НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ ІМЕНІ Б.ХМЕЛЬНИЦЬКОГО

Кафедра зв'язку, автоматизації та кібербезпеки інженерно-технічного факультету

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«ЗАХИСТ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ»
ОПП «Телекомунікації та радіотехніка»

Рівень вищої освіти: перший (бакалаврський)
Галузь знань: 17 Електроніка та телекомунікації
Спеціальність: 172 Телекомунікації та радіотехніка
Форма навчання: денна

Розглянуто та схвалено на засіданні кафедри
Протокол від «29» червня 2019 року № 16

Начальник кафедри
зв'язку, автоматизації та кібербезпеки
полковник Михайло СТРЕЛЬБІЦЬКИЙ
(військове звання, підпис, ім'я та прізвище)
«29» червня 2019 року

АНОТАЦІЯ КУРСУ

Навчальна дисципліна «Захист інформації в телекомунікаційних системах та мережах», є обов'язковою для вивчення ОПП «Телекомунікації та радіотехніка». Вивчається протягом 8-го семестру на кафедрі Зв'язку, автоматизації та кібербезпеки.

Метою вивчення навчальної дисципліни є підготовка офіцера, який має отримати знання і вміння, необхідні для впровадження в оперативно-службову діяльність підрозділів охорони кордону засобів зв'язку пов'язаних із боротьбою з комп'ютерною злочинністю, та навчити їх застосуванню методів та засобів захисту інформації у сучасних інформаційних системах та мережах і лініях телекомунікаційного зв'язку в умовах широкого використання сучасних інформаційних технологій, що стоять на озброєнні Державної прикордонної служби України.

Основне завдання навчальної дисципліни – формування у курсантів системних знань щодо правильного експлуатування засобів зв'язку та автоматизації з дотриманням вимог кібернетичної безпеки, які безпосередньо використовуються при здійснені оперативно-службової діяльності прикордонних підрозділів.

Курсант, який успішно завершив вивчення дисципліни, повинен:

знати: правову та організаційну основи забезпечення інформаційної безпеки у комп'ютерних системах і мережах, системах телекомунікаційного зв'язку та, зокрема, у системах та мережах, що використовуються у Державній прикордонній службі України; основні види загроз інформаційній безпеці в інформаційних системах і мережах та телекомунікацій-них каналах зв'язку, технічні канали витоку інформації з них, методи виявлення та блокування цих каналів; основні види та можливості технічних та програмних методів та засобів захисту, зокрема, криптографічних і стеганографічних систем захисту інформації.

вміти: планувати та організовувати свою роботу та роботу підрозділу з урахуванням вимог до захисту інформації з обмеженим доступом; планувати й організовувати роботи щодо створення та розвитку системи інформаційної безпеки у комп'ютерних системах та мережах; здійснювати ефективний вибір комп'ютерних систем захисту; використовувати комп'ютерні криптографічні, стеганографічні системи, антивірусні засоби.

ознайомитись: з сучасними засобами захисту інформації; з перспективами розвитку телекомунікаційних систем та мереж Державної прикордонної служби України та місцем систем криптографічного захисту інформації в побудові таких мереж.

ВИКЛАДАЧІ:

Начальник (завідувач) кафедри зв'язку, автоматизації та кібербезпеки доктор технічних наук, доцент Михайло СТРЕЛЬБІЦЬКИЙ.

Доцент кафедри зв'язку, автоматизації та кібербезпеки кандидат технічних наук Олександр БАСАРАБ.

ПЕРЕДУМОВИ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.

Комутація та системи абонентського доступу, Системи мобільного зв'язку, Метрологія, Стандартизація та сертифікація.

МАТЕРІАЛЬНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.

Комп'ютерні спеціалізовані класи (216, 314, 320, 324), Детектори прихованих камер, Цифрові ендоскопи, Тепловізори, Детектори поля, Пошукові прилади, Пошукові системи, Нелінійні локатори.

Програмне забезпечення: Операційні системи, Спеціальне програмне забезпечення пошукових систем.

ТРИВАЛІСТЬ ТА ОРГАНІЗАЦІЯ КУРСУ

Курс	Семестр	Кількість кредитів ECTS	Кількість годин																				Форми підсумкового контролю		
			Загальна	Усього аудиторних занять	Аудиторна робота										Індивідуальна робота								Самостійна робота	Екзамен	Диференційований залік	Залік
					лекції	групові заняття	групові вправи	практичні заняття	лабораторні заняття	семінари	рольові ігри	контрольна робота	індивідуальні заняття	модульний контроль	підсумковий контроль	Усього	реферат	конспект з теми	переклад текстів	розрахункове завдання	курсова робота	контрольна робота	модульний контроль				
4	**8**	**5**	**150**	**76**	16	18		18	20					4		74						38		36		+	
Всього		**5**	**150**	**76**	**16**	**18**		**18**	**20**					**4**		**74**						**38**		**36**		**+**	

Основні методи навчання: МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.

