Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми «Управління інформаційною та кібернетичною безпекою»
(назва)

Освітнього рівня другого (магістерського) рівня вищої освіти

Спеціальності 125 «Кібербезпека»

Галузь знань 12 «Інформаційні технології»

1. Назва освітньої компоненти "Управління інцидентами інформаційної безпеки"
(назва дисципліни)

2. Тип основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	6	180	18		18		154
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Нормативно-правове забезпечення інформаційної безпеки 2. Системний аналіз інформаційної безпеки 3. Менеджмент інформаційної безпеки 4. Аналіз та оцінка уразливостей інформаційних систем						
Освітні компоненти для яких є базовою	1.Управління ризиками інформаційної безпеки 2. Теорія ризиків 3. Управління інформаційною безпекою банків 4. Системи управління інформаційною безпекою 5. Аудит систем захисту інформації 6. Аудит інформаційної безпеки						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ОПП							
Знати			**Вміти**				
1. **ЗК 1.** Здатність застосовувати знання у практичних ситуаціях.			1. **ПП 1.** Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та кібербезпеки.				

2. **ЗК 5.** Здатність до пошуку, оброблення та аналізу інформації.	2. **ПРН 7.** Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
	3. **ПРН 46.** Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів захисту інформації.
Компетенції відповідно до вимог роботодавців	
1. Знання та розуміння стандартів ІБ ISO 27035.	1. Застосовувати на практиці здобуті знання, розуміти і використовувати у повсякденній діяльності методи та технології управління системами інформаційної безпеки підприємства.
2. Практичні навички впровадження систем менеджменту ІБ та системи управління інцидентами інформаційної безпеки.	2. Моделювати структуру дослідження, формулювати мету, об'єкт, предмет та задачі, упорядковувати та систематизувати результати.
3. Забезпечення аудиту процесів. Аналітичне та логічне мислення аудиторів.	3. Використовувати професійно профільовані знання, уміння й навички для формування системи (органів, підрозділів), що забезпечують інформаційну безпеку.
4. Моніторинг інцидентів інформаційної безпеки.	
6. Результати навчання відповідно до ОПП	
1. **ПП 9.** Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною безпекою.	
2. **ПП 11.** Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем.	
3. **ПРН 4.** Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності,які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.	
4. **ПРН 10.** Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.	
5. ПРН 19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.	

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1 **Основні положення теорії систем у сфері інформаційної безпеки**						
Розділ 1 **Побудова системи забезпечення ІБ на основі управління інцидентами інформаційної безпеки**						
Тема 1 **Основні поняття та принципи створення системи управління інцидентами інформаційної безпеки**						
	Лекція 1	**Концептуальний підхід до побудови ефективної системи ІБ**	1. Підхід до побудови ефективної системи ІБ 2. Заходи щодо захисту інформації.		посилання на електронний ресурс	http://dl.dut.edu.ua/course/view.php?id=2912

	Лекція 2	**Місце і роль управління інцидентами в системі забезпечення ІБ організації**	1. Кращі практики щодо керування інцидентами ІБ. 2. Методику оцінки ефективності СМІБ по реакції на інциденти.			http://dl.dut.edu.ua/course/view.php?id=2912
	Лекція 3	**Побудова процесу управління інцидентами**	1. Принципи побудови процесу управління інцидентами. 2. Основні завдання управління інцидентами.			http://dl.dut.edu.ua/course/view.php?id=2912
	Лекція 4	**Обробка і оцінка інцидентів інформаційної безпеки**	1.Процедури ефективної роботи групи реагування на інциденти. 2.Управління обробкою інцидентів інформаційної безпеки. 3. Оцінка інцидентів інформаційної безпеки на підставі їх факторів.			http://dl.dut.edu.ua/course/view.php?id=2912
	Лекція 5	**Розробка та впровадження комплексної системи управління інцидентами інформаційної безпеки**	1. Компоненти та принципи створення системи. управління інцидентами ІБ. 2. Методику створення системи управління інцидентами ІБ.			http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 1	**Аналіз міжнародних стандартів ISO/IEC та української нормативної бази в частині управління інцидентами інформаційної безпеки**	Вимоги стандартів до управління інцидентами інформаційної безпеки.	Впроваджувати вимоги стандартів та нормативних документів до систем управління інцидентами інформаційної безпеки		http://dl.dut.edu.ua/course/view.php?id=2912

