СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «Методи та засоби 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 Moodle**	**e-mail:**yakum14@ukr.net; **сторінка курсу в Moodle – https://dn.dut.edu.ua/course/view.php?id=412**	
Галузь знань			12 Інформаційні технології		**Рівень вищої освіти**	третій (освітньо-науковий) - доктор філософії	
Спеціальність			125 Кібербезпека		**Семестр**	1	
Освітня програма			КІБЕРБЕЗПЕКА		**Тип дисципліни**	вибірковий компонент ОНП	
Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінарських занять	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18	-	54

АНОТАЦІЯ КУРСУ

Мета курсу:	формування необхідних базових теоретичних знань, умінь і набуття практичних навичок їх застосування, необхідних для використання методів та засобів управління інцидентами інформаційної безпеки у дослідженні складних організаційно-технічних систем на об'єктах інформаційної діяльності.

Компетентності відповідно до освітньої програми

Загальні компетентності (ЗК)	**Фахові компетентності (ФК)**
	ФК-1. Інтегративна компетентність–здатність до інтеграції знань, умінь і навичок та їх ефективного використання в умовах швидкої адаптації організацій до вимог зовнішнього середовищ, що забезпечують виконання завдань науково-дослідної, науково-педагогічної, управлінської та інноваційної діяльності в інформаційній та безпековій сфері тощо. **ФК-2. Соціально-психологічна компетентність** (емоційні, перцептивні, концептуальні, поведінкові) – здатність особистості орієнтуватися у різних життєвих ситуаціях, ефективно працювати в умовах ринкової економіки; уміння реалізувати стратегії і плани; здатність до розуміння поведінки людей, мотивації та організації їх спільної діяльності тощо.

	ФК-6. Політехнічна компетентність –знання загальних (методологічних, історичних, економічних, ергономічних тощо) питань безпекової сфери, принципів дії і будови основних функціональних органів інформаційних систем; здатність до оволодіння… сучасними інформаційними та безпековими технологіями; здатність до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ФК-7**. Інженерна компетентність –здатність до виробничо-технологічної діяльності (розробки та впровадження інноваційних технологій інформаційної безпеки, вибору технології ІБ, устаткування та засобів, використання інформаційних технологій; розробки програм і методик випробувань систем інформаційної та кібербезпеки); здатність до організаційно-управлінської діяльності (організації процесу створення та надання інфокомунікаційних послуг); здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо. **ФК-8.** Ділова компетентність–здатність і готовність здійснювати ефективну професійну діяльність у відповідній галузі, надавати інфокомунікаційні послуги та послуги безпеки; здатність до планування й реалізації заходів із захисту інформації в ІКС, створення та забезпечення функціонування систем інформаційної та кібербезпеки; здатність до формування правильних висновків, оперативного приймання та реалізації нестандартних рішень тощо.
Програмні результати навчання (ПРН)	
ПРН-12 Уміти визначати основні параметри інформаційних ресурсів наукового дослідження (навчального процесу), планувати структуру, зміст та процес організації його проведення (лекцій, практично-семінарських занять). **ПРН-15** Уміти орієнтуватися у сучасних концепціях і моделях, методах та засобах управління інцидентами інформаційної безпеки. (ІБ). **ПРН-16**. Уміти розробляти та проектувати нові, вдосконалювати існуючі системи управління інформаційною безпекою. **ПРН-21**. Уміти аналізувати та розробляти алгоритми, методики, моделі та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки. **ПРН-25.** Уміти визначати можливості для підприємницької та громадської діяльності за напрямом захисту інформації, організації й забезпечення інформаційної та кібербезпеки об’єктів інформаційної діяльності. **ПРН-28**. Бути здатним до застосування різноманітних, професійно профільованих знань і практичних навичок у сфері захисту інформації. **ПРН-29**. Уміти розробляти та впроваджувати раціональні технології інформаційної безпеки, програми і методики випробувань систем інформаційної та кібербезпеки **ПРН-30.** Бути здатним до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки інформаційних і комунікаційних систем, до обробки та перетворення інформації тощо.	