Основні методи контролю навчальних досягнень: МК1.1; МК2.1; МК2.4; МК2.5; МК2.6; МК3.1; МК3.2; МК4.1; МК4.2; МК4.3.

КОМПЕТЕНТНОСТІ ТА КОНТРОЛЬ РІВНЯ ЇХ ДОСЯГНЕННЯ КУРСАНТАМИ

Шифр	Компетентність	Методи контролю
Загальні компетентності		
ЗК-2	Здатність застосовувати знання у практичних ситуаціях.	МК2.1; МК2.5; МК2.6; МК3.1; МК3.2; МК4.1; МК4.2; МК4.3.
ЗК-4	Знання та розуміння предметної області, розуміння професійної діяльності	МК1.1; МК1.4; МК2.3; МК2.4; МК2.5; МК2.6; МК2.7; МК3.2; МК3.3; МК4.1.
ЗК-8	Вміння виявляти, ставити та вирішувати проблеми.	МК1.1; МК2.1; МК2.4; МК2.6
Фахові компетентності спеціальності		
ФК-1	Здатність розуміти сутність і значення інформації в розвитку сучасного інформаційного суспільства.	МК1.1; МК1.3; МК2.1; МК2.4; МК2.5; МК2.6; МК3.2; МК3.3.
ФК-2	Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки.	МК1.1; МК1.4; МК2.3; МК2.4; МК2.5; МК2.6; МК2.7; МК3.2; МК3.3; МК4.1.
ФК-5	Здатність використовувати нормативну та правову документацію, що стосується інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем (закони України, технічні регламенти, міжнародні та національні стандарти, рекомендації Міжнародного союзу електрозв'язку і т.п.) для вирішення професійних завдань	МК2.5; МК2.6; МК2.7; МК3.3; МК4.4.
ФК-6	Здатність проводити інструментальні вимірювання в інформаційно-телекомунікаційних мережах, телекомунікаційних та радіотехнічних системах.	МК2.5; МК4.4.
ФК-8	Готовність сприяти впровадженню перспективних технологій і стандартів	МК1.1; МК2.1; МК2.4; МК3.2.
ФК-9	Здатність здійснювати приймання та освоєння нового обладнання відповідно до чинних нормативів.	МК2.5; МК2.6; МК2.7; МК3.3; МК4.4.
ФК-10	Здатність здійснювати монтаж, налагодження, налаштування, регулювання, дослідну перевірку працездатності, випробування та здачу в експлуатацію споруд, засобів і устаткування телекомунікацій та радіотехніки.	МК2.5; МК2.6; МК2.7; МК3.3; МК4.4.
ФК-11	Здатність складати нормативну документацію (інструкції) з експлуатаційно-технічного обслуговування інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем, а також за програмами випробувань.	МК2.1; МК2.4; МК2.5; МК2.6; МК3.2; МК3.3.
ФК-12	Здатність проводити роботи з керування потоками навантаження інформаційно-телекомунікаційних мереж.	МК1.1; МК1.3; МК2.1; МК2.4; МК2.5; МК2.6; МК3.2; МК3.3; МК4.4.

Шифр	Компетентність	Методи контролю
ФК-15	Здатність проводити розрахунки у процесі проектування споруд і засобів інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем, відповідно до технічного завдання з використанням як стандартних, так і самостійно створених методів, прийомів і програмних засобів автоматизації проектування.	МК1.4; МК2.6; МК2.7; МК3.3; МК4.4.

ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ, МЕТОДИ НАВЧАННЯ ТА КОНТРОЛЬ РІВНЯ ЇХ ДОСЯГНЕННЯ КУРСАНТАМИ

Шифр	Компетентність	Методи навчання	Оцінювання
ПРН-2	Застосовувати результати особистого пошуку та аналізу інформації для розв'язання якісних і кількісних задач подібного характеру в інформаційно-комунікаційних мережах, телекомунікаційних і радіотехнічних системах.	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	МК1.1; МК1.3; МК2.1; МК2.4; МК2.5; МК2.6; МК3.2; МК3.3; МК4.4.
ПРН-3	Визначати та застосовувати у професійній діяльності методики випробувань інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем на відповідність вимогам вітчизняних та міжнародних нормативних документів.	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	МК1.1; МК1.3; МК2.1; МК2.4; МК2.5; МК2.6; МК3.2; МК3.3; МК4.4.
ПРН-4	Пояснювати результати, отримані в результаті проведення вимірювань, в термінах їх значущості та пов'язувати їх з відповідною теорією.	МН1.1; МН1.3; МН2.2; МН3.1; МН3.2; МН3.5; МН4.2; МН4.4	МК1.2; МК1.4; МК2.2; МК2.3; МК2.5; МК2.6; МК2.7; МК3.3;МК4.1; МК4.4.
ПРН-5	Навички оцінювання, інтерпретації та синтезу інформації і даних.	МН1.3; МН 1.6; МН 2.1; МН2.3; МН3.2; МН3.4; МН3.6; МН3.7; МН4.1; МН4.2; МН4.4	МК1.4; МК2.2; МК2.7; МК2.8; МК3.3; МК4.1; МК4.4.
ПРН-6	Адаптуватись в умовах зміни технологій інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем.	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	МК2.1; МК2.3; МК2.5; МК2.6; МК3.1; МК4.1; МК4.4.
ПРН-9	Аналізувати та виконувати оцінку ефективності методів проектування інформаційно-	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3;	МК2.6; МК2.7; МК3.1; МК3.3; МК4.4.

