СИЛАБУС КОМПОНЕНТИ ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ

«Управління інцидентами інформаційної безпеки»

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/NzEyMjc0MTM3MTU0**
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	магістр
Спеціальність			125 Кібербезпека та захист інформації		**Семестр**	2
Освітньо-професійна програма			Управління інформаційною та кібернетичною безпекою		**Тип дисципліни**	Вибіркова компонента освітньо-професійної програми
Обсяг:	Кредитів ECTS	Годин	За видами занять:			
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	5	150	18	-	36	-	96

АНОТАЦІЯ КУРСУ

Мета курсу:	Формування у студентів знань та умінь, необхідних для організації управління інцидентами, які є основою забезпечення інформаційної безпеки підприємств.

Компетентності відповідно до освітньої програми	
Інтегральна компетентність	
Здатність розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки	
Загальні компетентності (КЗ)	**Фахові компетентності (КФ)**
КЗ1. Здатність застосовувати знання у практичних ситуаціях.	**КФ2.** Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки. **КФ4.** Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог. **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)

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
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 кібербезпекив цілому.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Модуль 1 «ПОБУДОВА СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІБ НА ОСНОВІ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»			
Тема 1. ***Управління інцидентами в системі забезпечення інформаційної безпеки організації*** ***Знати***: підходи до побудови ефективної системи інформаційної безпеки (ІБ), кращі практики щодо управління інцидентами ІБ, методику оцінки ефективності СМІБ по реакції на інциденти ІБ, вимоги міжнародних та вітчизняних документів з питань управління інцидентами ІБ, можливості використання процесного підходу до управління інцидентами, досвід виконання вимог міжнародних	Лекція 1	6*	Лекція-візуалізація
	Лекція 2		Кращі практики щодо управління інцидентами ІБ. Методика оцінки ефективності СМІБ по реакції на інциденти. Експрес-опитування студентів
	Практичне заняття 1		Управління інцидентами та проблемами в процесах підтримки IT -сервісів
	Практичне заняття 2		Аналіз стандартів ISO та української нормативної бази в частині управління інцидентами ІБ

документів щодо організації побудови процесу управління інцидентами в Україні. ***Вміти:*** розпізнавати виникнення інцидентів інформаційної безпеки та їх розслідування на прикладах. ***Формування компетенцій:*** К3 1, КФ4 ***Результати навчання:*** РН7, РН12 ***Рекомендовані джерела:*** **1,3,5,8,10,13,16,20,22,23,25,27,42,43**	Практичне заняття 3		Методика побудови процесу управління інцидентами ІБ
	Практичне заняття 4		Аналіз причин інцидентів інформаційної безпеки, пов'язані з роботою персоналу. Модульний контроль №1. Виконання кваліфікаційних завдань
Тема 2. ***Побудова та впровадження комплексної системи управління інцидентами інформаційної безпеки*** ***Знати***: Методику впровадження комплексної системи управління інцидентами ІБ, можливості системи підтримки управління інцидентами та проблемами, можливості використання інтелектуальної системи управління інцидентами інформаційної безпеки та підтримки прийняття рішень, принципи організації реагування на інциденти ІБ та підходи до оцінки інцидентів, структуру відповідальності в системі підтримки управління інцидентами та проблемами, можливості системи автоматизації процесу управління інцидентами ІБ в інформаційній системі, порядок використання моделей управління обробкою інцидентів ІБ. ***Вміти***: використовувати системи автоматизації процесу управління інцидентами ІБ в інформаційній системі- на прикладі SIEM, розробляти типове положення про групу реагування на інциденти інформаційної безпеки (ГРІІБ). ***Формування компетенцій:*** К31, КФ2, КФ4, КФ9 ***Результати навчання:*** РН4, РН16, РН21 ***Рекомендовані джерела:*** **1,4,5,6,8,11-13,16,17,22,35**	Лекція 3	6*	Використання багаторівневої моделі в системі підтримки управління інцидентами та проблемами. Лекція-візуалізація
	Лекція 4		Навчальна дискусія за темою Функції інтелектуальної системи підтримки прийняття рішень у рамках процесного підходу
	Практичне заняття 5		Розробка та впровадження комплексної системи управління інцидентами ІБ
	Практичне заняття 6		Створення системи інформаційної підтримки виявлення інцидентів безпеки. Підходи.
	Практичне заняття 7		Технічні засоби і системи виявлення інцидентів ІБ. Модульний контроль №2. Виконання кваліфікаційних завдань
Тема 3. ***Виявлення та документування інцидентів інформаційної безпеки*** ***Знати***: підходи до створення системи інформаційної підтримки виявлення інцидентів безпеки, можливості підтримки реагування на інциденти ІБ, можливості використання основних систем виявлення й попередження інцидентів, правила звітності про події та інциденти ІБ, вимоги стандартів до розробки і змісту Політики інформаційної безпеки організації, структурно-логічні схеми організації виявлення інцидентів ІБ, підходи до організації документування інцидентів інформаційної безпеки на рівні підприємства. ***Вміти***: використовувати захисні заходи і засоби від інцидентів; розробляти Керівництво по обробці інцидентів, пов'язаних з діями внутрішніх зловмисників.	Лекція 5	6*	Вимоги щодо політики управління інцидентами ІБ. Лекція-візуалізація
	Лекція 6		Система моніторингу подій і менеджмент інцидентів ІБ. Лекція-візуалізація з експрес-опитуванням студентів
	Практичне заняття 8		Організація реагування на інциденти ІБ. Аналіз можливостей використання основних систем виявлення й попередження інцидентів інформаційної безпеки
	Практичне заняття 9		Розробка типового положення про групу реагування на інциденти ІБ- ГРІІБ Обговорення щодо кращих політик інформаційної безпеки організації від компаній SANS і ін.
	Практичне заняття 10		Виявлення, обробка і звітність про події ІБ.

