НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
ІМЕНІ Б.ХМЕЛЬНИЦЬКОГО

Кафедра телекомунікаційних та інформаційних систем факультету забезпечення оперативно-службової діяльності

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ІТ 10.01 «ОСНОВИ БЕЗПЕКИ ІНФОРМАЦІЇ»
(вибіркова освітня компоненти/для набору 2021 року)
ОПП «ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ІНЖЕНЕРНО-ТЕХНІЧНИХ ПІДРОЗДІЛІВ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ»

Рівень вищої освіти: перший (бакалаврський)
Галузь знань: 25 Воєнні науки, національна безпека, безпека державного кордону
Спеціальність: 252 Безпека державного кордону
Кваліфікація: бакалавр безпеки державного кордону
Професійна кваліфікація:офіцер тактичного рівня Державної прикордонної служби України
Спеціалізація: Організація діяльності інженерно-технічних підрозділів Державної прикордонної служби України
Форма здобуття освіти: денна

Розглянуто та схвалено на засіданні кафедри
Протокол від «____» _____20___ року № _____

Начальник кафедри
телекомунікаційних та інформаційних систем
полковник Іван ЧЕСАНОВСЬКИЙ
(військове звання, підпис, ім’я та прізвище)
«____» _____ 2021 року

АНОТАЦІЯ КУРСУ

Навчальна дисципліна «Основи безпеки інформації» є дисципліною вільного вибору ОПП «Організація діяльності інженерно-технічних підрозділів Державної прикордонної служби України». Пропонується для вивчення протягом 7-го семестру на кафедрі телекомунікаційних та інформаційних систем.

Мета вивчення навчальної дисципліни – формування у офіцера-прикордонника за БАКАЛАВРСЬКИМ рівнем вищої освіти за спеціальністю «Безпека державного кордону» набору загальних та спеціальних компетенцій з основних питань сучасної теорії та практики захисту інформації: основні поняття захисту, методи і засоби захисту, вступ у моделювання захисту, організацію прихованого управління, основи нормативно-правових знань з питань захисту.

Завдання навчальної дисципліни – надати курсанту необхідних для виконання функціональних завдань за посадою знань, вмінь та навичок з питань безпечного функціонування об'єктів інформаційної діяльності, методів та способів забезпечення захисту інформації, здійснення прихованого управління підрозділами, застосування нормативно-правових документів в повсякденній діяльності.

Вивчення навчальної дисципліни забезпечує досягнення курсантами (або слухачами, студентами, ад'юнктами) наступних **програмних результатів навчання**:

ПРН 11 Організовувати заходи щодо режиму секретності, захисту інформації та протидії технічним засобам розвідки.

ПРН 21 Упевнено застосовувати штатне озброєння підрозділу; інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), спеціальне програмне забезпечення для розв'язування фахово-орієнтованих задач, у тому числі з використанням математичних методів; проводити процедури, пов'язані з перевіркою, обслуговуванням, ремонтом і застосуванням засобів зв'язку, технічних засобів охорони кордону та транспортних засобів в обсязі інструкції з експлуатації.

Досягнення програмних результатів навчання передбачає здатність демонструвати знання, розуміння, застосування, аналіз, синтез та оцінювання його складових.

ПРН 11 Організовувати заходи щодо режиму секретності, захисту інформації та протидії технічним засобам розвідки.

Знання:

основні засади забезпечення кібербезпеки України;
структуру та функціонування Національна система кібербезпеки;
поняття і визначення кіберпростір, кібербезпека та кібертероризм;
нормативно-правову базу в галузі захисту інформації.

Розуміння:

особливості захисту інформації в телекомунікаційних системах;
технічне завдання на розробку системи комплексного захисту інформації в АС;
план комплексного захисту об'єктів інформаційної діяльності;

Застосовування:

правильну та ефективну експлуатацію об'єктів інформаційної діяльності;
проектну документацію на КСЗІ в інформаційно-телекомунікаційній системі;

вимоги нормативних документів стосовно інформаційної безпеки;
план захисту інформації.