Шифр	Компетентність	Методи навчання	Оцінювання
	телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем.	МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	
ПРН-17	Розуміння та дотримання вітчизняних і міжнародних нормативних документів з питань розроблення, впровадження та технічної експлуатації інформаційно-телекомунікаційних мереж, телекомунікаційних і радіотехнічних систем.	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	МК1.2; МК2.3; МК2.4; МК2.5; МК2.7; МК3.2;МК3.3; МК4.4.
ПРН-19	Здійснювати стандартні випробування інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем на відповідність вимогам вітчизняних та міжнародних нормативних документів	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	МК2.5; МК2.6; МК2.7; МК3.2; МК4.3.
ПРН-22	Контролювати технічний стан інформаційно-комунікаційних мереж, телекомунікаційних і радіотехнічних систем у процесі їх технічної експлуатації з метою виявлення погіршення якості функціонування чи відмов, та його систематична фіксація шляхом документування.	МН1.1; МН1.2; МН1.3; МН1.5; МН2.1; МН2.3; МН3.1; МН3.2; МН3.6; МН4.1; МН4.2.	МК1.2; МК2.3; МК2.4; МК2.5; МК2.7; МК3.2;МК3.3; МК4.4.

ОРГАНІЗАЦІЯ НАВЧАННЯ

№ теми	Найменування теми	Кількість годин	Номери, вид занять та кількість годин								Місяць	Номери тем, занять та кількість годин	Кількість годин
			1	2	3	4	5	6	7	8			
1	Основи кібернетичної безпеки.	12	Л2	Л2	Л2	Л2	Л2	Гз2			01	1/1Л(2), 1/2Л(2), 1/3Л(2), 1/4Л(2), 1/5Л(2), 1/6Гз(2).	12
2	Технічний та програмний захист інформації в телекомунікаційних системах. **Модульний контроль № 1.**	22	Л2	Гз2	Лр2	Лр4	Пз2	Пз2	Лр4	Пз4 (Мк)	02/03	2/1 Л(2); 2/2 Гз(2); 2/3 Лр (2); 2/4 Лр(4); 2/5 Пз (2); 2/6 Пз (2); 2/7 Лр (4); 2/8 Пз (4).	22
3	Криптографічні методи захисту інформації.	22	Л2	Гз2	Гз2	Гз2	Пз4	Лр6	Лр4		03/04	3/1 Л(2); 3/2 Гз(2); 3/3 Гз(2); 3/4 Гз(2); 3/5 Пз(4); 3/6 Лр(6); 3/7 Лр(4);	22
4	Комплексні системи захисту інформації ДПСУ. **Модульний контроль № 2.**	16	Л2	Гз2	Гз2	Пз2	Пз4 (Мк)	Гз2	Гз2		05	4/1 Л(2); 4/2 Гз(2); 4/3 Гз(2); 4/4 Пз(2); 4/5 Пз(4); 4/6 Гз(2); 4/7 Гз(2);	16
Диференційований залік		4	Дз4								05	Дз (4)	4
Всього		**76**									**Всього**		**76**

Умовні скорочення:

Лекція - Л
Практичне заняття - Пз
Групове заняття – Гз
Лабораторна робота – Лр
Модульний контроль - Мк
Диференційований залік - Дз
Заняття, що обов’язкове для оцінювання - 2/3Лр(2)