Формування компетенцій: К31, КФ4, КФ7, КФ9 ***Результати навчання:*** РН7, РН9, РН16, ***Рекомендовані джерела:*** **1,5,10,13,14, 23,26,29,30,43**	Практичне заняття 11		Використання метрик щодо управління інцидентами ІБ. Модульний контроль №3. Виконання кваліфікаційних завдань
Тема 1. Управління інцидентами в системі забезпечення інформаційної безпеки організації **Тема 2** Побудова та впровадження комплексної системи управління інцидентами ІБ **Тема 3**. Виявлення та документування інцидентів інформаційної безпеки	Самостійна робота	6*	1. Концептуальний підхід до побудови ефективної системи інформаційної безпеки. 2. Заходи щодо захисту інформації і політика інформаційної безпеки. 3. Співвідношення ефективності і рентабельності систем інформаційної безпеки. 4. Методика оцінки ефективності СМІБ (СУІБ) по реакції на інциденти. 5. Приклади інцидентів інформаційної безпеки та їх причини. 6. Управління інцидентами та безпекою бізнесу в методології управління інформаційними технологіями. 7. Аналіз вимог стандартів ISO/IEC та української нормативної бази в частині управління інцидентами інформаційної безпеки 8. Реалізація процесу управління інцидентами і проблеми інформаційної безпеки. 9. Управління інцидентами та проблемами в процесах підтримки IT-сервісів у відповідності з вимогами. бібліотек ITIL. 10. Розробка та впровадження комплексної системи управління інцидентами інформаційної безпеки 11. Багаторівнева модель в системі підтримки управління інцидентами та проблемами. 12. Структурно-логічна схема дій керівництва з управління інцидентами на підприємстві. 13. Автоматизація процесу управління інцидентами інформаційної безпеки. 14. Функції інтелектуальної системи підтримки прийняття рішень у рамках процесного підходу ISO/IEC та моделі PDCA. 15. Процедури ефективної роботи групи реагування на інциденти 16. Системи виявлення й попередження вторгнень. 17. Звітність про події та інциденти інформаційної безпеки. 18. Політика управління інцидентами інформаційної безпеки згідно ISO 27035. 19. Організація документування інцидентів інформаційної безпеки.