Аналіз:

основні положення служби захисту інформації;
перспективи розвитку інформаційної безпеки Державної прикордонної служби України.

Синтез:

моделі загроз об’єкту інформаційної діяльності;
план захисту інформації.
проектну документацію на КСЗІ;

Оцінювання:

вимоги до комплексної системи захисту інформації;

ПРН 21 Упевнено застосовувати штатне озброєння підрозділу; інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), спеціальне програмне забезпечення для розв’язування фахово-орієнтованих задач, у тому числі з використанням математичних методів; проводити процедури, пов’язані з перевіркою, обслуговуванням, ремонтом і застосуванням засобів зв’язку, технічних засобів охорони кордону та транспортних засобів в обсязі інструкції з експлуатації.

Досягнення програмних результатів навчання передбачає здатність демонструвати:

Знання:

інформаційні технології та проблеми їхньої безпеки;
основи безпеки інформаційних ресурсів;
критерії безпеки інформаційних технологій;

Розуміння:

об’єкти захисту інформації;
технічне завдання на розробку системи комплексного захисту інформації в АС;
сучасні методи захисту інформації в комп’ютерних системах та телекомунікаційних мережах

Застосовування:

захист телекомунікаційної системи засобами ТЗІ;
моделі загроз об’єкту інформаційної діяльності;

Аналіз:

основні положення служби захисту інформації;
проектну документацію на КСЗІ;

Синтез:

моделі загроз об’єкту інформаційної діяльності;
план захисту інформації.
проектну документацію на КСЗІ;

Оцінювання:
якість організації інформаційної безпеки органів Державної прикордонної служби України.

ВИКЛАДАЧІ:

доцент кафедри телекомунікаційних та інформаційних систем кандидат технічних наук, працівник ДПСУ Олександр БАСАРАБ, e-mail: a_basarab@ukr.net.

ПЕРЕДУМОВИ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ.

Зв'язок прикордонних підрозділів, програмно-технічні комплекси прикордонних підрозділів.

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 ЄКТС	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	модульний контроль	підсумковий контроль	----------	Усього	реферат	конспект з теми	переклад текстів	розрахункове завдання	курсова робота	ІРГР	----------				
4	7	4	120	40	2	18		12		4				4		40		40						40		+	
Усього за дисципліну		4	120	40	2	18		12		4				4		40		40						40		+	

Основні методи навчання: МН1.1; МН1.2; МН1.3; МН1.4; МН1.5; МН2.2; МН2.3; МН3.2.

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

КОМПЕТЕНТНОСТІ ТА КОНТРОЛЬ РІВНЯ ЇХ ДОСЯГНЕННЯ КУРСАНТАМИ

Шифр	Компетентність	Оцінювання
Загальні компетентності		
ЗК-11	Навички використання інформаційних і комунікаційних технологій.	МК1.1; МК1.2; МК1.3; МК2.1; МК2.4; МК2.6; МК3.1; МК3.2; МК4.2; МК4.3
Спеціальні (фахові, предметні) компетентності		
СК-3	Здатність формувати систему та процеси забезпечення безпеки державного кордону, моделі інтегрованого управління кордонами, підсистеми побудови охорони державного кордону, застосовувати способи дій сил і засобів (у тому числі службових тварин), оцінювати їх ефективність.	МК1.1; МК1.2; МК3.1; МК3.2; МК4.3
СК-4	Здатність застосовувати тактичні прийоми загальновійськового бою та бойових дій прикордонних підрозділів, способи дій підрозділів, забезпечувати бойове, ресурсне, інженерно-технічне забезпечення та зв’язок у підрозділі в різних умовах функціонування та різних формах оперативно-службових дій	МК1.1; МК1.2; МК3.1; МК3.2; МК4.3