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
IV курс					
8 семестр					
1			**37**	**Основи кібернетичної безпеки**	
	1	Лекція	2	***Основні засади забезпечення кібербезпеки України*** 1. Понятійний апарат у галузі кібербезпеки. 2. Стратегічні аспекти кібербезпеки України. 3. Проблеми формування національної системи кібернетичної безпеки.	[1.1-1.3, 1.20]
	2	Лекція	2	***Національна система кібербезпеки, її структура та функціонування*** 1. Об'єкти кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки. 2. Об'єкти критичної інфраструктури. 3. Структура системи кібербезпеки.	[1.1-1.3, 1.20]
	3	Лекція	2	***Кіберпростір, кібербезпека та кібертероризм: поняття і визначення*** 1. Заходи України із забезпечення кібербезпеки національної інфосфери 2. Інциденти у сфері високих технологій: характерні ознаки та проблемні аспекти. 3. Кібератаки та кібертероризм: поняття і визначення.	[1.1-1.3, 1.20]
		Самостійна робота	2	1. Інформація, її види та властивості. 2. Інформаційні системи як об'єкти захисту.	[1.3-1.7], [2.1]
		Самостійна робота	2	1. Співвідношення інформаційної технології та інформаційної системи. 2. Класифікація та види інформаційних технологій.	[1.3-1.7], [2.1]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
	4	Лекція	2	***Інформаційні технології та проблеми їхньої безпеки*** 1. Визначення інформаційної технології. 2. Співвідношення інформаційної технології та інформаційної системи. 3. Класифікація та види інформаційних технологій. 4. Основні проблеми безпеки інформаційних технологій.	[1.7], [2.2, 2.3]
		Самостійна робота	2	1. Збитки як категорія класифікації загроз. 2. Класифікація загроз безпеці інформації. 3. Класифікація джерел загроз.	[1.7], [2.2, 2.3]
		Самостійна робота	2	1. Ранжирування джерел загроз. 2. Класифікація уразливостей безпеці. 3. Ранжирування уразливостей. 4. Класифікація актуальних загроз.	[1.7], [2.2, 2.3]
	5	Лекція	2	***Основи безпеки інформаційних ресурсів*** 1. Загрози безпеці інформації та інформаційних ресурсів. 2. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.	[1.8-1.19], [2.1]
		Самостійна робота	2	1. Архітектура відкритих систем. 2. Загрози в архітектурі відкритих мереж. 3. Процедури захисту. 4. Сервісні служби захисту. 5. Реалізація захисту.	[1.8-1.19], [2.1]
	6	Групове заняття	2	***Критерії безпеки інформаційних технологій*** 1. Загальні відомості про вимоги та критерії оцінки безпеки інформаційних технологій. 2. Функціональні вимоги до засобів захисту. 3. Вимоги гарантій засобів захисту.	[1.8-1.19], [2.1]
		Самостійна робота	2	1. Нормативно-правове забезпечення захисту державних інформаційних ресурсів. 2. Концептуальних аналіз уразливості державних інформаційних ресурсів. 3. Правові аспекти формування системи державних інформаційних ресурсів.	[1.1, 1.2] [2.1, 2.3, 2.4]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
		Індивідуальне завдання	13	Виконання вибіркового дослідницького завдання за заданою тематикою	[1.1-1.20], [2.1-2.7],[3.1-3.4]
2			**34**	**Технічний та програмний захист інформації в телекомунікаційних системах**	
	1	Лекція	2	***Сучасний стан безпеки інформації.*** 1. Призначення стандартів інформаційної безпеки. 2. Основні керівні документи з питань захисту інформації, їх зміст. 3. Технічні канали витоку інформації. Загрози безпеки для інформаційно-телекомунікаційних систем	[1.17-1.20] [2.8-2.15] [3.10-3.11]
		Самостійна робота	2	1. Класифікація комп'ютерних вірусів. 2. Технології виявлення комп'ютерних вірусів. 3. Засоби антивірусного захисту інформації у телекомунікаційних мережах.	[1.17-1.18] [2.20-2.24] [3.5-3.13]
	2	Групове заняття	2	***Особливості захисту інформації в телекомунікаційних системах*** 1. Мережні або віддалені атаки. Типові атаки на розподілені системи. 2. Причини уразливості розподілених систем. 3. Сервіси безпеки. Специфічні механізми безпеки.	[1.11-1.18] [2.5-2.14] [3.1-3.10]
		Самостійна робота	2	Методи захисту від побічних електромагнітних випромінювань і наведень в кабельних комунікаціях об'єктів зв'язку та інформатизації.	[1.9-1.16] [2.20-2.24] [3.5-3.12]
	3	Лабораторна робота СК ПТК	2	***Дослідження технічних каналів витоку інформації*** 1. Визначення технічних каналів витоку інформації з систем автоматизованої обробки інформації та телекомунікаційних мереж. 2. Визначення способів використання технічних каналів витоку для зняття інформації з систем автоматизованої обробки інформації та телекомунікаційних мереж. 3. Визначення методів та засобів блокування каналів високочастотного нав'язування.	[1.14-1.17] [2.13-2.17] [3.10-3.13]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
		Самостійна робота	2	1. Протидія технічним розвідкам. Загальні положення. 2. Основні демаскуючі ознаки військової техніки зв'язку. 3. Рекомендації щодо покращення ефективності протидії технічним розвідкам (маскування) вузлів зв'язку.	[1.15-1.20] [2.16-2.24] [3.13-3.14]
	4	Лабораторна робота СК ПТК	4	***Методи та засоби блокування витоку інформації*** 1. Визначення шляхів витоку інформації з каналів паразитних випромінювань та наводок. 2. Дослідження способів блокування витоку інформації з каналів паразитних випромінювань та наводок.	[1.14-1.20] [2.18-2.24] [3.13-3.15]
	5	Практична робота СК ПТК	2	***Формування політики облікових записів ОС WINDOWS*** 1. Налаштовування прав доступу користувачів до каталогів та файлів 2. Налаштовування сервісів операційної систеи 3. Налаштовування файлу завантаження операційної системи.	[1.9-1.16] [2.20-2.24] [3.5-3.12]
		Самостійна робота	2	1. Методи розмежування доступу. 2. Програмні засоби розмежування доступу до інформації. 3. Правила використання паролів. 4. Операційна безпека. 5. Програмна верифікація.	[1.14-1.17] [2.13-2.17] [3.10-3.13]
	6	Практична робота СК ПТК	2	***Захист автоматизованого робочого місця засобами реєстру операційної системи Windows*** 1. Конфігурування параметрів автентифікації 2. Налаштування переліку дозволених дій користувачеві 3. Конфігурування пунктів меню та окремих дозволів користувача	[1.15-1.20] [2.16-2.24] [3.13-3.14]
