СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«Методи виявлення та реєстрації загроз інформаційній безпеці»

Лектор курсу			**Якименко Юрій Михайлович**, кандидат військових наук, доцент, доцент кафедри "Управління інформаційною та кібернетичною безпекою"		**Контактна інформація лектора (e-mail), сторінка курсу в GWE**	**e-mail:**yakum14@ukr.net; **сторінка курсу в GWE –** https://classroom.google.com/u/1/c/NzEyMjY2NTAzMzg3	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	Магістр	
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	2	
Освітньо-професійної 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

Мета курсу:	набуття комплексу теоретичних знань, умінь і практичних навичок щодо використання сучасних методів виявлення, оцінювання і аналізу можливих загроз інформаційній безпеці.

Компетентності відповідно до освітньої програми

Загальні компетентності (КЗ)	**Фахові компетентності (КФ)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях.	КФ 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури. визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації. КФ7. Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Програмні результати навчання (РН)

РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому. РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому. РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Тема, опис теми	Вид заняття	Оцінювання за тему	Форми і методи навчання/питання до самостійної роботи
Модуль 1 «Методи виявлення та прогнозування загроз підприємства»			
Тема 1. ***Методи виявлення, аналізу, моніторингу загроз підприємства*** ***Знати***: узагальнений аналіз загроз інформаційного характеру економічній діяльності підприємства, механізм організації та проведення моніторингу загроз, методики оцінки небезпек та управління ризиком, методику проведення аналізу економічної безпеки організації, методику діагностики і оцінки стану економічної безпеки підприємства; методи виявлення, аналізу, моніторингу загроз. ***Вміти:*** аналізувати і оцінювати стан економічної безпеки підприємства, організовувати моніторинг загроз функціонуванню підприємства та використовувати методики діагностики і оцінки стану економічної безпеки підприємства, методики оцінки управління економічною та інформаційною безпекою підприємства. ***Формування компетенцій:*** К31; КФ7 ***Результати навчання:*** РН12 ***Рекомендовані джерела:*** 1,3-5, 9-13,15,21, 22,25,26,27,30,31,34	Лекція 1	12*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація, експрес-опитування студентів
	Лекція 3		Лекція-візуалізація
	Практичне заняття 1		Кількісна оцінка небезпек . Рішення задачі та обговорення результатів
	Практичне заняття 2		Якісний і кількісний аналіз ризику в підприємницькій діяльності- на прикладах. Обговорення результатів
	Практичне заняття 3		Характеристика економічної безпеки підприємства в ситуаційному менеджменті. Обговорення результатів
	Практичне заняття 4		Реалізація методики проведення аналізу економічної безпеки організації- на прикладі. Обговорення результатів
	Практичне заняття 5		Методика оцінки стану економічної безпеки підприємства - на прикладі. Обговорення результатів
	Практичне заняття 6		Реалізація методики оцінки управління економічною та інформаційною безпекою - на прикладах. Обговорення результатів