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

Шифр	Компетентність	Методи навчання	Оцінювання
ПРН-11	Організовувати заходи щодо режиму секретності, захисту інформації та протидії технічним засобам розвідки.	МН1.1; МН1.2; МН1.3; МН1.4; МН1.5; МН2.2; МН2.3; МН3.2	МК1.1; МК1.2; МК1.3; МК2.1; МК2.4; МК2.6; МК3.1; МК3.2; МК4.2; МК4.3
ПРН-21	Упевнено застосовувати штатне озброєння підрозділу; інформаційні системи, інформаційні технології, технології захисту даних, методи обробки, накопичення та оцінювання інформації, інформаційно-	МН1.1; МН1.2; МН1.3; МН1.4; МН1.5; МН2.2; МН2.3; МН3.2	МК1.1; МК1.2; МК1.3; МК2.1; МК2.4; МК2.6; МК3.1; МК3.2; МК4.2; МК4.3

Шифр	Компетентність	Методи навчання	Оцінювання
	аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні), спеціальне програмне забезпечення для розв’язування фахово-орієнтованих задач, у тому числі з використанням математичних методів; проводити процедури, пов’язані з перевіркою, обслуговуванням, ремонтом і застосуванням засобів зв’язку, технічних засобів охорони кордону та транспортних засобів в обсязі інструкції з експлуатації.		

ОРГАНІЗАЦІЯ НАВЧАННЯ

№ теми	Найменування теми	Кіль-кість годин	Номери, вид занять та кількість годин									Місяці	Номери тем, занять та кількість годин	Кількість годин
			1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**			
1	Теоретичні засади організації безпеки інформації	4	Л2	Гз2								09	1/1 Л (2); 1/2 Гз (2);	4
2	Технічний захист інформації	6	Гз2	Пз4								10	2/1 Гз (2); 2/2Пз(4); 3/1 Гз (2); 3/2 Гз (2);	10
3	Документальний супровід інформаційної безпеки	20	Гз2	Гз2	Пз2	Гз2	Гз2	Пз2	Гз2	Гз2	Сз2	11	3/3 Пз (2); 3/4 Гз (2); 3/5 Гз (2); 3/6 Пз (2); 3/7 Гз (2); 3/8 Гз (2);	12
4	Комплексні системи захисту інформації ДПСУ	6	Гз2	Пз4								12	3/9 Сз (4); 4/1 Гз (2); 4/2Пз(4); Дз(4)	14
Диференційований залік		4	Дз4									**Всього**		**40**
Всього		**40**												

Умовні скорочення:

Лекція – Л; Практичне заняття – Пз; Групове заняття – Гз; Семінарське заняття - Сз; Диференційований залік - Дз

Заняття, що обов’язкове для оцінювання - Пз2

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
1	**2**	**3**	**4**	**5**	**6**
4 курс					
VII семестр					
1			**46**	**ТЕМА 1: ОРГАНІЗАЦІЯ БЕЗПЕКИ ІНФОРМАЦІЇ**	
	1	лекція	2	**Основи інформаційної безпеки.** 1. Введення в дисципліну. Мета, задачі та структура навчальної дисципліни; 2. Основні поняття інформаційної безпеки. 3. Загрози інформаційній безпеці, методи і засоби забезпечення інформаційної безпеки	1.1-1.20; 2.1; 2.2
		індивідуальна робота (конспект з теми)	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; 2.1; 2.2
		самостійна робота	2	1. Інформація, її види та властивості. 2. Інформаційні системи як об'єкти захисту.	1.7
		індивідуальна робота (конспект з теми)	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; 2.1; 2.2
		індивідуальна робота (конспект з теми)	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; 2.1; 2.2
	2	групове заняття	2	**Інформаційні технології та проблеми їхньої безпеки** 1. Визначення інформаційної технології. 2. Співвідношення інформаційної технології та інформаційної системи. 3. Класифікація та види інформаційних технологій.	1.1; 2.1; 2.2

