеці.
43. Причини, умови виникнення та наслідки злочинів у сфері використання ПЕОМ.

44. Державна політика у сфері інформаційної безпеки України.
45. Формування позитивного іміджу України у світовому інформаційному простору.
46. Фундаментальні національні інтереси держави згідно із Законом “Про національну безпеку України”.