Інформаційний пакет освітніх компонент навчального плану
освітньо-професійної програми Інформаційна та кібернетична безпека
(назва)

Освітнього рівня **бакалавр**

Спеціальності **125 «Кібербезпека»**

Галузь знань **12 «Інформаційні технології»**

1. Назва освітньої компоненти Політики безпеки
(назва дисципліни)

2. Тип основна

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18		18	18	36
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Теоретичні основи захищених інформаційно-комунікаційних технологій 2. Аналіз та оцінка уразливостей інформаційних систем						
Освітні компоненти для яких є базовою	1. Комплексні системи захисту інформації 2. Кібербезпека банківських та комерційних структур						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ООП							
Знати			**Вміти**				
1. Знання та розуміння предметної області та розуміння професії.			1. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та кібербезпеки				
2. Здатність до пошуку, оброблення та аналізу інформації.			2. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та кібербезпеки				
3.			3. 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.
Компетенції відповідно до вимог роботодавців	
1. Знання та розуміння формування політики безпеки інформації	1. Здатність упроваджувати в інформаційні і комунікаційні системи сучасні методи забезпечення інформаційної безпеки відповідно до вимог вітчизняних та міжнародних стандартів
2. Знання та розуміння про моделювання уразливостей, загроз та атак в розподілених системах	2. Здатність упроваджувати в інформаційні і комунікаційні системи сучасні методи забезпечення інформаційної безпеки відповідно до вимог вітчизняних та міжнародних стандартів

6. Результати навчання відповідно до ОПП

1. 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

2. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах..

3. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і кібербезпеки.

4. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і кібербезпеки.

5. Застосовувати різні класи політик інформаційної безпеки та кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.

7. План вивчення освітньої компоненти

Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
Вступ	Лекція 1	Тема: Введення в дисципліну.	1. Роль і місце курсу в загальній системі підготовки бакалавра. 2. Об'єкти і предмети вивчення дисципліни. 3. Загальну структуру курсу			http://dl.dut.edu.ua/course/view.php?id=2021
	Практичне заняття 1	Тема: Введення в дисципліну.	1. Поняття політики безпеки інформації. 2. Головні етапи створення політики безпеки інформації.			http://dl.dut.edu.ua/course/view.php?id=2021

			3. Інциденти у сфері високих технологій. 4. Етапи життєвого циклу інформації та її загальні властивості.			
Розділ 2						
Технологія попереднього аудиту безпеки інформаційно-комунікаційної системи як передумова побудови політики безпеки	Лекція 1	Тема: Необхідність захисту інформації в сучасних умовах.	1. Основні положення системно-концептуального підходу до захисту інформації. Класифікація цілей захисту. 2. Визначення і аналіз поняття загрози безпеці інформації. 3. Особливості реалізації атак та заходи послаблення їх деструктивного впливу. 4. Систему показників уразливості інформації і вимоги до первинних даних.			http://dl.dut.edu.ua/course/view.php?id=2021
	Лекція 2	Тема: Аналіз організації функціонування автоматизованої системи.	1. Аналіз організації функціонування автоматизованої системи. 2. Порядок проведення робіт з обстеження АС. 3. Аналіз умов функціонування ОІД, його розташування на місцевості 4. Ситуаційний план ОІД 5. План-схема контрольованої території ОІД 6. Генеральні плани поверхів будівлі, на яких розташовано ОІД 7. ОТЗ, схеми розташування			http://dl.dut.edu.ua/course/view.php?id=2021

			на ОІД, та їх опис 8. ДТЗС, схеми розташування на ОІД, та опис схем 9. Система електроживлення 10. Система заземлення 11. Система телефонного зв'язку 12. Системи охоронної і пожежної сигналізації 13. Системи опалення, водопостачання та каналізації 14. Виявлення незадіяних та транзитних електропровідних кабелів, кіл, дротів 15. Визначення наявності на ОІД діючих засобів та систем технічного захисту інформації 16. Перевірка наявності НД системи ТЗІ			
	Лекція 3	Тема: Моделі порушника та загроз, аналіз ризику функціонування АС.	1. Модель загроз інформації в РКМ. 2. Неформальна модель порушника в РКМ. 3. Аналіз ризику функцюнування автоматизованих систем			http://dl.dut.edu.ua/course/view.php?id=2021
	Практичне заняття 1	Тема: Необхідність захисту інформації в сучасних умовах.		1. Застосовувати системно-концептуальний підхід до захисту інформації. 2. Визначати особливості реалізації атак та заходи послаблення їх		http://dl.dut.edu.ua/course/view.php?id=2021