	7	Лабораторна робота СК ПТК	4	***Дослідження уразливостей телекомунікаційної системи*** 1. Дослідження вразливостей телекомунікаційної системи штатними засобами операційної системи 2. Дослідження вразливостей телекомунікаційної системи програмними засобами 3. Перехоплення мережевого обміну.	[1.14-1.20] [2.18-2.24] [3.13-3.15]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
		Самостійна робота	2	1. Роль, значення і стан захисту інформації в сучасному світі. 2. Основні види загроз конфіденційної інформації. 3. Основні міри, способи та засоби захисту інформації в ПК.	[1.17-1.20] [2.8-2.15] [3.10-3.11]
	8	Практичне заняття СК ПТК	4	***Захист телекомунікаційної системи засобами операційної системи*** 1. Визначення уразливостей телекомунікаційної системи 2. Налаштування міжмережевого екрану 3. Оцінювання рівня захищеності телекомунікаційної системи	[1.17-1.18] [2.20-2.24] [3.5-3.13]
Модульний контроль № 1					
		Самостійна робота	2	1. Апаратні методи та засоби розмежування доступу: можливості та межі застосування. 2. Голосовий ключ – метод ідентифікації людини за голосом при розмежуванні доступу. Основні недоліки голосових ключів. Тенденції розвитку. 3. Апаратні ключі – основа апаратно-програмного захисту інформації. 4. Біометрична інформація як джерело ідентифікаційних ознак особи. 5. Переваги та вади апаратно-програмних методів розмежування доступу до інформації.	[1.10, 1.14-1.20] [2.13-2.24] [3.8-3.11, 3,14]
3			**32**	**Криптографічні методи захисту інформації**	
	1	Лекція	2	***Основи криптографічного захисту інформації*** 1. Завдання криптографічного захисту інформації. 2. Основи класичної криптографії та крипто аналізу та їх історичний розвиток. 3. Процес механізації та автоматизації криптографії та крипто аналітики.	[2.10, 2.15-2.24]
	2	Групове заняття	2	***Основи криптографії*** 1. Поняття криптографії та крипто аналітики. 2. Поняття шифру та коду. Код Навахо.	[2.10, 2.15-2.24]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
		Самостійна робота	2	1. Національні та міжнародні стандарти криптографічного захисту інформації. 2. Криптографічна стійкість.	[2.10, 2.15-2.17]
	3	Групове заняття	2	***Методи шифрування інформації*** 1. Абсолютно стійке шифрування. Метод разового шифроблокноту. Основні положення теорії К. Шеннона. 2. Сучасні методи шифрування. Симетричні методи шифрування. Алгоритм шифрування DES. 3. Асиметричні методи шифрування. Основи модульної арифметики. Алгоритм шифрування з відкритим ключем RSA.	[2.10, 2.15]
		Самостійна робота	2	***Алгоритми з відкритими ключами*** 1. Алгоритм рюкзака. 2. Алгоритм RSA. 3. Алгоритм ROHLIGE–HELLMAN. 4. Алгоритм RABIN. 5. Алгоритм ElGAMAL. 6. Алгоритм McELIECE. 7. Алгоритм LUC. 8. Криптосистеми на базі кінцевих автоматів.	[2.17, 2.18]
		Самостійна робота	2	***Види засобів криптографічного захисту інформації*** 1. Апаратні засоби. 2. Програмні засоби 3. Програмно-апаратні комплекси.	[2.20]
	4	Групове заняття	2	***Методи шифрування повідомлень*** 1. Методи шифрування повідомлень та їх історичний розвиток. Основні правила шифрування. 2. Поняття стійкості шифру, незламного шифру, разового шифроблокноту.	[2.15-2-24]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
	5	Практичне заняття СК ПТК	4	***Методи шифрування*** 1. Практичне ознайомлення з методом шифрування повідомлень та практичних програм з використанням емуляторів електромеханічних шифрувальних машин. 2. Отримання практичних навичок шифрування з використанням емулятора шифрувальної машини “Енігма”.	[2.18]
	6	Лабораторна робота СК ПТК	6	***Дослідження шифрів*** 1. Шифр простої буквенної (цифрової) заміни 2. Шифр перестановки 3. Шифр гамування 4. Магічний квадрат 5. Шифр Полібія	[2.18]
		Самостійна робота	2	1. Пакет захисту PGP. 2. Стенографічні методи захисту інформації.	[2.16-2.20]
	7	Лабораторна робота	4	***Дослідження алгоритму шифрування RSA*** 1. Атака на алгоритм шифрування RSA за допомогою метода Ферма. 2. Атака на алгоритм шифрування RSA методом без ключового читання. 3. Атака на алгоритм шифрування RSA який заснований на теоремі про залишки.	[2.16, 2.18]
		Самостійна робота	2	1. Електронний цифровий підпис. 2. Способи захисту електронної пошти.	[2.22]
4			**43**	**Комплексні системи захисту інформації ДПСУ**	
	1	Лекція	2	***Об’єкти захисту інформації*** 1. Комплексна система захисту інформації. 2. Об’єкти захисту та їх властивості. 3. Розроблення та оцінювання захищених систем.	[1.12]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
	2	Групове заняття	2	***Вимоги до комплексної системи захисту інформації (КСЗІ)*** 1. Обґрунтування потреби у створенні системи захисту. Обстеження середовища функціонування ІТС. 2. Визначення й аналіз можливих загроз безпеці. 3. Розроблення політики безпеки. Створення КСЗІ.	[1.1-1.19]
	3	Групове заняття	2	***Моделі загроз інформації*** 1. Формування вимог до моделі загроз інформації на ОІД. 2. Модель порушника.	[1.1-1.19]
	4	Практичне заняття СК ПТК	2	***Розробка моделі загроз об'єкту інформаційної діяльності (ОІД)*** 1. Аналіз функціонування ОІД 2. Визначення загроз інформації на ОІД 3. Формування моделі порушника	[1.1-1.19]
	5	Практичне заняття СК ПТК	4	***Формування проектної документації на КСЗІ в інформаційно-телекомунікаційній системі*** 1. Розробка технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі 2. Формування переліку робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі	[1.1-1.19]
Модульний контроль № 2					
		Індивідуальне завдання	25	Виконання вибіркового дослідницького завдання за заданою тематикою	
	6	Групове заняття	2	***Служба захисту інформації*** 1. Положення про захист інформації в АС. Загальні положення. 2. Завдання та функції служби захисту інформації. Права та обов'язки персоналу служби захисту інформації. 3. Взаємодія служби захисту з іншими підрозділами та організаціями.	[1.1-1.19]

