Інформаційний пакет освітніх компонент навчального плану
освітньо-наукової програми «Кібербезпека»
(назва)

Освітнього-наукового рівня «Доктор філософії»

Спеціальності 125 Кібербезпека

Галузь знань 12 Інформаційні технології

1. Назва освітньої компоненти Організація і проведення спеціальних досліджень на об'єктах інформаційної діяльності

(назва дисципліни)

2. Тип вибіркова

3. Обсяг:	Кредитів ECTS	Годин	За видами занять:				
			Лекцій	Семінар	Практичних занять	Лабораторних занять	Самостійна підготовка
	3	90	18	-	18		54
4. Взаємозв'язок у структурно-логічній схемі							
Освітні компоненти, які передують вивченню	1. Теорія захисту інформаційних ресурсів обмеженого доступу 2. Технологія створення та застосування комплексів захисту інформації з обмеженим доступом та охорони обєктів інформаційної діяльності						
Освітні компоненти для яких є базовою	1. Ліцензування, атестація та сертифікація у сфері безпеки обєктів інформаційної діяльності						
5. Компетенції відповідно до ОПП та вимог роботодавців:							
Компетенції відповідно до ОПП							
Знати			**Вміти**				
1. Правові основи захисту інформації та інформаційної безпеки;			1. Використовувати інформаційне поле в області захисту інформації, інформаційної безпеки при проведенні спеціальних досліджень на об'єктах інформаційної діяльності;				
2.Принципи організації спеціальних досліджень на об'єктах			2. Вміти використовувати технічні засоби захисту інформації під час				

інформаційної діяльності;	проведення спеціальних досліджень на об’єктах інформаційної діяльності;
3.Порядок проведення спеціальних досліджень на об’єктах інформаційної діяльності;	3. Використовувати отримані знання під час проектування та побудови захищених інформаційно-комунікаційних систем та систем захисту інформації від несанкціонованого витоку (розповсюдження) ;
4.Організаційні заходи та технічні засоби захисту інформації під час проведення спеціальних досліджень на об’єктах інформаційної діяльності.	4.Розробляти технічне завдання на створення комплексних систем захисту інформації.
Компетенції відповідно до вимог роботодавців	
1. Основні нормативні положення Законодавства України, нормативно-правові акти у галузі інформаційної безпеки.	1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника.
2. Вітчизняні та міжнародні нормативні, методичні документи з питань розробки та впровадження новітніх зразків засобів технічного захисту інформації.	2. Обґрунтувати необхідність проведення спеціальних досліджень на об’єктах інформаційної діяльності.
3. Стандарти, технічні умови та інші нормативні й керівні матеріали з проектування, розроблення й оформлення технологічної документації комплексних систем захисту інформації.	3. Оформити політику безпеки.
4.Методики проведення випробувань комплексних систем захисту інформації на відповідність вимогам вітчизняних та міжнародних нормативних документів.	4.Розробляти технічне завдання на проведення спеціальних досліджень на об’єктах інформаційної діяльності.
6. Результати навчання відповідно до ОПП	
1. Уміти використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об’єктів інформаційної діяльності, а також наукових досліджень вищих рівнів.	
2. Уміти розробляти та впроваджувати раціональні технології інформаційної безпеки, програми і методики випробувань систем інформаційної та кібербезпеки.	
3. Уміти проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та кібербезпеки об’єктів інформаційної діяльності.	
4. Уміти обґрунтовувати раціональні шляхи щодо захисту інформації на об’єктах інформаційної діяльності та інформації, що циклює в ІТ системах та мережах.	

7. План вивчення освітньої компоненти						
Змістовний розділ	Вид заняття	Тема	Знати	Вміти	План заняття	Лекція, методична розробка
Розділ 1						
	Лекція 1	Тема: Вступ до дисципліни Організація і проведення спеціальних досліджень на об'єктах інформаційної діяльності. Загальні положення.	1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Національні нормативні документи з технічного захисту інформації	1.Вміти проводити пошук необхідних норм, методик, інструкцій, положень, загальних вимог до систем захисту інформації.		
	Лекція 2	Тема: Класифікація закладних пристроїв та їх де маскувальні ознаки.	1.Демаскуючі ознаки закладних пристроїв. 2. Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам вітчизняних та міжнародних стандартів.	1.Виявляти закладні пристрої. 2. Практичного застосування системи захисту інформації для проведення спеціальних досліджень на об'єктах інформаційної діяльності.		
	Лекція 3	Тема: Технічні засоби пошуку закладних пристроїв, та інших засобів негласного отримання інформації.	1.Спеціальні пошукові пристрої. 2. Фізичні принципи роботи спеціальних пошукових пристроїв.	1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника. 2. Працювати з спеціальними приладами пошуку сигналів несанкціонованого знімання інформації.		
	Лекція 4	Тема: Склад і послідовність робіт з підготовки та проведення комплексних спеціальних перевірок приміщень та	1. Порядок створення, структуру служби захисту інформації. 2. Завдання, функції та повноваження служби	1.Розробляти план робіт з спеціальних досліджень об'єктів інформаційної діяльності та інших питань;		

