НАЦІОНАЛЬНА АКАДЕМІЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ
ІМЕНІ Б. ХМЕЛЬНИЦЬКОГО

кафедра національної безпеки та управління
факультету підготовки керівних кадрів

СИЛАБУС
НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
ООК 15 «ІНФОРМАЦІЙНА ПОЛІТИКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА»

Рівень вищої освіти: другий (магістерський)

Галузь знань: 25 Воєнні науки, національна безпека, безпека державного кордону

Спеціальність: 256 Національна безпека (сфера прикордонної діяльності)

Кваліфікація: Магістр національної безпеки (сфера прикордонної діяльності)

Професійна кваліфікація: офіцер оперативно-тактичного рівня Державної прикордонної служби України

ВСТУПНІ РЕКВІЗИТИ

Статус дисципліни: Навчальна дисципліна обов'язкового компонента.

Тривалість курсу: 4 кредити (120 годин).

Мова викладання: українська.

Мета вивчення навчальної дисципліни – є формування у слухачів сучасних теоретичних і практичних знань, умінь і навичок з державної інформаційної політики, комунікативної політики органів охорони державного кордону та оволодіння основними теоретичними положеннями у галузі інформаційної безпеки держави, безпеки інформаційних технологій та базовими засадами забезпечення інформаційної безпеки України.

Завдання навчальної дисципліни: формування у офіцера-прикордонника за другим магістерським рівнем вищої освіти за спеціальністю 256 Національна безпека (сфера прикордонної діяльності), відповідних програмних компетентностей, достатніх для виконання функціональних обов'язків за відповідними посадами.

Анотація курсу:

Актуальність курсу підтверджується потребою врахування в оперативно-службової діяльності органів охорони державного кордону державної інформаційної політики, застосування сучасних методів щодо забезпечення інформаційної безпеки та здійснювати стратегічні комунікації в ході виконання поставлених завдань.

В межах курсу підготовка офіцера-керівника оперативно-тактичного рівня здійснюється шляхом надання знань, вироблення вмінь та формування практичних навичок необхідних для виконання обов'язків на посадах керівного складу ДПСУ, формування здатності розв'язувати складні завдання і проблеми прикордонної діяльності у галузі національної безпеки, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог, інтегрування знань різних сфер національної безпеки, автономне прийняття рішень в складних і непередбачуваних умовах неповної/недостатньої інформації та суперечливих вимог, що потребує застосування нових підходів і прогнозування, створення відповідної бази для подальшого професійного становлення та самовдосконалення з урахуванням конкретних потреб ДПСУ.

Вивчення курсі сприяє набуттю спроможності здійснювати керівництво органами охорони державного кордону, оцінювати рівень ризику, приймати

рішення та управляти підлеглими в загальній системі національної безпеки держави.

Матеріали курсу розроблені на основі європейського досвіду і досвіду країн НАТО щодо здійснення інформаційної політики та інформаційної безпеки держави.

Пререквізити курсу: Базові знання основ управління, філософії, психології.

Викладач:

Доцент кафедри національної безпеки та управління кандидат військових наук, доцент Ігор Морозов, e-mail: smorozov13@gmail.com

КОМПЕТЕНТНОСТІ ТА РЕЗУЛЬТАТИ НАВЧАННЯ

Вивчення навчальної дисципліни забезпечує формування у слухачів наступних **компетентностей**:

А) Загальні компетентності:

ЗК 2 Знання та розуміння функціонування системи забезпечення національної безпеки та безпеки державного кордону на рівні новітніх досягнень.

ЗК 4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК 7 Здатність приймати обґрунтовані рішення у складних і непередбачуваних умовах, що потребує застосування нових підходів та прогнозування.

Б) Спеціальні (фахові, предметні) компетентності:

ФК 2.Здатність забезпечити спроможність частин, підрозділів та органів управління Державної прикордонної служби України (інших військових формувань та правоохоронних органів, утворених відповідно до Законів України) до виконання завдань за призначенням у системі національної безпеки.

ФК 6.Здатність до керівництва розвідувальною, контррозвідувальною, інформаційно-аналітичною та оперативно-розшуковою діяльністю, здійснення адміністративно-правових процедур в інтересах забезпечення національної безпеки України.

ФК 7.Здатність до організації взаємодії та співробітництва з суб'єктами забезпечення національної безпеки та інтегрованого управління кордонами, виконання координаційних функцій, налагодження стратегічних комунікацій з громадськістю з питань безпеки державного кордону.