Тема 1. **Методи виявлення, аналізу, моніторингу загроз підприємства**	Самостійна робота		1. Процеси економічної діяльності підприємства і роль інформації у них 2. Види та характеристика загроз економічній діяльності підприємства 3. Класифікація загроз інформаційного характеру економічній діяльності підприємства 4. Ризик як кількісна оцінка небезпек 5. Аналіз ризику в підприємницькій діяльності 6. Методика аналізу ризиків 7. Методи реагування на загрози та інформаційні ризики 8. Характеристика економічної безпеки підприємства 9. Стратегічний аналіз економічної безпеки організації 10. Методи і принципи забезпечення інформаційної безпеки 11. Показники економічного потенціалу організації 12. Методика оцінки економічної та інформаційної безпеки підприємства 13. Методи виявлення,аналізу, моніторингу загроз 14. Напрямки покращення методів виявлення, аналізу, моніторингу загроз
Тема 2. ***Методи оцінки та прогнозування загроз і інформаційних ризиків підприємства*** ***Знати***: методи і технології оцінки та прогнозування загроз інформаційним ресурсам та системам забезпечення економічної діяльності підприємства, методичні підходи щодо оцінки уразливості інформації, порядок використанням методу аналізу ієрархій (MAI) для оцінки та прогнозування загроз і інформаційних ризиків, методичні підходи до виявлення та прогнозування загроз функціонуванню підприємства, методики і програмні продукти для оцінки ризиків в інформаційних системах, підхід до оцінки та прогнозуванню загроз і інформаційних ризиків за допомогою методики «матриця» та методу SWOT- аналізу, підхід до оцінки та прогнозуванню загроз і інформаційних ризиків за допомогою методу аналогій. ***Вміти:*** використовувати методи і технології оцінки та прогнозування загроз інформаційним ресурсам в системі забезпечення економічної діяльності підприємства, методики і програмні продукти для оцінки ризиків в інформаційних системах. ***Формування компетенцій:*** КФ7	Лекція 4	14*	Лекція-візуалізація
	Лекція 5		Лекція-візуалізація, експрес-опитування студентів
	Лекція 6		Лекція-візуалізація
	Практичне заняття 7		Методи виявлення та прогнозування загроз функціонуванню підприємства – вивчення на прикладах. Обговорення результатів
	Практичне заняття 8,9		Використання програмних продуктів для оцінки ризиків в інформаційних системах підприємства – елементи ділової гри. Обговорення результатів
	Практичне заняття 10,11		Використання методу аналізу ієрархій в оцінці безпеки комерційного банку – на прикладі. Обговорення результатів
	Практичне заняття 12		Оцінка і прогнозування загроз та інформаційних ризиків за методикою «матриця» підприємства – на прикладі. Обговорення результатів

Результати навчання: РН12 ***Рекомендовані джерела:*** 1,3,4,9-12,17,18,19,21, 22,23,28,32,36,37	Практичне заняття 13,14		Оцінка та прогнозування загроз і інформаційних ризиків за допомогою методу SWOT- аналізу – на прикладі. Обговорення результатів
	Практичне заняття 15		Модульний контроль №1. Виконання кваліфікаційних завдань. Тестування
Тема 2. **Методи оцінки та прогнозування загроз і інформаційних ризиків підприємства**			1. Методичні підходи та інструменти оцінки та прогнозування загроз інформаційним ресурсам та системам забезпечення економічної діяльності підприємства. 2. Система показників уразливості інформації. 3. Методи та моделі оцінки уразливості інформації 4. Методи оцінки інформаційних ризиків. 5. Особливості оцінки загроз та інформаційних ризиків за методикою MAI. 6. Методи виявлення та прогнозування загроз функціонуванню підприємства 7. Аналіз існуючих програм до оцінки ризиків (CRAMM., FRAP, OCTAVE, RiskWatch та інші. 8. Методика оцінки безпеки комерційного банку з використанням MAI. 9. Оцінка та прогнозування загроз і інформаційних ризиків за допомогою методики «матриця» 10. Особливості оцінки загроз та інформаційних ризиків з використанням методу SWOT- аналізу.
Модуль 2 «Виявлення загроз від комп'ютерних атак та захист комп'ютерних систем підприємства»			
Тема 3. ***Методи реагування на загрози і інструменти захисту від атак на комп'ютерні мережі*** ***Знати***: перелік комп'ютерних загроз та системи їх виявлення, можливості моделей загроз безпеці систем і способи їх реалізації, недоліки сучасних систем виявлення мережевих вторгнень, види комп'ютерних атак та способи їх реалізації, моделі порушника, програмні продукти для тестування комп'ютерної мережі, методичні інструменти захисту програмного забезпечення комп'ютерних систем, можливі канали витоку інформації.	Лекція 7	14*	Лекція-візуалізація
	Лекція 8		Лекція-візуалізація, експрес-опитування студентів
	Лекція 9		Лекція-візуалізація
	Практичне заняття 16		Підходи до визначення критеріїв уразливості і стійкості систем деструктивним впливам. Вивчення - на прикладах. Обговорення результатів
	Практичне заняття 17		Методи і засоби знімання та захисту інформації комп'ютерних систем. Вивчення - на прикладах. Обговорення результатів