ОРГАНІЗАЦІЯ НАВЧАННЯ			
Тема, опис теми	**Вид заняття**	**Оцінювання за тему**	**Форми і методи навчання/питання до самостійної роботи**
Змістовий модуль 1. "УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ"			
Тема 1. ***Підходи до управління інцидентами в системі забезпечення інформаційної та кібербезпеки 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. ***Вміти:*** розпізнавати виникнення інцидентів інформаційної безпеки та їх розслідування на прикладах. ***Формування компетенцій:*** ФК3, ФК4 ***Результати навчання:*** ПРН 12, ПРН16 ***Рекомендовані джерела:*** **1,3,5,8,10,13-16,18,24-27, 30-31,33**	Лекція 1	5,5*	Лекція-візуалізація
	Лекція 2		Лекція-візуалізація. Експрес-опитування студентів
	Практичне заняття 1		Аналіз причин інцидентів інформаційної безпеки, пов'язані з роботою персоналу та їх розслідування
	Практичне заняття 2		Управління інцидентами та безпекою бізнесу в методології управління інформаційними технологіями Модульний контроль №1. Виконання кваліфікаційних завдань
Тема 2***. Використання вимог нормативних документів у побудові процесів управління інцидентами інформаційної та кібербезпеки організації*** ***Знати***: досвід виконання вимог міжнародних документів щодо організації побудови процесу управління інцидентами в Україні, принципи організації реагування на інциденти ІБ та підходи до оцінки інцидентів, методику впровадження комплексної системи управління інцидентами ІБ, основні завдання управління інцидентами, компоненти та принципи створення системи. управління інцидентами ІБ,методику створення системи управління інцидентами ІБ, структуру відповідальності в системі підтримки управління інцидентами та проблемами, можливості системи автоматизації процесу управління інцидентами ІБ в інформаційній системі. ***Вміти***: розробляти типове положення про групу реагування на інциденти інформаційної безпеки (ГРІБ). ***Формування компетенцій:*** ФК4 ***Результати навчання:*** ПРН12, ПРН15 ***Рекомендовані джерела:*** **1,4,5,6,8,11,13,17,18,21,22,24,30-32**	Лекція 3	5,5*	Лекція-візуалізація
	Лекція 4		Лекція-візуалізація. Експрес-опитування студентів
	Лекція 5		Навчальна дискусія за темою Розробка та впровадження комплексної системи управління інцидентами ІБ
	Практичне заняття 3		Методика оцінки витрат організації на інформаційну безпеку. Вирішення практичної задачі- розробка типового положення про ГРІБ.
	Практичне заняття 4		Використання метрик управління інформаційною безпекою Модульний контроль №2. Виконання кваліфікаційних завдань

Тема 1. Підходи до управління інцидентами в системі забезпечення інформаційної та кібербезпеки організації **Тема 2.** Використання вимог нормативних документів у побудові процесів управління інцидентами інформаційної та кібербезпеки організації	Самостійна робота		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.
Змістовий модуль 2. " РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ "			
Тема 3. ***Створення систем моніторингу подій та розслідування інцидентів інформаційної та кібербезпеки*** ***Знати:*** основні вимоги та заходи до моніторингу подій іменеджменту інцидентів інформаційної безпеки, підхід до	Лекція 6	5,5*	Експрес-опитування студентів. Лекція-візуалізація
	Лекція 7		Навчальна дискусія за темою заняття