				деструктивного впливу. 4. Застосовувати систему показників уразливості інформації і вимоги до первинних даних		
	Практичне заняття 2, 3, 4, 5	Тема: Опис інформаційно-комунікаційної системи та середовища її функціонування.		1. Аналізувати організацію функціонування автоматизованої системи. 2. Проводити роботи з обстеження АС. 3. Аналізувати умови функціонування ОІД.		http://dl.dut.edu.ua/course/view.php?id=2021
	Практичне заняття 6	Тема: Моделі порушника та загроз, аналіз ризику функціонування АС.		1. Розробляти модель загроз інформації в РКМ. 2. Розробляти неформальну модель порушника в РКМ. 3. Аналізувати ризики функціонування автоматизованих систем		http://dl.dut.edu.ua/course/view.php?id=2021
Розділ 3						
Основи аналізу і синтезу політик безпеки	Лекція 1	Тема: Основи аналізу політик безпеки та класифікація політик безпеки	1. Документи, що забезпечують політику безпеки інформації. 2. Гарантії правильності забезпечення політики безпеки інформації			http://dl.dut.edu.ua/course/view.php?id=2021
	Лекція 2	Тема: Аналіз кращих зразків створення політик інформаційної безпеки	1. Концепцію розроблення захищених систем компанії IBM. 2. Концепцію розроблення захищених систем компанії Microsoft. 3. Концепцію розроблення захищених систем компанії Sun Microsystems.			http://dl.dut.edu.ua/course/view.php?id=2021

			4. Архітектуру безпеки SAFE компанії Cisco Systems. 5. Концепцію розроблення захищених систем компанії Symantec. 6. Підхід компанії SANS			
Розділ 4						
Оцінка політики безпеки	Лекція 1	Тема: Сервіси безпеки як основа підтримки політики безпеки	1. Сервіси безпеки. 2.Ідентифікація/автентифікація. 3. Розмежування доступу. 4. Протоколювання й аудит. 5. Екранування. 6. Тунелювання. 7. Шифрування. 8. Контроль цілісності. 9. Контроль захищеності. 10. Виявлення відмов й оперативне відновлення. 11. Управління.			http://dl.dut.edu.ua/course/view.php?id=2021
	Лекція 2	Тема: Нормативно-правова основа створення політик безпеки.	1. Національні стандарти. 2. Міжнародні стандарти.			http://dl.dut.edu.ua/course/view.php?id=2021
	Лекція 3	Тема: Стандартизовані моделі та методи оцінки ефективності захисту інформації.	1. Модель, що покладена в основу міжнародного стандарту ISO 7498-2. 2. Модель, що покладена в основу НД ТЗІ 2.5. 3. Модель, що покладена в основу міжнародного стандарту ISO/IEC 15408.			http://dl.dut.edu.ua/course/view.php?id=2021
	Практичне заняття 1	Тема: Сервіси безпеки як основа підтримки політики безпеки		1. Пред’являти вимоги до ідентифікації/автентифікації. 2. Пред’являти вимоги до		http://dl.dut.edu.ua/course/view.php?id=2021

				розмежування доступу. 3. Пред'являти вимоги до протоколюванню й аудиту. 4. Пред'являти вимоги до екрануванню. 5. Пред'являти вимоги до тунелюванню. 6. Пред'являти вимоги до шифрування. 7. Пред'являти вимоги до контролю цілісності. 8. Пред'являти вимоги до контролю захищеності.		
	Практичне заняття 2	Тема: Стандартизовані моделі та методи оцінки ефективності захисту інформації.		1. Застосовувати модель, що покладена в основу міжнародного стандарту ISO 7498-2. 2. Застосовувати модель, що покладена в основу НД ТЗІ 2.5. 3. Застосовувати модель, що покладена в основу міжнародного стандарту ISO/IEC 15408.		http://dl.dut.edu.ua/course/view.php?id=2021
	Лабораторне заняття 1	Тема: Ознайомлення з СПЗ «Гриф-2006».	1. Основи СПЗ «Гриф-2006». 2. Основні функції СПЗ «Гриф-2006». 3. Правила роботи з СПЗ «Гриф-2006».			http://dl.dut.edu.ua/course/view.php?id=2021
	Лабораторне заняття 2, 3	Тема: Моделювання ІКС за допомогою СПЗ «Гриф-2006».		Моделювати вибраний варіант ІКС за допомогою СПЗ «Гриф-2006».		http://dl.dut.edu.ua/course/view.php?id=2021
	Лабораторне заняття 4	Тема: Встановлення зв'язків між елементами ІКС за допомогою СПЗ «Гриф-2006».		Встановлювати зв'язки між елементами ІКС за допомогою СПЗ «Гриф-2006».		http://dl.dut.edu.ua/course/view.php?id=2021