Вміти: аналізувати можливості сучасних систем виявлення мережевих вторгнень і ознак комп'ютерних атак, аналізувати загрози та канали можливого витоку інформації. ***Формування компетенцій:*** К31, КФ3, КФ9 ***Результати навчання:*** РН20, РН12, РН14 ***Рекомендовані джерела:*** 2-8,10-12,14-18,30,33,35,38	Практичне заняття 18		Модульний контроль №2. Виконання кваліфікаційних завдань. Тестування
Тема 3. **Методи реагування на загрози і інструменти захисту від атак на комп'ютерні мережі** ***Формування компетенцій:*** К31, КФ3 ***Результати навчання:*** РН20 ***Рекомендовані джерела:*** 2-8,10-12,14-18,30,33,35,38	Самостійна робота		1. Система виявлення мережевих вторгнень і ознак комп'ютерних атак 2. Характеристика комп'ютерних атак та їх реалізація 3. Моделі і етапи реалізації атак на комп'ютерні мережі 4. Моделі порушника 5. Програми для тестування комп'ютерної мережі 6. Загрози безпеці інформації та програмного забезпечення 7. Методи і засоби аналізу безпеки програмного забезпечення 8. Можливості моделей загроз безпеці систем і способів їх реалізації 9. Критерії уразливості і стійкості систем деструктивним впливам 10. Моделі загроз безпеці систем і способи їх реалізації 11. Класифікація можливих каналів витоку інформації. 12. Технічні канали витоку інформації. 13. Методи і засоби знімання та захисту інформації

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять: Спеціалізована лабораторія: «Управління інформаційною та кібербезпекою».
- програмне забезпечення перевірки СУІБ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Резнікова О.О. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналітична доповідь / О. О. Резнікова і інші. - Київ : НІСД, 2020. 84 с. URL: https://niss.gov.ua/sites/default/files/2020-07/dopovid.pdf .
2. Технології захисту інформації. Текст лекцій. Тернопіль: ТНЕУ – 2017. – 86с. URL: http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf
3. Козюра В. Д. Захист інформації в комп'ютерних системах: підручник/ В. Д. Козюра ,В. О., Хорошко і інші. – Ніжин: ФОП Лук'яненкоВ.В., ТПК «Орхідея», 2020. – 236с.URL: http://ir.stu.cn.ua/handle/123456789/19248?locale-attribute=uk
4. Захист інформації в автоматизованих системах управління. навч. посібник/ І.А.Пількевич, і інші. –Житомир: Вид-во ЖДУ ім. І. Франка, 2015. –226с. URL: http://ir.znau.edu.ua/bitstream/123456789/3073/1/Zahyst_informacii_ASU.PDF
5. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — Київ: Видавнича трупа BNV, 2009. —608 с. URL: http://is.ipt.kpi.ua/wp-content/uploads/sites/4/2015/03/Graivorovskyi_Novikov.pdf
6. Ластівка Г. І. Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / Г. І. Ластівка і інші – Чернівці:

Чернівецький національний університет, 2018. – 252 с. URL: http://radiotech.cv.ua/documents/book/KONSPEKT_KANAL.pdf
7. Захист інформації від витоку технічними каналами. URL: https://tzi.com.ua/zaxist-nformacz-vd-vitoku-texnchnimi-kanalami.html
8. Антонюк А. О. Моделювання систем: навчальний посібник / А.О. Антонюк. –Ірпінь: Університет ДФС України, 2019. –412с. URL: http://ir.nusta.edu.ua/jspui/bitstream/123456789/5500/1/4944_IR.pdf
9. Якименко Ю. М. Особливості використання методичних заходів захисту інформації підприємства від сучасних видів загроз, кібератак і ризиків // Матеріали: Всеукраїнська наукова конференція, Актуальні проблеми кібербезпеки, 27 жовтня 2021. Тези доповідей — Київ: ДУТ, 2021.- С.173-176. URL : http://www.dut.edu.ua/uploads/p_2099_79407917.pdf
10. Якименко Ю.М., Мужанова Т.М., Легомінова С.В. (2021). Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка" 4(12), 36-50. URL: https://doi.org/10.28925/2663-4023.2021.12.3650
11. Якименко Ю.М., Савченко В.А., Легомінова С.В. Системний аналіз інформаційної безпеки: сучасні методи управління: підручник. Київ: Державний університет телекомунікацій, 2022. 308 с. URL: https://www.dut.edu.ua/uploads/l_2230_88161692.pdf
12. Мужанова Т.М., Легомінова С.В., 11.Якименко Ю.М., Мордас І.В.(2021). Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка", 1(13), 50-62. URL: https://doi.org/10.28925/2663-4023.2021.13.5062
13. Варенко В. М. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – Київ : Університет «Україна», 2013. – 203 с. URL: http://er.nau.edu.ua/handle/NAU/20105 , http://er.nau.edu.ua:8080/handle/NAU/20105.
14. Побудова Системи управління інформаційною безпекою. URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/.
15. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України. URL: https://zakon.rada.gov.ua/laws/show/v0365500-11.
16. Бурячок В.Л., Толюпа С.В., Аносов А.О., Козачок В.А., Лукова-Чуйко Н.В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В.Л. Бурячок, С.В.Толюпа, А.О. Аносов, В.А.Козачок, Н.В. Лукова-Чуйко / – Київ: ДУТ, 2015. – 345 с. URL: http://www.dut.edu.ua/uploads/l_1242_54311567.pdf , https://app.box.com/s/g7bqinazmw3i52kp43qizon9v6u9ryxd .
17. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
18. ДСТУ ISO/IEC 27002:2015 (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014), Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки.
19. ДСТУ ISO/IEC 27003:2018 (ISO/IEC 27003:2017, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Настанова . (ISO/IEC 27003:2010)
20. ISO/IEC 27004:2009 Інформаційні технології. Методи захисту. Управління інформаційною безпекою. Вимірювання
21. ДСТУ ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. (ДСТУ ISO/IEC 27005:2015)
22. ДСТУ ISO/IEC TS 27008:2019 (ISO/IEC TS 27008:2019, IDT) Інформаційні технології. Методи захисту. Настанова щодо оцінювання захисту інформаційної безпеки. (ДСТУ ISO/IEC TR 27008:2018)
23. ДСТУ ISO/IEC 27009:2018 (ISO/IEC 27009:2016, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Визначення для сфери застосування ISO/IEC 27001. Вимоги
24. ДСТУ ISO/IEC 27011:2018 (ISO/IEC 27011:2016, IDT) Інформаційні технології. Методи захисту. Настанова для телекомунікаційних організацій щодо керування інформаційною безпекою на основі ISO/IEC 27002. (ISO/IEC 27011:2008)
25. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. Корченко О.Г., Гнатюк С.О., Казмірчук С.В.та ін. – Київ : Центр навч.-наук. та наук.-пр. видань НАСБ України, 2014. –190с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
26. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. Підприємницька,

торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку: Матеріали II Міжнародної НПК 11-12 лютого 2021 року. – Київ: ДУТ, 2021.- С. 279-282.
27. Якименко Ю. М. Підвищення ефективності системи менеджмента інформаційної безпеки організаці Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції 27 жовтня 2022 року.-.Київ: ДУТ, 2022. - С.198-200
28. Якименко Ю.М., Чернявський І.Р., Ризикоорієнтований підхід до управління інформаційною безпекою на підприємстві. Київ: Сучасний захист інформації,
29. Якименко Ю.М., Рабчун Д.І., Капелюшна Т.В. Використання методичних підходів системного аналізу до забезпечення інформаційної безпеки об'єктів критичної інфраструктури. Державний університет телекомунікацій, Київ.2023
30. Якименко Ю.М., Легомінова С.В., Щавінський Ю.В., Рабчун Д.І. Управління інцидентами інформаційної безпеки. Сучасні методи і засоби: навчальний посібник. Київ: Державний університет телекомунікацій, 2023. 241 с.
31. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (Постанова Кабінету Міністрів України від 24.03.2023 № 257).
32. Професійний стандарт Фахівець із кібердосліджень та розробок систем безпеки, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-iz-kiberdoslidzhen-ta-rozrobok-sistem-bezpeki.
33. Фахівець з планування політики та стратегії кібербезпеки, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-z-planuvannya-politiki-ta-strategiyi-kiberbezpeki.
34. Професійний стандарт Аудитор інформаційних технологій (з кібербезпеки), https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-auditor-informaciinikh-tekhnologii-z-kiberbezpeki.
35. Професійний стандарт Фахівець з реагування на інциденти кібербезпеки, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-z-reaguvannya-na-incidenti-kiberbezpeki.
36. Професійний стандарт Аналітик з оцінки вразливостей, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-analitik-z-ocinki-vrazlivostei
37. Професійний стандарт Фахівець з оцінки заходів захисту інформації (кібербезпеки), https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-z-ocinki-zakhodiv-zakhistu-informaciyi-kiberbezpeki.
38. Професійний стандарт Керівник структурного підрозділу з питань безпеки інформації та кіберзахисту. https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-kerivnik-strukturnogo-pidrozdilu-z-pitan-bezpeki-informaciyi-ta-kiberzakhistu.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