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
		Самостійна робота	2	1. Атестація комплексу технічного захисту інформації на об'єктах інформаційної діяльності. 2. Функції виконавця робіт з атестації комплексу технічного захисту інформації	[1.1-1.19]
	7	Групове заняття	2	***План захисту інформації*** 1. Завдання захисту інформації в АС. Класифікація інформації, що обробляється в АС. 2. Компоненти АС і технології оброблення інформації. Загрози інформації в АС. 3. Політика безпеки інформації в АС. План робіт із захисту інформації в АС.	[1.1-1.19]
Диференційований залік			**4**		
Разом за 8 семестр			**76**		
Разом за IV курс			**150**		
Усього за дисципліну			**150**		

ІНФОРМАЦІЙНІ РЕСУРСИ

1. Нормативно-правові акти

1.1. Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»

1.2. Рішення Ради національної безпеки і оборони України від 28 квітня 2014 року Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України

1.3. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення.

1.4. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.

1.5. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

1.6. Закон України. Про захист інформації в автоматизованих системах (Відомості Верховної Ради (ВВР), 1994, № 31, ст.286) (Вводиться в дію Постановою ВР № 81/94-ВР від 05.07.94, ВВР, 1994, № 31, ст.287)

1.7. Закон України. Про інформацію N 2657-XП від 2 жовтня 1992 року.

1.8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

1.9. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

1.10. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

1.11. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

1.12. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

1.13. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

1.14. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.

1.15. НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.

1.16. НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.

1.17. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.

1.18. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.

1.19. НД ТЗІ 2.3-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності (базова).

1.20. Закон України. Про основні засади забезпечення кібербезпеки України.

2. Базова література

2.1. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – Харків: Консум, 2004. – 508 с.

2.2. 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.– К.: ДУТ, 2015.– 288 с.