	Практичне заняття 2	**Оцінка витрат організації на забезпечення інформаційної безпеки**	Методику оцінки витрат організації на інформаційну безпеку.	1. Аналізувати витрати на забезпечення інформаційної безпеки. 2. Проводити оцінку витрат організації на інформаційну безпеку.		http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 3	**Процедури оцінки ефективності системи управління інцидентами інформаційної безпеки**	Заходи вимірювання, які пов'язані з управлінням інцидентами ІБ.	Проводити оцінку ефективності системи управління інцидентами.		http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 4	**Використання метрик управління безпекою**	Перелік і методику оцінювання ефективності метрик управління інформаційною безпекою.	Застосувати метрики управління інформаційною безпекою.		http://dl.dut.edu.ua/course/view.php?id=2912
Розділ 2 **Методичні підходи щодо процесів функціонування системи управління інцидентами інформаційної безпеки**						
Тема 2 **Реалізація концепції системи управління інформаційними інцидентами**						
	Лекція 6	**Система моніторингу подій ІБ**	1.Підхід до побудови системи моніторингу ІБ. 2.Порядок використання DLP-системи при моніторингу ІБ.			http://dl.dut.edu.ua/course/view.php?id=2912
	Лекція 7	**Система розслідування інцидентів.**	1. Порядок розслідування і запобігання випадків з інцидентами 2. Підход до організації реагування на інциденти			http://dl.dut.edu.ua/course/view.php?id=2912
	Лекція 8	**Інтелектуальна система управління інцидентами інформаційної безпеки та підтримки прийняття рішень**	1. Практику застосування інтелектуальних систем управління. 2. Чинники, критерії, показники та складнощі сучасних інформаційних телекомунікаційних технологій.			http://dl.dut.edu.ua/course/view.php?id=2912

			3. Функції інтелектуальної системи підтримки прийняття рішень у рамках процесного підходу ISO/IEC та моделі PDCA.			
	Лекція 9	**Управління інцидентами та безпекою бізнесу в методології управління інформаційними технологіями.**	1. Підходи до управління інцидентами та проблемами в процесах підтримки IT-сервісів. 2. Підходи до управління процесами підтримки IT-сервісів у відповідності з ITIL.			http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 5	**Топ 20 найбільш критичних захисних заходів та засобів.**	Найбільш важливі захисні заходи і засоби від інцидентів.	Використовувати Топ-20 найбільш важливих захисних заходів і засобів від інцидентів.		http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 6	**Керівництво по обробці інцидентів, пов'язаних з витоком внутрішньої інформації і діями внутрішніх зловмисників**.	Вимоги Керівництв по обробці інцидентів, пов'язаних: - з витоком внутрішньої інформації, - з діями внутрішніх зловмисників.	Використовувати вимоги Керівництв по обробці інцидентів.		http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 7	**Керівництво по обробці інцидентів, пов'язаних з зараженням вірусною програмою Windows і DDoS-атаками.**	Вимоги Керівництв по обробці інцидентів, пов'язаних: - з зараженням шкідливою програмою Windows-комп'ютера; - з DDoS-атаками..	Використовувати вимоги Керівництв по обробці інцидентів.		http://dl.dut.edu.ua/course/view.php?id=2912
	Практичне заняття 8	**Забезпечення безперервності бізнес-процесів і управління інцидентами**	Вимоги до планування безперервності бізнесу бізнесу і відновлення після інциденту.	Використовувати вимоги по забезпеченню безперервності бізнес-процесів і управління інцидентами		http://dl.dut.edu.ua/course/view.php?id=2912

	Практичне заняття 9	**Практична реалізація концепції системи управління інформаційними інцидентами**	Досвід: - моделювання процесів управління інцидентами ІБ; - створення системи управління інформаційними інцидентами.	Використовувати досвід створення системи управління інформаційними інцидентами.		http://dl.dut.edu.ua/course/view.php?id=2912

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. Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. К.: НАНУ, 2009- 143с.
7. 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
8. 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.
9. ДСТУ ISO/IEC 27001:2015 (Ідентичний до міжнародного ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements).
10. 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
11. 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)