Вивчення навчальної дисципліни забезпечує досягнення слухачами наступних **програмних результатів навчання**:

ПРН 4 Розробляти інформаційно-аналітичні матеріали, доповіді та інші службові (службово-бойові) документи.

ПРН 5 Виявляти та прогнозувати ризики від впливу реальних та потенційних загроз безпеці державного кордону, обґрунтовувати заходи щодо їх мінімізації на місцевому рівні, застосовуючи технологію аналізу ризиків та кримінального аналізу.

ПРН 7 Виконувати функції управління (прийняття рішення, планування, організація, мотивація та контроль) прикордонною діяльністю в різних режимах функціонування та умовах обстановки.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Концептуальні основи інформаційної політики.

Державна інформаційна політика. Принципи інформаційних відносин. Інформаційна політика: сутність, напрями, види. Державна інформаційна політика України та шляхи її вдосконалення. Центральні органи державної виконавчої влади України в галузі інформації. Інформаційна політика зарубіжних країн. Основні аспекти зарубіжного досвіду регулювання інформаційної сфери. Інформаційна політика Європейського Союзу щодо побудови інформаційного суспільства. Інформаційна політика ООН. Основні напрями інформаційної політики ООН. Просування України до інформаційного суспільства за відповідними критеріями. Інформаційна політика міжурядових європейських організацій. Європейські інститути: тенденції міжнародних інформаційних відносин. Міжнародний форум інформаційного суспільства Організації центральноєвропейська ініціатива. Інформаційна проблематика в діяльності ОБСЄ і НАТО. Концепція національної інформаційної політики. Концепція розвитку державної інформаційної інфраструктури

Тема 2. Стратегічні комунікації.

Сутність та зміст стратегічних комунікацій. Поняття стратегічних комунікацій. Основні компоненти стратегічних комунікацій за стандартами НАТО. Завдання національної системи стратегічних комунікацій. Стратегічні комунікації як інформаційний інструмент захисту та реалізації інтересів держави. Еволюція проблематики стратегічних комунікацій. «Стратегічні комунікації» та «пропаганда»: проблемні аспекти сепарації. Проблема визначення наративів стратегічних комунікацій. Система формування іміджу організації. Зміцнення позитивного іміджу ДПСУ. Засоби масової інформації. Основні принципи взаємодії із засобами масової інформації. Планування роботи зі ЗМІ. Вирішення конфліктних ситуацій зі ЗМІ. Робота керівника організації із засобами масової інформації. Підготовка та участь керівника вищої ланки до прямого ефіру. Основні правила при наданні коментаря для сюжету в теленовинах. Підготовка керівника організації до проведення прес-

конференції. Співпраця ДПСУ з об’єднаннями громадян. Об’єднання громадян як цільова аудиторія стратегічних комунікацій. Механізми співпраці з об’єднаннями громадян.

Тема 3. Інформаційна безпека.

Суспільно-психологічна характеристика інформаційного простору. Когнітивні підходи до аналізу інформаційного простору. Особливості захоплення і захисту інформаційного простору. Інформаційно-комунікативні процеси в сучасних суспільствах. Державне управління в умовах інформаційного суспільства. Стратегічні, інформаційні і віртуальні потоки. Стратегічні і тактичні , інформаційні та віртуальні потоки. Управління масовою свідомістю та активністю населення в соціосистемах. Інформаційне протиборство і національна безпека. Інформаційне протиборство та операції національної безпеки. Пропаганда та комунікативні складники інформаційно-психологічної боротьби. Інформаційні та віртуальні потоки в соціосистемах. Військові дослідження проблем комунікації та мислення. Підготовка спеціалістів у сфері інформаційного протиборства на пострадянському просторі. Інформаційне протиборство: сучасність. Росія і Україна у співставленні їх комунікативних пропагандистських можливостей. Особливості пропагандистських механізмів з двох боків російсько-українського конфлікту.

Тема 4. Основи кібернетичної безпеки.

Основні засади забезпечення кібербезпеки України. Національна система кібербезпеки, її структура та функціонування. Кіберпростір, кібербезпека та кібертероризм: поняття і визначення. Інформаційні системи, як об'єкти інформаційної безпеки. Інформаційні технології та проблеми їхньої безпеки. Основи безпеки інформаційних ресурсів. Критерії безпеки інформаційних технологій. Захист державних інформаційних ресурсів.