2.3. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. – К.: КНТ, 2006. – 280 с. (Серія: Національна і міжнародна безпека)

2.4. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник.– К.: Видавничо-поліграфічний центр “Київський університет”, 2008.– 274 с.

2.5. Почепцов Г. Сучасні інформаційні війни. – К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.

2.6. Почепцов Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах. – К.: .: Вид. дім «Києво-Могилянська академія», 2016. 316 с.

2.7. Копійка В. Гібридна війна Росії проти України після Революції гідності: Монографія / [В. Копійка, М. Дорошко, В. Балюк та ін.] ; наук. ред. М Дорошко, В Балюк. – Київ : Ніка-Центр, 2018. – 280 с.

2.8. Кавун С.В., Носов В.В., Манжай О.В. Інформаційна безпека. – Харків. Вид. ХНЕУ, 2008. – 321 с.

2.9. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.

2.10. Рибальський О.В. Захист інформації в інформаційно-комунікаційних системах. Навчальний посібник для курсантів ВНЗ МВС України / О.В. Рибальський, В.Г. Хахановський, В.А. Кудінов, В.М. Смаглюк. – К.: Вид. Національної академії внутріш. справ, 2013. – 118 с.

2.11. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник в 2-х т. / В.В. Поповский, А.В. Персиков. – Харьков: ООО «Компания СМИТ», 2006. – 238 с. [1]. – 292 с. [2].

2.12. Марущак А.І. Інформаційне право: Доступ до інформації: Навчальний посібник / А.І. Марущак. – К.: КНТ, 2007. – 532 с.

2.13. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с.: іл.

2.14. Вербіцький О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 247 с.

2.15. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия – Телеком, 2002. – 175 с.

2.16. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

2.17. Щербаков А. Ю., Домашев А. В. Прикладная криптография: использование и синтез криптографических интерфейсов. – М.: Русская Редакция, 2003. – 416 с.

2.18. Масленников М. Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 с.

2.19. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. – М.: Вильяме, 2001. – 672 с.

2.20. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. – СПб.: «Лань», 2000.

2.21. Конхейм А. Г. Основы криптографии. – М.: Радио и связь, 1987.

2.22. Венбо Мао Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. – М.: Вильямс, 2005. – 768 с.

2.23. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004.

2.24. Ященко В. В. Введение в криптографию. – СПб.: Питер, 2001.

3. Допоміжна література

3.1. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. – М.: ИНФРА-М, 20010 – 304 с.

3.2. Пастернак-Таранущенко Г. Економічна безпека держави. Статика процесу забезпечення. Підручник для державних службовців, науковців, студентів і аспірантів вищих навчальних закладів економічного профілю / За ред. професора Богдана Кравченка. - К.: "Кондор", 2002. - 302 с

3.3. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: Навчальний посібник. – Харків: Фоліо, 2002. – 285 с

3.4. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. – К.: МОУ, 1999. – 456 с.

3.5. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 386 с.

3.6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – М.: Триумф, 2002. – 816 с.

3.7. Щербаков А. Ю., Домашев А. В. Прикладная криптография: использование и синтез криптографических интерфейсов. – М.: Русская Редакция, 2003. – 416 с.
3.8. Масленников М. Практическая криптография. – СПб.: БХВ-Петербург, 2003. – 464 с.
3.9. Столлингс В. Криптография и защита сетей: принципы и практика. – 2-е изд. – М.: Вильяме, 2001. – 672 с.
3.10. Молдовян А. А., Молдовян Н. А., Советов Б. Я. Криптография. – СПб.: «Лань», 2000.
3.11. Конхейм А. Г. Основы криптографии. – М.: Радио и связь, 1987.
3.12. Венбо Мао Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. – М.: Вильямс, 2005. – 768 с.
3.13. Рябко Б.Я., Фионов А.Н. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004.
3.14. Ященко В. В. Введение в криптографию. – СПб.: Питер, 2001.
3.15. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика, 1997. – 386 с.

4. Інформаційні ресурси в інтернет (інтранет)

1. Бібліотека кафедри зв'язку, автоматизації та захисту інформації, режим доступу - http://10.241.24.235/librery.
2. Методичне забезпечення дисципліни „Інформаційно-телекомунікаційні системи прикордонних підрозділів", режим доступу - http://10.241.24.235/kaf4.
3. Автоматизована електрона система навчання, режим доступу - http://10.241.24.9/.
4. Методичне забезпечення дисципліни «Інформаційна безпека», режим доступу - http://10.241.24.235/kaf18.

ОЦІНЮВАННЯ

Поточне рубіжне та підсумкове оцінювання здійснюється відповідно до положення https://nadpsu.edu.ua/wp-content/uploads/2020/01/polozh-otsinka-2020-_12.01.-.pdf.

ПОЛІТИКА КУРСУ («ПРАВИЛА ГРИ»)

Середовище в аудиторії є творчим, відкритим до конструктивної критики.

Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни. Якщо здобувач вищої освіти був відсутній на заняттях з будь-якої причини, він/вона відпрацьовують навчальні питання та завдання в часи самостійної підготовки та у встановлені викладачем терміни обов'язково звітують про опанування ними навчального матеріалу. Курсанти, які пропустили більше 30% з тих занять, де було передбачено оцінювання, одержали середньоарифметичну з поточних оцінок нижче 2,60, тобто менше 70% позитивних оцінок від загальної кількості, не відзвітували за індивідуальну та самостійну роботу, до семестрового контролю не допускаються.

У разі коли курсант не виконав умови допуску до складання семестрового контролю, завчасно, але не пізніше трьох робочих днів до складання семестрового контролю, рішенням кафедри йому встановлюється індивідуальний термін ліквідації заборгованості. Якщо курсант (слухач, студент) не ліквідовує заборгованість у визначений кафедрою термін, то він вважається таким, що не виконав вимоги робочої

програми навчальної дисципліни і в відомості обліку успішності, в графі «підсумкова оцінка», йому виставляється оцінка «незадовільно» за національною шкалою, 50 балів за 100-бальною шкалою і FX – за шкалою ЄКТС. При повній відсутності позитивних поточних оцінок, за визначені звітності, і не ліквідації заборгованості у визначений кафедрою термін, курсанту (слухачу, студенту) курс з навчальної дисципліни не зараховується і в графі «підсумкова оцінка», йому виставляється оцінка «недопущений» за національною шкалою, 17 балів за 100-бальною шкалою і F за шкалою ЄКТС. В такому випадку курсант (слухач, студент) представляється на засідання Вченої ради факультету, академії і йому пропонується пройти повний курс повторно. У разі відмови розглядається питання про його відрахування з академії.

Дотримання академічної доброчесності

Під час навчання учасники освітнього процесу зобов'язані дотримуватися академічної доброчесності: етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання та/або наукових (творчих) досягнень.

Дотримання академічної доброчесності науково-педагогічним складом передбачає:

- посилання на джерела інформації у разі використання ідей, тверджень, відомостей;
- дотримання норм законодавства про авторське право;
- надання достовірної інформації про результати досліджень та власну педагогічну (науково-педагогічну, творчу) діяльність;
- контроль за дотриманням академічної доброчесності здобувачами освіти.

Дотримання академічної доброчесності здобувачами освіти передбачає:

- самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливим освітніми потребами ця вимога застосовується з урахуванням їх індивідуальних потреб і можливостей);
- посилання на джерела інформації у разі використання ідей, тверджень, відомостей;
- дотримання норм законодавства про авторське право;
- надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності.

За порушення академічної доброчесності учасники освітнього процесу закладу вищої освіти можуть бути притягнені до такої академічної відповідальності.

Нормативно-правове забезпечення: https://nadpsu.edu.ua/osvita/normatyvno-pravove-zabezpechennia/.

Додаток А
Методи навчання та методи контролю навчальних досягнень

Шифр	Метод навчання
1. Словесні методи	
МН 1.1	Лекція
МН 1.2	Розповідь
МН 1.3	Пояснення
МН 1.4	Бесіда
МН 1.5	Інструктаж
МН 1.6	Дискусія
МН 1.7	Диспут
2. Наочні методи	
МН 2.1	Демонстрація
МН 2.2	Ілюстрація
МН 2.3	Спостереження
3. Практичні методи	
МН 3.1	Лабораторна робота
МН 3.2	Практична робота
МН 3.3	Пробні вправи
МН 3.4	Творчі вправи
МН 3.5	Усні вправи
МН 3.6	Практичні вправи
МН 3.7	Графічні вправи
МН 3.8	Технічні вправи
МН 3.9	Групові вправи
4. Методи самостійного та індивідуального навчання	
МН 4.1	Рецептивний
МН 4.2	Репродуктивний
МН 4.3	Евристичний
МН 4.4	Дослідницький

Шифр	Метод контролю навчальних досягнень
1. Попередній контроль	
МК 1.1	Вибірковий усний
МК 1.2	Фронтальний письмовий
МК 1.3	Фронтальний тестовий
МК 1.4	Фронтальний проблемний
2. Поточний контроль	
МК 2.1	Вибірковий усний
МК 2.2	Колоквіум
МК 2.3	Контрольна робота
МК 2.4	Тестування
МК 2.5	Захист звіту з лабораторної роботи
МК 2.6	Захист звіту з практичної роботи
МК 2.7	Індивідуальна розрахункова робота
МК 2.8	Реферат
3. Рубіжний контроль	
МК 3.1	Фронтальний письмовий
МК 3.2	Фронтальний тестовий
МК 3.3	Фронтальний проблемний
4. Підсумковий контроль	
МК 4.1	Усний
МК 4.2	Письмовий
МК 4.3	Тестовий
МК 4.4	Проблемний