- Курс передбачає роботу в колективі.
- Середовище в аудиторії є дружнім, творчим, відкритим до конструктивної критики.
- Освоєння дисципліни передбачає обов'язкове відвідування лекцій і практичних занять, а також самостійну роботу.
- Самостійна робота включає в себе теоретичне вивчення питань, що стосуються тем лекційних занять, які не ввійшли в теоретичний курс, або ж були розглянуті коротко, їх поглиблена проробка за рекомендованою літературою.
- Усі завдання, передбачені програмою, мають бути виконані у встановлений термін.
- Якщо студент відсутній з поважної причини, він презентує виконані завдання під час самостійної підготовки та консультації викладача.
- Під час роботи над завданнями не допустимо порушення академічної доброчесності: при використанні Інтернет ресурсів та інших джерел інформації студент повинен вказати джерело, використане в ході виконання завдання. У разі виявлення факту плагіату студент отримує за завдання 0 балів.
- Студент, який спізнився, вважається таким, що пропустив заняття з неповажної причини з виставленням 0 балів за заняття, і при цьому має право бути присутнім на занятті.
- За використання телефонів і комп'ютерних засобів без дозволу викладача, порушення дисципліни студент видаляється з заняття, за заняття отримує 0 балів.

*КРИТЕРІЇ ТА МЕТОДИ ОЦІНЮВАННЯ

Умовою допуску до підсумкового контролю є набрання студентом 30 балів у сукупності за всіма темами дисципліни		
Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• участь у експрес-опитуванні	за кожну правильну відповідь 0,25 бала
	• доповідь з презентацією за тематикою самостійного вивчення дисципліни (оцінка залежить від повноти розкриття теми, якості інформації, самостійності та креативності матеріалу, якості презентації і доповіді), підготовка реферату	за кожну презентацію (реферат) максимум 3 бали
	• усне опитування, тестування, рішення практичних задач	за кожну правильну відповідь 0,5 бала
	• участь у навчальній дискусії, обговоренні ситуаційного завдання	за кожну правильну відповідь 2 бали
	• участь у діловій грі	за кожну участь 1 бал
РУБІЖНЕ ОЦІНЮВАННЯ (МОДУЛЬНИЙ КОНТРОЛЬ)	Модульний контроль № 1 «МЕТОДИ ВИЯВЛЕННЯ ТА ПРОГНОЗУВАННЯ ЗАГРОЗ ПІДПРИЄМСТВА»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «ВИЯВЛЕННЯ ЗАГРОЗ ВІД КОМП'ЮТЕРНИХ АТАК ТА ЗАХИСТ КОМП'ЮТЕРНИХ СИСТЕМ ПІДПРИЄМСТВА»	максимальна оцінка –15 балів
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	30 балів