побудови системи моніторингу ІБ, порядок використання DLP-системи при моніторингу ІБ, організація моніторингу подій та реагування на інциденти ІБ, порядок оцінки ефективності процесу управління інцидентами ІБ, організацію обробки інцидентів ІБ, основні структури SIEM-систем з моніторингу подій ІБ, порядок розслідування і запобігання випадків з інцидентами, вимоги та порядок побудови системи розслідування інцидентів ІБ, можливості моделей по розслідуванню інцидентів ІБ . ***Вміти***: використовувати системи автоматизації процесу управління інцидентами ІБ в інформаційній системі- на прикладі SIEM, використовувати методичні інструменти щодо застосовування при розслідуванні інцидентів ІБ. ***Формування компетенцій:*** ФК4 ***Результати навчання:*** ПРН12, ПРН15 ***Рекомендовані джерела:*** **1,3,4,7,22-24,30-32**	Практичне заняття 5		Оцінка ефективності процесу управління інцидентами ІБ.
	Практичне заняття 6		Правила виявлення та звітності про події та інциденти ІБ
	Практичне заняття 7		Розробка положення про групу реагування на інциденти ІБ
	Практичне заняття 8		Побудова системи розслідування інцидентів ІБ Модульний контроль №3. Виконання кваліфікаційних завдань
Тема 4. ***Міжнародні практики щодо управління інцидентами інформаційної та кібербезпеки у забезпеченні безперервності бізнесу*** ***Знати***: вимоги до організації безперервності бізнесу підприємства і управління інцидентами; методології, стандарти і нормативні вимоги в галузі управління безперервністю бізнесу; найкращі міжнародні практики щодо управління інцидентами ІБ, вимоги до управління інцидентами по забезпеченню безперервності бізнес-процесів і відновленню після інцидентів. ***Вміти***: оцінювати ефективність управління інцидентами інформаційної безпеки і організації відновлення після інциденту. ***Формування компетенцій:*** ФК3, ФК4 ***Результати навчання:*** ПРН12, ПРН15, ПРН16 ***Рекомендовані джерела:*** **1,5,6,9,12,21-29**	Лекція 8	5,5*	Лекція-візуалізація. Експрес-опитування студентів
	Лекція 9		Навчальна дискусія за темою Структуру системи управління інцидентами інформаційної безпеки (на прикладі NAU-CERT)
	Практичне заняття 9		Вимоги по забезпеченню безперервності бізнес-процесів, відновленню процесів після інцидентів і їх реалізація Модульний контроль №4. Виконання кваліфікаційних завдань
Тема 3. Створення систем моніторингу подій та розслідування інцидентів інформаційної безпеки **Тема 4.** Міжнародні практики щодо управління інцидентами інформаційної безпеки у забезпеченні безперервності бізнесу	Самостійна робота		1. Система моніторингу подій інформаційної безпеки 2. Підходи до побудови та реалізація систем відображення атак і запобігання вторгнень 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

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: засоби підтримки прийняття рішень у сфері ІБ

ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДИСЦИПЛІНИ

1. Роїк О. М. Системний аналіз. Навчальний посібник / О. М. Роїк, А. А. Шиян, Л.О. Нікіфорова – Вінниця : ВНТУ, 2015. – 83 с. URL: http://nikiforova.vk.vntu.edu.ua/file/bfb63146b18f718fe1ff1ed4ce9b9a58.pdf

2. Варенко В. М. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – К. : Університет «Україна», 2013. – 203 с. URL: http://er.nau.edu.ua/handle/NAU/20105; http://er.nau.edu.ua:8080/handle/NAU/20105

3. 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 / – К.:ДУТ, 2015. – 345 с. URL: http://www.dut.edu.ua/uploads/l_1242_54311567.pdf https://app.box.com/s/g7bqinazmw3i52kp43qizon9v6u9ryxd.

4.Маркіна І.А. Основи формування системи менеджменту інформаційної безпеки підприємства. URL: http://dspace.pdaa.edu.ua:8080/bitstream/123456789/3092/1/piprp_2016_3%281%29__18.pdf.

5.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 .

6.Соколов В.Ю. «Інформаційні системи і технології: Навчальний посібник». ДУІКТ, 2010. URL: http://www.dut.edu.ua/uploads/l_603_15334144.pdf

7. Пєклун К. В. Теорія систем і системний аналіз. Одеса: ОРІДУ НАДУ при Президентові України, 2013. URL: http://oridu.odessa.ua/7/7/pdffile/6.pdf.

8. Побудова Системи управління інформаційною безпекою (СУІБ). URL: https://zahyst-ua.com/pobudova-sistemi-upravlinnya-informacijnoju-bezpekoju-suib/.