		програмних комплексів.	захисту інформації. 3. Порядок Оформлення політики безпеки; 4. Порядок розробки Моделі загроз і Моделі порушника.	Визначати: 1. Перелік об'єктів захисту. 2. Потенційні загрози для інформації. Розробляти: 3. Модель загроз. 4. Модель порушника.		
	Лекція 5	Тема: Методики виконання робіт на підготовчому етапі та на етапі безпосередньої комплексної перевірки.	1.Правові основи захисту інформації 2. Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам вітчизняних та міжнародних стандартів.	Формувати загальні вимоги до проведення спеціальних досліджень на об'єктах інформаційної діяльності. Формувати завдання на проведення спеціальних досліджень на об'єктах інформаційної діяльності.		
	Лекція 6	Тема: Пощук закладних пристроїв за видами каналів передачі інформації.	1.Фізичні принципи демаскування закладних пристроїв. 2. Методики виявлення джерел акустичних і відеоінформаційних закладних пристроїв на об'єктах інформаційної діяльності..	1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника. 2. Використовувати інформаційне поле в області захисту інформації, інформаційної безпеки при проведенні спеціальних досліджень на об'єктах інформаційної діяльності;		
	Лекція 7	Дослідження приміщень на наявність акустичного та віброакустичного каналів витоку інформації.	1.Фізичні принципи демаскування закладних пристроїв, які здійснюють несанкціоноване зняття інформації через акустичні і віброакустичні канали. 2. Методики виявлення	1.Здійснювати відео спостереження. 2. Виявляти та локалізувати засоби несанкціонованого зняття інформації акустичними і віброакустичними		

			джерел акустичних і віброакустичних закладних пристроїв на об’єктах інформаційної діяльності..	каналами.		
	Лекція 8	Візуальний огляд і пошук закладних пристроїв	1.Демаскуючі ознаки закладних пристроїв. 2. Фізичні принципи роботи спеціальних пошукових приладів..	1.Виявляти закладні пристрої. 2. Здійснювати зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам вітчизняних та міжнародних стандартів.		
	Лекція 9	Методика виконання робіт на завершеному етапі комплексної перевірки приміщень та програмних комплексів	Порядок розробки політики безпеки інформації на об’єктах інформаційної діяльності.	Розробляти Політику безпеки інформації на об’єктах інформаційної діяльності.		
	Практичне заняття 1	Тема: Підготовка плану проведення спеціальних досліджень на об’єктах інформаційної діяльності..	1.Правові основи захисту інформації 2. Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам вітчизняних та міжнародних стандартів.	Вміти проводити пошук необхідних норм, методик, інструкцій, положень, загальних вимог до систем захисту інформації.		
	Практичне заняття 2	Тема: Методика пошуку закладних пристроїв з використанням пошукового програмно-апаратного комплексу ПАК DigiScan.	1.Кореляційні функції, амплітудні і спектральні характеристики сигналів. 2.Призначення і принцип роботи пошукового програмно-апаратного комплексу ПАК DigiScan.	1.Виявляти радіосигнали з закладних пристроїв. 2. Визначати частоти, полоси пропускання радіосигналів з закладних пристроїв.		

	Практичне заняття 3	Тема: Методика пошуку закладних пристроїв з використанням пошукового пристрою ST 031 “Піранья».	Призначення і принцип роботи багатофункціонального пошукового приладу ST 031 “Піранья».	1.Проводити заходи щодо виявлення і локалізації спеціальних технічних засобів негласного зняття інформації. 2. Виявляти істотні і штучно створенні канали витоку інформації. 3. Здійснювати контроль якості захисту інформації.		
	Практичне заняття 4	Тема: Методика пошуку закладних пристроїв з використанням нелінійного локатору NR-900EM.	Призначення і принцип роботи нелінійного локатору ТК900ЕМ.	1.Здійснювати пошук довільних видів радіо мікрофонів, в тому числі з дистанційним керуванням. 2.Здійснювати пошук мікрофонних підсилювачів провідних мікрофонів. 3. Здійснювати пошук засобів негласного зняття інформації інфрачервоного і ультразвукового діапазонів та засобів звукозапису.		
	Практичне заняття 5	Тема: Методика пошуку закладних пристроїв з використанням індикатора поля PROTECT 1203.	Призначення і принцип роботи індикатора поля PROTECT 1203.	1.Здійснювати пошук засобів негласного зняття інформації, які знаходяться в активному режимі і використовують в якості каналу передачі інформації електромагнітне випромінювання.		
	Практичне заняття 6	Тема: Виявлення демаскуючих ознак закладних пристроїв .	1.Фізику електромагнітних полів радіочастотного каналу передачі. 2.Фізику електромагнітного	1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника.		