ПІДСУМКОВА ОЦІНКА ЗА ДИСЦИПЛІНУ

бали	**Критерії оцінювання**	**Рівень компетентності**	**Оцінка** */запис в екзаменаційній відомості*
90-100	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає робочій програмі дисципліни, правильно й обґрунтовано приймає необхідні рішення в різних нестандартних ситуаціях. Вміє реалізувати теоретичні положення дисципліни в практичних розрахунках, аналізувати та співставляти дані об 'єктів діяльності фахівця на основі набутих з даної та суміжних дисциплін знань та умінь. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань проявив вміння самостійно вирішувати поставлені завдання, активно включатись в дискусії, може відстоювати власну позицію в питаннях та рішеннях, що розглядаються. Зменшення 100-бальної оцінки може бути пов'язане з недостатнім розкриттям питань, що стосується дисципліни, яка вивчається, але виходить за рамки об'єму матеріалу, передбаченого робочою програмою, або студент проявляє невпевненість в тлумаченні теоретичних положень чи складних практичних завдань.	**Високий** Повністю забезпечує вимоги до знань, умінь і навичок, що викладені в робочій програмі дисципліни. Власні пропозиції студента в оцінках і вирішенні практичних задач підвищує його вміння використовувати знання, які він отримав при вивчені інших дисциплін, а також знання, набуті при самостійному поглибленому вивчені питань, що відносяться до дисципліни, яка вивчається.	Відмінно / Зараховано (А)

82-89	Студент демонструє гарні знання, добре володіє матеріалом, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати теоретичні положення при вирішенні практичних задач, але допускає окремі неточності. Вміє самостійно виправляти допущені помилки, кількість яких є незначною. Знає сучасні технології та методи розрахунків з даної дисципліни. За час навчання при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, дає вичерпні пояснення.	**Достатній** Забезпечує студенту самостійне вирішення основних практичних задач в умовах, коли вихідні дані в них змінюються порівняно з прикладами, що розглянуті при вивчені дисципліни	Добре / Зараховано (B)
75-81	Студент в загальному добре володіє матеріалом, знає основні положення матеріалу, що відповідає робочій програмі дисципліни, робить на їх основі аналіз можливих ситуацій та вміє застосовувати при вирішенні типових практичних завдань, але допускає окремі неточності. Вміє пояснити основні положення виконаних завдань та дати правильні відповіді при зміні результату при заданій зміні вихідних параметрів. Помилки у відповідях/ рішеннях/ розрахунках не є системними. Знає характеристики основних положень, що мають визначальне значення при проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	**Достатній** Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання викликають утруднення.	Добре / Зараховано (C)
64-74	Студент засвоїв основний теоретичний матеріал, передбачений робочою програмою дисципліни, та розуміє постанову стандартних практичних завдань, має пропозиції щодо напрямку їх вирішень. Розуміє основні положення, що є визначальними в курсі, може вирішувати подібні завдання тим, що розглядались з викладачем, але допускає значну кількість неточностей і грубих помилок, які може усувати за допомогою викладача. .	**Середній** Забезпечує достатньо надійний рівень відтворення основних положень дисципліни	Задовільно / Зараховано (D)
60-63	Студент має певні знання, передбачені в робочій програмі дисципліни, володіє основними положеннями, що вивчаються на рівні, який визначається як мінімально допустимий. З використанням основних теоретичних положень, студент з труднощами пояснює правила вирішення практичних/розрахункових завдань дисципліни. Виконання практичних / індивідуальних / контрольних завдань значно формалізовано: є відповідність алгоритму, але відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)
35-59	Студент може відтворити окремі фрагменти з курсу. Незважаючи на те, що програму навчальної дисципліни студент виконав, працював він пасивно, його відповіді під час практичних робіт в більшості є невірними, необґрунтованими. Цілісність розуміння матеріалу з дисципліни у студента відсутні.	**Низький** Не забезпечує практичної реалізації задач, що формуються при вивчені дисципліни	Незадовільно з можливістю повторного складання) / Не зараховано (FX) *В залікову книжку не проставляється*
1-34	Студент повністю не виконав вимог робочої програми навчальної дисципліни. Його знання на підсумкових етапах навчання є фрагментарними. Студент не допущений до здачі екзамену.	**Незадовільний** Студент не підготовлений до самостійного вирішення задач, які окреслює мета та завдання дисципліни	Незадовільно з обов'язковим повторним вивченням / Не допущений (F) *В залікову книжку не проставляється*