				4. Основні проблеми безпеки інформаційних технологій.	
		самостійна робота	2	1. Співвідношення інформаційної технології та інформаційної системи. 2. Класифікація та види інформаційних технологій.	2.1; 2.2
		індивідуальна робота (конспект з теми)	2	**Основи безпеки інформаційних ресурсів** 1. Загрози безпеці інформації та інформаційних ресурсів. 2. Основні напрями забезпечення безпеки інформації та інформаційних ресурсів.	1.1; 2.1; 2.2
		самостійна робота	2	1. Архітектура відкритих систем. 2. Загрози в архітектурі відкритих мереж.	2.1
		самостійна робота	2	1. Процедури захисту. 2. Сервісні служби захисту. 3. Реалізація захисту.	2.2.
		самостійна робота	2	1. Збитки як категорія класифікації загроз. 2. Класифікація загроз безпеці інформації. 3. Класифікація джерел загроз.	2.2, 2.3
		індивідуальна робота (конспект з теми)	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.	2.1; 2.2
		самостійна робота	2	1. Ранжирування джерел загроз. 2. Класифікація уразливостей безпеці. 3. Ранжирування уразливостей. 4. Класифікація актуальних загроз.	2.2, 2.3
		індивідуальна робота (конспект з теми)	2	**Нормативно-правове забезпечення захисту державних інформаційних ресурсів** 1. Нормативно-правове забезпечення захисту державних інформаційних ресурсів. 2. Концептуальних аналіз уразливості державних інформаційних ресурсів. 3. Правові аспекти формування системи державних інформаційних ресурсів	2.2, 2.3
		самостійна робота	2	1. Вимоги до системи захисту інформації 2. Вимоги до захисту інформації 3. Види забезпечення системи захисту інформації	2.4; 2.5
		самостійна робота	2	1. Державна таємниця 2. Комерційна таємниця	2.3 – 2.6

				3. Персональні дані	
		індивідуальна робота (конспект з теми)	2	**Законодавчий рівень інформаційної безпеки** 1. Основні поняття законодавчого рівня інформаційної безпеки 2. Законодавство в галузі інформаційної безпеки 3. Стандарти та специфікації в галузі безпеки інформаційних систем	2.3 – 2.6
		самостійна робота	2	1. Структура правових актів 2. Нормативно-правові документи 3. Форми правового захисту інформації	2.3 – 2.6
		індивідуальна робота (конспект з теми)	2	**Адміністративний рівень інформаційної безпеки** 1. Поняття політики безпеки 2. Розробка та реалізація політики безпеки 3. Управління ризиками	2.3 – 2.6
		індивідуальна робота (конспект з теми)	2	**Організаційний рівень інформаційної безпеки** 1. Основні класи заходів організаційного рівня 2. Управління персоналом 3. Реагування на порушення режиму безпеки	2.3 – 2.6
		самостійна робота	2	1. Фізичний захист 2. Підтримка працездатності 3. Служба безпеки	2.3 – 2.6
		індивідуальна робота (конспект з теми)	2	**Інженерно-технічний рівень інформаційної безпеки** 1. Поняття інженерно-технічного захисту 2. Фізичні засоби захисту 3. Програмно-апаратні засоби захисту	2.3 – 2.6
		самостійна робота	2	1. Методи шифрування 2. Криптографічні протоколи 3. Стеганографічні засоби захисту	2.3 – 2.6
2			**18**	**ТЕМА 2: ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**	
	1	групове заняття	2	**Технічні канали витоку інформації** 1. Поняття технічного каналу витоку інформації 2. Організаційно технічні заходи щодо ТЗІ на ОІД 3. Класифікація каналів витоку інформації	2.3; 2.6
		індивідуальна робота (конспект з теми)	2	**Основні засади технічного захисту інформації в ДПСУ** 1. Основні поняття та категорії 2. Нормативно-правове забезпечення технічного захисту інформації 3. Структура та завдання підрозділів технічного захисту інформації	2.3; 2.6