Модуль 2 «РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ»			
Тема 4. ***Моніторинг подій та реагування на інциденти інформаційної безпеки*** ***Знати:*** основні вимоги та заходи до моніторингу подій іменеджменту інцидентів інформаційної безпеки, підхід до побудови системи моніторингу ІБ, призначення та принципи побудови систем відображення атак і запобігання вторгнень, організація моніторингу подій та реагування на інциденти ІБ, основні структури SIEM-систем з моніторингу подій ІБ, порядок оцінки ефективності процесу управління інцидентами ІБ, витрати та підходи до оцінки забезпечення інформаційної безпеки, порядок розслідування і запобігання випадків з інцидентами, порядок використання DLP-системи при моніторингу ІБ, вимоги та порядок побудови системи розслідування інцидентів ІБ, , можливості моделей по розслідуванню інцидентів ІБ . ***Вміти***: використовувати методичні інструменти щодо застосовування при розслідуванні інцидентів ІБ. ***Формування компетенцій:*** КФ4, КФ7, КФ9 ***Результати навчання:*** РН8, РН12, РН14, РН21 ***Рекомендовані джерела:*** **1,3,4,7,12,20,21,27,32,33,36,41,42**	Лекція 7	6*	Підходи до побудови систем моніторингу інформаційної безпеки, відображення атак і запобігання вторгнень. Лекція-візуалізація
	Лекція 8		Заходи з вдосконаленням процесу управління інцидентами ІБ. Експрес-опитування студентів
	Практичне заняття 12		Використання метрик управління ІБ
	Практичне заняття 13		Система автоматизації процесу управління інцидентами ІБ в ІС.
	Практичне заняття 14		Досвід впровадження концепції ITSM в управлінні інцидентами ІБ Модульний контроль №4. Виконання кваліфікаційних завдань
Тема 5. ***Оцінка ефективності та вдосконалення процесу управління інцидентами інформаційної безпеки*** ***Знати***: Підходи до розробки та використання метрик інцидентів інформаційної безпеки, вимоги до організації безперервності бізнесу підприємства і управління інцидентами, методології, стандарти і нормативні вимоги в галузі управління безперервністю бізнесу, організацію проведення аудиту інформаційної безпеки ІС, найкращі міжнародні практики щодо управління інцидентами ІБ, вимоги бібліотек ITIL до управління інцидентами, методичні інструменти оцінки ефективності процесу управління інцидентами ***Вміти***: оцінювати ефективність інцидентів інформаційної безпеки організації за допомогою метрик безпеки. ***Формування компетенцій:*** К31, КФ2, КФ7, КФ9 ***Результати навчання:*** ПРН6-8, ПРН10, ПРН14 ***Рекомендовані джерела:*** **1,5,6,9,16,17-19,21,24,25,27,28,31,34,37-40,42**	Лекція 9	6*	Автоматизація моніторингу та розслідування інцидентів ІБ. Лекція-візуалізація
	Практичне заняття 15		Забезпечення безперервності бізнес-процесів і управління інцидентами ІБ. Вимоги
	Практичне заняття 16		Структура SIEM-Систем з моніторингу подій ІБ і оцінка ефективності процесу управління інцидентами
	Практичне заняття 17		Витрати на забезпечення ІБ організації і їх аналіз.
	Практичне заняття 18		Методологія аудиту інформаційної безпеки ІС. Модульний контроль №5. Виконання кваліфікаційних завдань
Тема 4. Моніторинг подій та реагування на інциденти інформаційної безпеки **Тема 5.** Оцінка ефективності та вдосконалення процесу управління	Самостійна робота	4*	1. Система моніторингу подій інформаційної безпеки 2. Підходи до побудови та реалізація систем відображення атак і запобігання вторгнень

інцидентами інформаційної безпеки			3. Досвід з організації моніторингу інцидентів інформаційної безпеки на рівні підприємства 4. Типові структури SIEM-систем з моніторингу подій інформаційної безпеки 5. Оцінка ефективності процесу управління інцидентами. 6. Порушення правил і завдання для успішного розслідування інцидентів інформаційної безпеки 7. Роботи, пов'язані з розслідуванням порушень інформаційної безпеки 8. Метрики безпеки і їх приклади 9. Контрольна карта Шухарта 10. Безперервність бізнесу і відновлення після інциденту 11. Процес визначення метрик і їх оцінки відповідно до нормативних документів і стандарту ISO 27004 12. Особливості методик проведення аудиту інформаційної безпеки 13. Особливості управління інцидентами інформаційною безпекою у процесах ITSM 14. Заходи з вдосконалення процесу управління інцидентами інформаційної безпеки

МАТЕРІАЛЬ НО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

- мультимедійна система Acer X113 DLP
- комп'ютери Asus
- комп'ютерний клас для проведення занять.