	Лабораторне заняття 5, 6	Тема: Введення технології обробки інформації в ІКС за допомогою СПЗ «Гриф-2006».		Вводити технології обробки інформації в ІКС за допомогою СПЗ «Гриф-2006».		http://dl.dut.edu.ua/course/view.php?id=2021
	Лабораторне заняття 7, 8	Тема: Введення розробленої політики безпеки ІКС за допомогою СПЗ «Гриф-2006».		Вводити розроблену політику безпеки ІКС за допомогою СПЗ «Гриф-2006».		http://dl.dut.edu.ua/course/view.php?id=2021
	Лабораторне заняття 9	Тема: Оцінка розробленої політики безпеки ІКС за допомогою СПЗ «Гриф-2006».		Проводити оцінку розробленої політики безпеки ІКС за допомогою СПЗ «Гриф-2006».		http://dl.dut.edu.ua/course/view.php?id=2021
	Самостійна робота	Тема 1 Технологія попереднього аудиту безпеки інформаційно-комунікаційної системи як передумова побудови політики безпеки. Тема 2 Основи аналізу і синтезу політик безпеки Тема 3 Розробка та реалізація політик безпеки Тема 4 Оцінка політики безпеки	1. Склад та характеристика існуючої системи захисту. 2. Основні показники політики безпеки. 3. Вимоги міжнародних стандартів. 4. Рівні захисту ресурсів.			http://dl.dut.edu.ua/course/view.php?id=2021

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. Бармен С. Разработка правил информационной безопасности. - М.: Издательский дом ‘‘Вильямс’’, 2012. - 208 с.
2. Безопасность информационных технологий. Курс БТ01. М.: Учебный центр ‘‘Информзащита’’, 2013. - 233 с.
3. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій - К.: ДУІКТ, 2010. - 508 с.

4. Богуш В.М., Довидьков О.А. Проектування захищених комп’ютерних систем та мереж, навчальний посібник, -К.; ДУІКТ, 2008. – 500 с.
5. Бурячок В.Л., Грищук Р.В., Хорошко В.О. Політика інформаційної безпеки, підручник, -К.; ПВП «Задруга», 2014. - 222 с.
6. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Изд-во агентства "Яхтсмен", 1996. - 192 с.
7. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
8. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. Чинний від 01.07.1997 р. - К.: Держстандарт України, 1997. - 7 с.
9. ДСТУ 2941-94. Системи оброблення інформації. Розроблення систем. Терміни та визначення. Чинний від 28.11.1994 р. - К.: Держстандарт України, 1994. - 19 с.
10. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.
11. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 04.12.2000 р. № 53.
12. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.
13. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.
14. НД ТЗІ 2.5-010-03. Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від від 02.04.2003 р. № 33.
15. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 20.12.2000 р. № 60.
16. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. Затверджено наказом ДСТЗІ СБ України від 28.04.1999 р. № 22.
17. НД ТЗІ 3.7-005-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Затверджено наказом ДСТЗІ СБ України від 08.11.2005 р. № 125.
18. Петренко С.А., Курбатов В.А. Политики информационной безопасности. - М.: Компания АйТи, 2006. - 400 с.
19. British Standard. Information security management systems - Specification with guidance for use. British Standard Institution, BS 7799- 2, 2002.
20. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 2.1. - CCIMB- 99- 031, August 1999.
21. Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements. Version 2.1. - CCIMB- 99- 032, August 1999.
22. Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. Version 2.1. - CCIMB- 99- 033, August 1999.
23. Common Methodology for Information Technology Security Evaluation. Part 2: Evaluation Methodology. Version 1.0. - CEM- 99/045, August 1999.
24. DoD 5200.28-STD, Department technology Security techniques Evaluation Criteria. December 1985. NY: U.S. Government printing office, 1999. 122 pp.

25. ISO/IEC 15408-1: Information technology. Security techniques - Evaluation criteria for IT security, Part 1: Introduction and general model, 1999.
26. ISO/IEC 15408-2: Information technology. Security techniques - Evaluation criteria for IT security, Part 2: Security functional requirements, 1999.
27. ISO/IEC 15408-3: Information technology. Security techniques - Evaluation criteria for IT security, Part 3: Security assuracce requirements, 1999. 28.
29. ISO/IEC 17799: Information technology - Code of practice for Information security management, 2000.
30. ISO/IEC 7498-2. Information processing systems Open Systems Interconnection Basic Reference Model. Part 2: Security Architecture. Switzeland, 1989. 32 pp.
31. Neumann P.G. Practical Architectures for survivable Systems and Networks. Technical Report. - SRI International: Computer Science Laboratory, 2001. - 209 pp. - http://www.csl.sri.com/neumann/survivability.dvi.
32. RFC 1244. Site Security Handbook.
33. Tanenbaum A.S. Computer Networks. - NY.: Prentice Hall, 1996.
34. Toward a secure system engineering methodology / C. Salter, O. Saydjari, B. Schneier, J. Wallner.

10. Методи оцінювання, підсумкові звітності за освітньою компонентою

(заліки, екзамени, курсові проекти, тестування)

екзамен

11. Матеріально-технічне забезпечення освітньої компоненти

Макет ПК.
Принтер HP.
Жорсткий диск SATA, PATA.
Digital security (Гриф-2006)