9. Данілова Е.І. Концепція системного підходу до управління економічною безпекою підприємства. Монографія. Вінниця: Європейська наукова платформа, 2020. 342с. URL: https://ojs.ukrlogos.in.ua/index.php/monograph/article/view/danilova.kontseptsiia-2020/1859

10. Грецька Г. М. Конспект лекцій з курсу «Теорія систем і системний аналіз»/ Г. М. Грецька: Харк. нац. акад. міськ. госп-ва. - Х.: ХНАМГ. 2011. - 148 с.

11. Рудий Т.В.,Кулешник Я.Ф. Організаційні принципи створення системи управління інформаційною безпекою інформаційних систем спеціального призначення.- Таврійський державний агротехнологічний університет.с.347-354. URL: http://www.nbuv.gov.ua/old_jrn/soc_gum/znptdau/2012_2_2/18-2-43.pdf

12. Система управління подіями інформаційної безпеки IBM QRadar. URL: https://pirit.biz/reshenija/informacionnaja-bezopasnost/sistema-upravleniya-sobytiyami-informacionnoj-bezopasnosti-ibm-qradar/.

13. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. К.: НАНУ, 2009- 143с.

14. 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). Київ,ДУТ, 2021. С.173-176. URL: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

15. Savchenko V. Coordination Model for the National Cyber Security System of Ukraine / V. Savchenko, S. Kononenko. V. Bobylov, L. Drok // Сучасні інформаційні технології у сфері безпеки та оборони. – К.: НУОУ, 2017, № 1 (28).

16. Савченко В. А. Управління ризиками кібербезпеки на основі теоретико-ігрового підходу / Савченко В. А., Мацько О. Й. // Сучасний захист інформації №2(38), 2019 – С. 6-16.

17. Савченко В. А., Моделювання кібератак засобами теорії графів // В. А. Савченко, О. Й. Мацько, С. В. Легомінова, І. С. Полторак, В. В. Марченко // Сучасний захист інформації №4(40), 2019. – С. 6-11.

18. Модель трансформації національної системи кібербезпеки в умовах дії гібридних загроз / Боярчук Р. М., Савченко В. А., Мацько О. Й., Новікова І. В. // Сучасний захист інформації №1(41), 2020. – С. 6–10.

19. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov, V. Savchenko and others. – Kharkiv: PC Technology Center, 2021. – 188 p.

20. Мужанова Т.М., Легомінова С.В., Якименко Ю.М., Мордас І.В. 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.

21. Якименко Ю.М. Особливості реалізації системного методу стосовно побудови систем управління інформаційною безпекою організації. Матеріали:

«Актуальні проблеми управління інформаційною безпекою держави: нові виклики та стратегії протидії». X Всеукраїнська науково-практична конференція. Збірник тез наукових доповідей. Електронне видання. Київ: Нац. акад. СБУ, 2019. С. 144-147. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf.

22. Якименко Ю.М., Мужанова Т.М., Легомінова С.В. Системний аналіз технічних систем забезпечення інформаційної безпеки підприємств від компанії FIREEYE. Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка&quot. Київ, 2021. 4(12), 36-50. URL : https://doi.org/10.28925/2663-4023.2021.12.3650 .

23. 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). Київ,ДУТ, 2021. С.173-176. URL: http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

24. 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

25. ДСТУ ISO/IEC 27000:2019 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. (ISO/IEC 27000:2018, IDT) . (ДСТУ ISO/IEC 27000:2017).

26. ДСТУ ISO/IEC 27001:2015.(Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).

27. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. (Ідентичний до міжнародного ISO/IEC 27002:2013 Cor 1:2014).

28. ДСТУ ISO/IEC 27007:2018. Інформаційні технології. Методи захисту. Настанова щодо аудиту систем керування інформаційною безпекою. (ISO/IEC 27007:2017, IDT).

29. ДСТУ ISO/IEC 27031:2015. Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. (ISO/IEC 27031:2011, IDT).

30. 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.

31. 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.

32. ДСТУ ISO 19011:2019. Настанови щодо проведення аудитів систем управління. (ISO 19011:2018, IDT).

33. ДСТУ ISO 31000:2018.Менеджмент ризиків. (ISO 31000:2018, IDT).