		самостійна робота	2	1. Загальний підхід до технічного каналу витоку інформації 2. Фізичні основи утворення технічного каналу витоку інформації 3. Основи несанкціонованого зняття інформації	2.3; 2.6
		індивідуальна робота (конспект з теми)	2	**Методи та засоби блокування технічних каналів витоку акустичної інформації** 1. Принципи виявлення технічних каналів витоку інформації 2. Виявлення та блокування технічних каналів витоку акустичної інформації 3.Захист акустичної інформації.	2.3; 2.6
		самостійна робота	2	1. Методи пошуку радіозакладних пристроїв 2. Захист письмової інформації від оптичного зняття	2.3; 2.6
		індивідуальна робота (конспект з теми)	2	**Методи та засоби блокування технічних каналів витоку за електромагнітним випромінюванням** 1. Захист інформації від витоку по каналам, утворених допоміжними технічними пристроями. 2. Захист інформації від несанкціонованого запису звукозаписувальними пристроями 3. Захист електронної інформації	2.3; 2.6
		самостійна робота	2	1. Випромінювання допоміжних пристроїв 2. Способи перевипромінювання інформації допоміжними пристроями	2.3; 2.6
	2	практичне заняття	4	**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.	2.3; 2.6
3			**36**	**ТЕМА 3: ДОКУМЕНТАЛЬНИЙ СУПРОВІД БЕЗПЕКИ ІНФОРМАЦІЇ**	
	1	групове заняття (ДСК)	2	**Основні засади забезпечення збереження державної таємниці в України** 1. Загальні положення, основні терміни та поняття. 2. Віднесення інформації до державної таємниці. 3. Основні організаційно-правові засади щодо охорони державної таємниці. 4. Порядок здійснення технічного та криптографічного захисту інформації.	1.21; 1.23; 1.24

		індивідуальна робота (конспект з теми)	2	**Здійснення діяльності пов'язаної з державною таємницею** 1. Порядок отримання спеціального дозволу на провадження діяльності пов'язаної з охороною державної таємниці. 2. Права та обов'язки режимно секретного органу. 3. Порядок надання допуску до державної таємниці.	1.21; 1.22;
		самостійна робота	2	1. Обов'язки та обмеження прав громадян яким надано допуск та доступ до державної таємниці.	1.21; 1.22;
	2	групове заняття (ДСК)	2	**Порядок віднесення інформації до державної таємниці** 1. Засекречування та розсекречування інформації. 2. Звод відомостей що становлять державну таємницю. 3. Перегляд грифу секретності. 4. Порядок проведення експертизи матеріального носія інформації.	1.21; 1.22; 1.23;
		індивідуальна робота (конспект з теми)	2	**Порядок обладнання об'єктів інформаційної діяльності** 1. Вимоги до режимних приміщень та контрольованих зон. 2. Вимоги до сховищ для зберігання матеріальних носіїв інформації.. 3. Пропускний та внутрішньооб'єктовий режим.	1.21; 1.22; 1.29; 1.30
	3	практичне заняття (ДСК)	2	**Практична робота щодо отримання спеціального дозволу пов'язаною з охороною державної таємниці** 1. Складання мотивованого листа на щодо отримання ліцензії на провадження діяльності пов'язаної з державною таємницею. 2. Оформлення акту спеціальної експертизи. 3. Складання номенклатури посад що передбачає наявність форми допуску.	1.21; 1.22;
	4	групове заняття (ДСК)	2	**Документообіг пов'язаний з державною таємницею** 1. Організація окремого секретного діловодства. 2. Облік секретних документів. 3. Облік, зберігання та видача робочих зошитів, спецваліз. 4. Облік секретних виробів.	1.21; 1.22;
	5	групове заняття (ДСК)	2	**Відпрацювання секретних документів** 1. Складання та оформлення секретних документів. 2. Друкування секретних документів. 3. Виготовлення та облік секретних документів.	1.21; 1.22;
		індивідуальна робота (конспект з теми)	2	**Пересилка секретних документів та виробів** 1. Порядок оформлення пакетів. 2. Пересилка секретних документів працівниками режимно – секретних органів.	1.21; 1.22;