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Аудит та управління інцидентами інформаційної безпеки: навч. посіб. /[КорченкоО.Г.,ГнатюкС.О., КазмірчукС.В.та ін.]. – Київ : Центр навч.-наук. та наук.-пр.виданьНАСБ України, 2014. –190с. URL: https://er.nau.edu.ua/bitstream/NAU/38027/1/Audit%26Incident_15042014.pdf
2. Якименко Ю. М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства.- / Ю. М. Якименко, Т.М. Мужанова // Економіка. Менеджмент. Бізнес.– № 1(31). – К.: ДУТ, 2020. – С. 64-6 9. URL: http://journals.dut.edu.ua/index.php/emb/article/view/2377/2277
3. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— Київ : ДУТ, 2015.— 288 с.
4. Якименко Ю. М. Системний аналіз методологічних підходів до управління підприємством у сфері інформаційних технологій. // II Міжнародна науково-практична конференції «Підприємницька, торговельна, біржова діяльність: тенденції, проблеми та перспективи розвитку», 11лютого 2021 року.— Київ: ДУТ, 2021.- С. 279-282. URL: http://www.dut.edu.ua/uploads/n_9074_59003267.pdf
5. 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
6. Суворова О.Р. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки. Урок №12. URL: https://naurok.com.ua/keruvannya-mehanizmami-zahistu-mizhnarodni-standarti-informaciyno-bezpeki-104726.html
7. Рой Я.В., Мазур Н.П., Складанний П.М.Аудит інформаційної безпеки –основа ефективного захисту підприємств./ Кібербезпека: освіта, наука, техніка №1(1) - Київ: Київський університет імені Бориса Грінченка, 2018 с.87-93. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/23
8. Якименко Ю. М. Методологічні аспекти впровадження системного аналізу в побудові системи управління інформаційною безпекою.- Професійний розвиток фахівців у системі освіти дорослих: історія, теорія,технології: програма ІУ-ої Всеукраїнської Інтернет-конференції 16 жовтня 2019 р., м. Київ.-/ за наук. ред. В.В. Сидоренко; упорядкування Я.Л. Швень, М.І. Скрипник. К.: Агроосвіта, 2019.- С.41-43.
9. Якименко Ю. М. Аналіз стану використання методичних підходів до оцінки рівня економічної безпеки підприємства.- / Ю. М. Якименко, Т.М. Мужанова // Економіка. Менеджмент. Бізнес. – № .1 –К.: ДУТ, 2020. – С. 64-69. URL: http://journals.dut.edu.ua/index.php/emb/article/view/2386
10. Якименко Ю. М. Методичні піходи системного аналізу до вирішення проблем управління інформаційною безпекою в системі національної безпеки держави / Ю.М. Якименко // Актуальні проблеми управління інформаційною безпекою держави: XII Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей. Електронне видання — Київ: Нац. акад. СБУ, 2021.- С. 162-164. URL: http://academy.ssu.gov.ua/upload/file/%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D1%96%D1%8F%2026.03.2021.pdf
11. Якименко Ю. М. Управління інцидентами інформаційної безпеки в організації системи забезпечення кіберстійкості підприємства. Матеріали Всеукраїнської НПК Інтернет-конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу», 25 лютого 2021 року. Тези доповідей – Київ: ННІЗІ ДУТ, 2021.- С.24-25. URL: http://www.dut.edu.ua/uploads/l_2173_91341086.pdf.
12. Yakymenko, Y., Muzhanova, T., & Lehominova, S. (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
13. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
14. 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.
15. ДСТУ ISO/IEC 27031:2015 (ISO/IEC 27031:2011, IDT) Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу
16. ДСТУ ISO/IEC 27035-1:2018 (ISO/IEC 27035-1:2016, IDT). Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи керування інцидентами.
17. ДСТУ ISO/IEC 27035-2:2018 (ISO/IEC 27035-2:2016, IDT) Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 2. Настанова щодо планування та підготовки до реагування на інциденти.
18. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.
19. ISO/IEC 27002:2013 Technologies de l’information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l’information
20. ДСТУ ISO/IEC 27007:2018 (ISO/IEC 27007:2017, IDT) Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою
21. ДСТУ ISO 19011:2019 (ISO 19011:2018, IDT)Настанови щодо проведення аудитів систем управління
22. Якименко Ю.М. Використання спеціалізованих платформ і рішень з безпеки інформації в системному аналізі інформаційної безпеки організацій. // Матеріали: Науково-практична інтернет-конференція, Цифрова трансформація кібербезпеки. — Київ: ДУТ, 2021.- С.5-8. URL : http://www.dut.edu.ua/uploads/n_9126_17047934.pdf
23. Чернявський І.Р., Якименко Ю.М. Ризикоорієнтований підхід до управління інформаційною безпекою на підприємстві - Київ: ДУТ, 2022..- с. 38-45 URL: http://journals.dut.edu.ua/index.php/dataprotect/issue/view/164
24. Якименко Ю.М. Методичний підхід до забезпчення безперервності бізнесу й відновлення після інциденту