			випромінювання низької частоти з магнітною складовою. 2.Класифікацію демаскуючих закладних пристроїв, види пошукового устаткування та види виявлення закладних пристроїв.	2. Використовувати інформаційне поле в області захисту інформації, інформаційної безпеки при проведенні спеціальних досліджень на об'єктах інформаційної діяльності;		
	Практичне заняття 7	Тема: Виявлення демаскуючих ознак закладних пристроїв .	1.Фізику інфрачервоного випромінювання. 2.Класифікацію демаскуючих закладних пристроїв, види пошукового устаткування та види виявлення закладних пристроїв.	1. Аналізувати потенційні загрози для інформації, модель загроз та модель порушника. 2. Використовувати інформаційне поле в області захисту інформації, інформаційної безпеки при проведенні спеціальних досліджень на об'єктах інформаційної діяльності;		
	Практичне заняття 8	Тема: Підготовка акту проведення спеціальних досліджень на об'єктах інформаційної діяльності.	1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Національні нормативні документи з технічного захисту інформації	1.Складати акт здійснення спеціальних досліджень на об'єктах інформаційної діяльності.		
	Практичне заняття 9	Тема: Створення рекомендацій по підвищенню захищеності перевірених об'єктів інформаційної діяльності.	1. Загальні положення та вимоги в частині організації робіт із захисту інформації 2. Національні нормативні документи з технічного захисту інформації. 3. Перелік технічних засобів і систем захисту інформації,	1.Виявляти потенційні технічні канали витоку інформації. 2.Оцінювати ймовірність використання противником потенційних технічних каналів витоку інформації та захищеність об'єктів		

			які підвищують захист об'єктів інформаційної діяльності.	інформаційної діяльності.		
	Самостійна робота	**Тема 1** Технології розпізнавання аналогових сигналів негласного отримання інформації. **Тема 2** Технології розпізнавання цифрових сигналів негласного отримання інформації.	1.Характеристики аналогових сигналів. 2.Алгоритми перетворення аналогових сигналів в цифрові. 2.Принципи дії приладів розпізнавання сигналів негласного зняття інформації в зоні легального радіоефіру.	1.Виявляти потенційні технічні канали витоку інформації. 2.Оцінювати ймовірність використання противником потенційних технічних каналів витоку інформації та захищеність об'єктів інформаційної діяльності.		
Розділ 2						
	…	…				
Розділ …						
	…	…				

8. Мова вивчення освітньої компоненти

(українська, англійська, розділи, що викладаються англійською мовою)

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.Доктрина інформаційної безпеки України, затверджена указом Президента України 25 лютого 2017 року №47/2017;
2.Закон України «Про інформацію»;
3.Закон України «Про доступ до публічної інформації»;
4.Закон України «Про захист персональних даних»;
5.Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;
6.Закон України «Про захист інформації в автоматизованих системах»;
7.Постанова Кабінету Міністрів України "Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах" від 29.03.2006 № 373.
8. НД ТЗІ 2.6-003-2015- Порядок зіставлення компонентів довіри до безпеки, визначених ISO/IEC 15408, з вимогами НД ТЗІ 2.5-004-99.
9. НД ТЗІ 2.7-013-2016- Методичні вказівки з виконання зіставлення результатів оцінювання засобів захисту інформації від несанкціонованого доступу на відповідність вимогам ISO/IEC 15408 з вимогами НД ТЗІ 2.5-004-99.