				3. Дотримання режиму секретності під час транспортування секретних виробів.	
		самостійна робота	2	**Формування, облік та зберігання секретних справ** 1. Порядок складання номенклатури секретних справ. 2. Підготовка та передача секретних справ на архівне зберігання.	1.21; 1.22;
	6	практична робота (ДСК)	2	**Експертиза цінності матеріальних носіїв інформації** 1. Проведення експертизи цінності матеріальних носіїв інформації. 2. Порядок оформлення опису справ, що підлягають передачі на зберігання в архів.	1.21; 1.22;
		самостійна робота	2	**Порядок знищення МНСІ** 1. Знищення секретних документів. 2. Знищення секретних виробів.	1.2
	7	групове заняття (Т)	2	**Використання засобів ЕОТ під час обробки таємної інформації** 1. Порядок введення в експлуатацію ОІД 2. Порядок введення в експлуатацію засобів ЕОТ на ОІД. 3. Забезпечення режиму секретності під час обробки інформації, що містить державну таємницю в автоматизованих системах.	1.21; 1.22;
		самостійна робота	2	**Порядок поводження з шифротелеграмами** 1. Порядок оформлення з шифротелеграм. 2. Порядок обліку та передачі шифротелеграм. 3. Порядок знищення шифротелеграм.	1.21; 1.22; 1.34
	8	групове заняття (ДСК)	2	**Порядок поводження із секретними документами під час нарад та у відряджені** 1. Особливості поводження із секретними технічними документами. 2. Проведення нарад з використанням секретної інформації. 3. Поводження з секретними документами і виробами під час відрядження	1.21; 1.22; 1.34
		самостійна робота	2	**Особливості збереження державної таємниці при роботі іноземних делегацій та в особливих умовах** 1. Порядок виїзду за кордон громадянами яким надано допуск до державної таємниці. 2. Забезпечення режиму секретності під час міжнародного співробітництва. 3. Забезпечення режиму секретності в умовах особливого періоду або надзвичайного стану.	1.21; 1.22;
	9	семінар (ДСК)	4	**Відповідальність посадових осіб за порушення вимог щодо поводження з державною таємницею**	1.21; 1.22; 1.31 – 1.33

				1. Порядок здійснення контролю за додержанням державної таємниці. 2. Порядок проведення службових розслідувань пов'язаних з порушенням вимог режиму секретності. 3. Адміністративна та кримінальна відповідальність за порушення режиму секретності.	
4			**16**	**ТЕМА 4:КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДПСУ**	
	1	групове заняття	2	**Об'єкти захисту інформації** 1. Комплексна система захисту інформації. 2. Об'єкти захисту та їх властивості. 3. Розроблення та оцінювання захищених систем.	1.3-1.19; 1.24-1.30
		індивідуальна робота (конспект з теми)	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.	1.3-1.19; 1.24-1.30
		індивідуальна робота (конспект з теми)	2	**Моделі загроз інформації** 1. Формування вимог до моделі загроз інформації на ОІД. 2. Модель порушника.	1.3-1.19; 1.24-1.30
		індивідуальна робота (конспект з теми)	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.	1.3-1.19; 1.24-1.30
		самостійна робота	2	1. Атестація комплексу технічного захисту інформації на об'єктах інформаційної діяльності. 2. Функції виконавця робіт з атестації комплексу технічного захисту інформації	1.3-1.19; 1.24-1.30
		індивідуальна робота (конспект з теми)	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.	1.3-1.19; 1.24-1.30

	2	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	1.3-1.19; 1.24-1.30
Диференційований залік			4		
Разом за VII семестр			120		
Разом за 4 курс			120		
Усього за дисципліну			120		

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-XII 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.

1.21. Закон України. «Про державну таємницю» N 3855-XII від 21 січня 1994 року.

1.23. Наказ служби безпеки України. «Про затвердження зводу відомостей, що становлять державну таємницю» N 440 від 12 серпня 2005 року.

1.24. Закон України. «Про захист інформації в інформаційно-телекомунікаційних системах» (зі змінами).

1.25. Указ Президента України. «Положення про технічний захист інформації в Україні» від 27.09.1999 № 1229.

1.26. Постановою Кабінету Міністрів України. «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373.

1.27. Наказ АДПСУ. "Про затвердження Інструкції про порядок проведення службового розслідування у Державній прикордонній службі України" від 14.02.2005 № 111.

1.28. Кодекс України про адміністративні правопорушення. №8073-X від 7 грудня 1984 року.

1.29. Кримінальний кодекс України. №2341-III від 5 квітня 2001 року.

1.30. Указ президента України. «Про Положення про порядок здійснення криптографічного захисту і Україні» №505/98 від 22 травня 1998 року.