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 35 балів у сукупності за всіма темами дисципліни

Форми контролю	Види навчальної роботи	Оцінювання
ПОТОЧНИЙ КОНТРОЛЬ	***Робота на заняттях,*** *у т.ч.:*	
	• присутність на заняттях (при пропусках занять з поважних причин допускається відпрацювання пройденого матеріалу)	за кожне відвідування 0,55 балів
	• 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 «УПРАВЛІННЯ ІНЦИДЕНТАМИ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ ОРГАНІЗАЦІЇ»	максимальна оцінка – 15 балів
	Модульний контроль № 2 «РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ІНЦИДЕНТАМИ»	максимальна оцінка – 15 балів
Додаткова оцінка	Участь у наукових конференціях, підготовка наукових публікацій, участь у Всеукраїнських та Міжнародних конкурсах наукових студентських робіт за спеціальністю, створення кейсів тощо.	Звільняється від заліку
ПІДСУМКОВЕ ОЦІНЮВАННЯ ***Залік***	Метою заліку є контроль сформованості практичних навичок та професійних компетентностей, необхідних для виконання професійних обов'язків. Залік проходить у письмовій формі.	40 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 (В)
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	Достатній Конкретний рівень, за вивченим матеріалом робочої програми дисципліни. Додаткові питання про можливість використання теоретичних положень для практичного використання	Добре / Зараховано (С)

	проведенні практичних занять, при виконанні індивідуальних / контрольних завдань та поясненні прийнятих рішень, в межах дисципліни, що вивчається.	викликають утруднення.	
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 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*

8. Мова вивчення освітньої компоненти
(українська, англійська, розділи, що викладаються англійською мовою)
українська
9. Інформаційне забезпечення освітньої компоненти
Рекомендовані джерела та інші навчальні ресурси: вказати підручники, навчальні посібники не пізніше 2010 року видання, які є у нас у бібліотеці на державній мові; електронні ресурси, посилання, електронна бібліотека ДУТ, іншомовні джерела

1. Роїк О. М. Системний аналіз. Навчальний посібник / О. М. Роїк, А. А. Шиян, Л.О. Нікіфорова – Вінниця : ВНТУ, 2015. – 83 с. http://nikiforova.vk.vntu.edu.ua/file/bfb63146b18f718fe1ff1ed4ce9b9a58.pdf
2. Варенко В. М. Системний аналіз інформаційних процесів : навч. посіб. / В. М. Варенко, І. В. Братусь, В. С. Дорошенко, Ю. Б. Смольников, В.О. Юрченко. – К. : Університет «Україна», 2013. – 203 с. http://er.nau.edu.ua/handle/NAU/20105 http://er.nau.edu.ua:8080/handle/NAU/20105
3. 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 / – К.:ДУТ, 2015. – 345 с. http://www.dut.edu.ua/uploads/l_1242_54311567.pdf https://app.box.com/s/g7bqinazmw3i52kp43qizon9v6u9ryxd.
4. Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. Управление инцидентами информационной безопасности и непрерывностью бизнеса. Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2013. — 170 с.
5. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью Учебное пособие для вузов.2-е изд., испр.Серия «Вопросы управления информационной безопасностью. Выпуск 1» 2016 г.244 с. http://www.techbook.ru/book.php?id_book=687.
6. Руководство по реагированию на инциденты информационной безопасности. Управление технологических решении. Версия 1.0. М.:Kaspersky Lab, 2017 . — Электронный ресурс. Режим доступа: Incident_Response_Guide_rus.pdf
7. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. К.: НАНУ, 2009- 143с.
8. 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
9. 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.
10. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
11. 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
12. ISO/IEC 27035:2011«Information technology. Security techniques. Information security incident management»

10. Методи оцінювання, підсумкові звітності за освітньою компонентою
(заліки, екзамени, курсові проекти, тестування)
Тестування, залік
11. Матеріально-технічне забезпечення освітньої компоненти
Спеціалізована лабораторія: «Управління кібербезпекою» (комп’ютери, комп’ютерна локальна мережа, мультимедійний проектор, екран)
Використання програмного забезпечення виявлення загроз інформаційній безпеці у режимі реального часу (IBM Security QRadar SIEM)