25. Якименко Ю.М. Підвищення ефективності системи менеджмента інформаційної безпеки організації
26. Легомінова С.В., Мужанова Т.М., Якименко Ю.М., Власенко В.О. Засоби інформування й навчання персоналу у сфері інформаційної безпеки в умовах цифровізації. Зв'язок. 2021. №4 (152). С.14-16.
27. 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://dut.edu.ua/uploads/l_2230_88161692.pdf .
28. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури (Постанова Кабінету Міністрів України від 24.03.2023 № 257).
29. 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.
30. Фахівець з планування політики та стратегії кібербезпеки, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-z-planuvannya-politiki-ta-strategiyi-kiberbezpeki.
31. Професійний стандарт Аудитор інформаційних технологій (з кібербезпеки), https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-auditor-informaciinikh-tekhnologii-z-kiberbezpeki.
32. Професійний стандарт Фахівець з реагування на інциденти кібербезпеки, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-fakhivec-z-reaguvannya-na-incidenti-kiberbezpeki.
33. Професійний стандарт Аналітик з оцінки вразливостей, https://cip.gov.ua/ua/news/proyekt-profesiinogo-standartu-analitik-z-ocinki-vrazlivostei
34. 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.
35. 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.
36. Мужанова Т.М., Легомінова С.В., 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.
37. Якименко Ю.М. Вирішення проблеми забезпечення безперервності бізнесу завдяки впровадженню центру кіберстійкості. Матеріали онлайн-конференціЇ Стратегії кіберстійкості: управління ризиками та безперервність бізнесу, 24 лютого 2022.. - Київ: ДУТ, 2022. - С.15-19 URL: https://dut.edu.ua/uploads/p_2121_33783557.pdf
38. Якименко Ю.М. Процесний підхід до управління безперервністю бізнесу на основі управління інформаційною безпекою. Матеріали онлайн-конференції Стратегії кіберстійкості: управління ризиками та безперервність бізнесу, 24 лютого 2022. /Якименко Ю.М., Шилан А.О.//.- Київ: ДУТ, 2022. – С.7-12 URL: https://dut.edu.ua/uploads/p_2121_33783557.pdf
39. Якименко Ю. М. Підвищення ефективності системи менеджмента інформаційної безпеки організації. Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції 27 жовтня 2022 року.-.Київ: ДУТ, 2022. - С.198-200
40. Якименко Ю.М., Дьячук О.С. Методичний підхід до забезпечення безперервності бізнесу й відновлення після інциденту Стратегії кіберстійкості: управління ризиками та безперервність бізнесу. Матеріали Всеукраїн. наук.- практ. конф., (м. Київ, Україна, 23 лютого 2023 р.). Київ: ДУТ, 2023. С. 49-51
41. Якименко Ю.М Підвищення ролі DLP - систем у розслідуванні інцидентів (кіберінцидентів) інформаційної безпеки. Всеукраїнська науково-практична конференція «Цифрова трансформація кібербезпеки» від 27 квітня 2023 року. - Київ: ДУТ, 2023.
42. Якименко Ю.М., Рабчун Д.І., Капелюшна Т.В. Використання методичних підходів системного аналізу до забезпечення інформаційної безпеки об’єктів критичної інфраструктури, Київ, 5с.
43. 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.

ПОЛІТИКА КУРСУ

- 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 виконане 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 40 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)	Змістовий контроль № 1	максимальна оцінка – 6 балів
	Змістовий контроль № 2	максимальна оцінка – 6 балів
	Змістовий контроль № 3	максимальна оцінка – 6 балів
	Змістовий контроль № 4	максимальна оцінка – 6 балів
	Змістовий контроль № 5	максимальна оцінка – 6 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*
1	Студент демонструє повні й міцні знання навчального матеріалу в обсязі, що відповідає	**Високий**	Відмінно /

	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.	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.	Зараховано (A)
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	**Середній** Є мінімально допустимим у всіх складових навчальної програми з дисципліни	Задовільно / Зараховано (E)

	відсутнє глибоке розуміння роботи та взаємозв'язків з іншими дисциплінами.		
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 заліку.	**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*