1.31. Указ президента України. «Про Положення про порядок здійснення технічного захисту і Україні» №505/98 від 22 травня 1998 року.

2. Базова

2.1. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – Харків: Консум, 2004. – 508 с – 10 примірників.

2.2. 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)

2.3. Рибальський О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту інформації. Посібник для курсантів ВНЗ МВС України. – К.: Вид. Національної академії внутріш. справ, 2012. – 104 с.

2.4. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2007. – 352 с.

2.5. Кавун С. В. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2008. – 196 с.

2.6. Лужецький В.А., Основи інформаційної безпеки : навчальний посібник / В.А. Лужецький, А.Д. Кожухівський, О.П. Войтович. – Вінниця : ВНТУ, 2013. – 221 с.

3. Допоміжна

1.1. Катеринчук І.С., Желдак А. А., Основи телекомунікаційних мереж, - НАДПСУ, 2009. – 159 с.
1.2. Катеринчук І.С., Мул Д.А., та ін. Програмно-технічні комплекси підрозділів охорони кордону. – НАДПСУ, 2009. – 270с.
1.3. Литвин М.М. Інтегроване управління кордонами. – Хмельницький: Видавництво НАДПСУ, 2012. – 416 с.
1.4. Уенстон М. Организация защиты сетей Cisco. – Москва. Видавництво «Вильямс», 2005.-768 с.
1.5. Журнал “Защита информации: Конфидент».
1.6. Журнал ”Безопасность информации”.

X. ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТ (ІНТРАНЕТ)

1. Бібліотека кафедри зв’язку, автоматизації та кібербезпеки, режим доступу - http://10.241.24.235/librery.
2. Методичне забезпечення дисципліни «Зв'язок у прикордонних підрозділах», режим доступу - http://10.241.24.235/kaf4.
3. Автоматизована електрона система навчання (модульне середовище), режим доступу - http://10.241.24.9/moodle.

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 диференційованого заліку не допускаються.

У разі коли курсант не виконав умови допуску до складання диференційованого заліку, завчасно, але не пізніше трьох робочих днів до складання диференційованого заліку, рішенням кафедри йому встановлюється індивідуальний термін ліквідації заборгованості. Якщо курсант 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 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 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 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. Традиційні методи навчання	
МН.1.1.	Усне викладення навчального матеріалу (*розповідь, пояснення, лекція*)
МН.1.2.	Обговорення матеріалу, що вивчається (*бесіда, дискусія, брифінг, диспут*)
МН.1.3.	Наочні методи (*ілюстрація, демонстрація*)
МН.1.4.	Практичні методи (*лабораторна робота, практична робота, пробні вправи, творчі вправи, усні вправи, практичні вправи, графічні вправи, технічні вправи*)
МН.1.5.	Методи самостійного та індивідуального навчання (*рецептивний, репродуктивний, евристичний, дослідницький*)
2. Активні методи навчання	
МН.2.1.	Ігрові (*професійні ігри, професійний тренінг*)
МН.2.2.	Неігрові (*аналіз конкретної ситуації, круглий стіл, навчання через науково-дослідну роботу*)
МН.2.3.	Неімітаційні (*групова дискусія, індивідуальні практикуми, метод «ХОБО», активні види лекційних і семінарських занять*)
3. Інтерактивні методи навчання	
МН.3.1.	Інтерактивні методи в малих групах
МН.3.2.	Інтерактивні методи в великих групах
МН.3.3.	Інтерактивні методи під час самостійної роботи

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
МК 1.5	Виконання нормативу
МК 1.6	Виконання вправи
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
МК 2.9	Виконання нормативу
МК 2.10	Виконання вправи
3. Рубіжний контроль	
МК 3.1	Фронтальний письмовий
МК 3.2	Фронтальний тестовий
МК 3.3	Фронтальний проблемний
МК 3.4	Виконання нормативу
МК 3.5	Виконання вправи
4. Підсумковий контроль	
МК 4.1	Усний
МК 4.2	Письмовий
МК 4.3	Тестовий
МК 4.4	Проблемний
МК 4.5	Практичний