10. НД ТЗІ Р-001-2000 Засоби активного захисту мовної інформації з акустичними та віброакустичним джерелами випромінювання. Класифікація та загальні технічні вимоги. Рекомендації.
11. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.5-001-2000 "Радіовиявлювачі. Класифікація. Загальні технічні вимоги".
12. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-001-2001 "Радіовиявлювачі вимірювальні. Методи та засоби випробувань".
13. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-004-2001 "Радіовиявлювачі індикаторні. Методи та засоби випробувань".
14. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-005-2001 "Радіовиявлювачі панорамні. Методи та засоби випробувань".
15.Нормативний документ системи технічного захисту інформації НД ТЗІ 2.3-006-2001 "Радіовиявлювачі аналізувальні. Методи та засоби випробувань".
16. Нормативний документ системи технічного захисту інформації НД ТЗІ 1.4-002-08 "Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань".
17. Нормативний документ системи технічного захисту інформації НД ТЗІ 2.7-011-2012 "Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв".
18.Бурячок В.Л. Грищук Р.В.,Хорошко В.О. Політика інформаційної безпеки: підручник за заг. ред. д.т.н., проф. Хорошка В.О. К.: ПВП «Задруга». 2014. 222 с.
19. Кривцун А.В.Использование новых возможностей комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу [Электронный ресурс] /А.В. Кривцун А.В.Захаров режим доступа: http://www.inspectorsoft.ru/article.php?id=388 (24.05.2019).
20. Максименко Г. А., Хорошко В. А. Методы выявления, обработки и идентификации сигналов радиозакладных устройств. К: ПолиграфКонсалтинг. 2004. 317 с.
21. Патент UA 86600 Пристрій пошуку закладного пристрою за допомогою акустичної локації кл. G 01 S 7/52, 15/10 бюл. №1 опубл. 10.01.2014.
22. Патент на корисну модель 108734 Україна, H 04 B 7/165. Пристрій для вимірювання відношення сигнал/шум в приймальних комплексах адаптивного 140 мобільного радіозв'язку / Сайко В.Г., Наритник Т.М., Грищенко М.М., Бреславський В.О., Лисенко Д.Р., Дакова Л.В. Заявник і патентовласник Державній університет телекомунікацій; заявл.17.02.2016; опубл. 25.07.2016 // Бюл. № 14. 76.
23. Поисковые комплексы . [Электронный ресурс]. https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (03.05.2019).
24. Поисковые комплексы . [Электронный ресурс]. https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (03.05.2019).
25. Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб, затверджене наказом ДСТСЗІ СБУ від 22.02.2002 № 9, зареєстроване Міністерством юстиції України 13.03.2002 за № 245/6533.
26. Постанова Кабінету Міністрів України від 08 жовтня 1997 року № 1126 "Про затвердження Концепції технічного захисту інформації в Україні".

27. Постанова Кабінету Міністрів України від 14 травня 2015 р. № 295 «Про внесення змін до Плану використання радіочастотного ресурсу України».
28. Хорев А.А. Защита информации от утечки по техническим каналам. Технические каналы утечки информации: учебное пособие /– М.: Гостехкомиссия России. 1998. 320 с.
29. Хорев А.А.Техническая защита информации: учебное пособие для студентов вузов. В 3 т. Т. 1./ Технические каналы утечки информации. - М: «НПЦ Аналитика», 2008. 436 с.
30. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации / Ковтанюк Ю. С., ред. К: Юниор. 2003. 502 с.
31. Цифровой пеленгатор "Rohde & Schwarz DDF0xE" / Техника для спец служб, бюро научно-технической информации, основано в 1999 году. [Электронный ресурс] режим доступа:http://www.bnti.ru/des.asp?itm=4446&tbl =04.01.01.01.01. (24.05.2019).

10. Методи оцінювання, підсумкові звітності за освітньою компонентою

(заліки, екзамени, курсові проекти, тестування)

Залік

11. Матеріально-технічне забезпечення освітньої компоненти

1. комп'ютери ITS 5400 - 17 шт. (2014 р.)
2. мультимедійна система Acer 113 -1

3. **Обладнання:** 4. відеокамери (DS-2CD1331-I, DS-2CD2125F-I , DS-2CD2420F-I, DS-2CD1021-I, DS-2CD4A26FWD-IZS/P, DS-7608NI-E2/8P); 5. генератор шуму "KVS-3000"; 6. детектор відеокамер "KVS-D"; 7. оглядовий комплект дзеркал «Огляд-1»; 8. портативний скануючий приймач AR 8200; 9. пошукова система DigiSkan EX; 10. скануючі приймачі IC-R2500, IC-R20; 11. багатофункціональний пошуковий прилад ST-032; 12. портативний цифровий детектор PROTECT-1206i; 13. персональний детектор поля PROTECT-1210; 14.Локатор нелінійностей NR-900 EM.

Інформаційний пакет освітньої компоненти, яка викладається англійською мовою, додатково розміщується на сторінці кафедри на англійській мові