ОРГАНІЗАЦІЯ НАВЧАННЯ

Розподіл навчального часу за курсами, семестрами та видами навчального навантаження

Курс	Семестр	Кількість кредитів ЄКТС	Кількість годин																	Форми підсумкового контролю		
			Загальна	Усього аудиторних занять	Аудиторна робота								Індивідуальна робота							Самостійна робота			
					лекції	практичні заняття	семінари	лабораторні заняття	групові заняття	групові вправи	рольові ігри	контрольна робота	підсумковий контроль	Усього	вибіркове дослідницьке завдання	конспект з теми	переклад текстів	розрахункове завдання	курсова робота	ІРГР		Екзамен	Диференційований залік	Залік
2	**3**	**2**	**54**	**8**	8									**30**	30						**16**			
2	**4**	**2**	**66**	**6**	4								2	**22**	22						**38**		+	
Усього за дисципліну		**4**	**120**	**14**	**12**								**2**	**52**	**52**						**54**			

Запланована кількість аудиторного навантаження – 14 годин

№ теми	Найменування теми	Кількість годин	Номери, вид занять та кількість годин							Місяці	Номери тем, занять та кількість годин	Кількість годин
			1	**2**	**3**	**4**	**5**					
1	Концептуальні основи інформаційної політики	**4**	Л-2	Л-2						**09**	1/1-Л(2); 1/2-Л(2); 2/1-Л(2); 2/2-Л(2);	**8**
2	Стратегічні комунікації	**4**	Л-2	Л-2						**04**	3/1-Л(2); 4/1-Л(2); ДЗ(2)	**6**
3	Інформаційна безпека	**2**	Л-2									
4	Основи кібернетичної безпеки	**2**	Л-2									
Диференційований залік		**2**										
Всього		**14**								**Всього**		**14**

Умовні скорочення:
Лекція - Л
Практичне заняття - Пз
Групова вправа- ГВ
Семінарське заняття - Сз
Диференційований залік - ДЗ
Заняття, що обов’язкове для оцінювання - 5/3Пз(2)

4.4. Тематичний план

№ теми	№ заняття	Види навчальних занять, завдань	Кількість годин	Найменування теми і навчальні питання	Література
1	**2**	**3**	**4**	**5**	**6**
II курс					
III семестр					
1			**30**	**Концептуальні основи інформаційної політики**	
	1	лекція	2	***Державна інформаційна політика. Основні принципи інформаційних відносин*** 1. Основні категорії державної інформаційної політики. 2. Принципи інформаційних відносин.	[1.1-1.19], [2.1, 2.3]
	2	лекція	2	***Державна інформаційна політика України*** 1. Інформаційна політика: сутність, напрями, види. 2. Державна інформаційна політика України та шляхи її вдосконалення. 3. Центральні органи державної виконавчої влади України в галузі інформації.	[1.1-1.19], [2.1-2.3]
		самостійна робота	2	***Інформаційна політика зарубіжних країн*** 1. Основні аспекти зарубіжного досвіду регулювання інформаційної сфери. 2. Інформаційна політика Європейського Союзу щодо побудови інформаційного суспільства.	[2.1]
		самостійна робота	2	***Інформаційна політика ООН*** 1. Основні напрями інформаційної політики ООН. 2. Просування України до інформаційного суспільства за відповідними критеріями ООН.	[2.1]
		самостійна робота	2	***Інформаційна політика міжурядових європейських організацій*** 1. Європейські інститути: тенденції міжнародних інформаційних відносин. 2. Міжнародний форум інформаційного суспільства Організації центральноєвропейська ініціатива.	[2.1]

1	2	3	4	5	6
				3. Інформаційна проблематика в діяльності ОБСЄ і НАТО.	
		самостійна робота	2	***Концепції державної інформаційної політики*** 1. Концепція національної інформаційної політики 2. Концепція розвитку державної інформаційної інфраструктури	[1.1-1.19], [2.1-2.3]
		індивідуальна робота	16	ІР – 1 Виконання вибіркового дослідницького завдання за заданою тематикою	[1.1-1.22], [2.1-2.5], [3.1-3.2]
		самостійна робота	2	***Визначення основних напрямів інформаційної політики ДПС Синіх у наступному календарному році.*** 1. Визначення основних суб'єктів інформаційних відносин в діяльності ДПС Синіх у наступному календарному році. 2. Визначення основних напрямів інформаційної політики ДПС Синіх у наступному календарному році.	[1.1-1.22], [2.1-2.5], [3.1-3.2]
2			**24**	**Стратегічні комунікації**	
	1	лекція	2	***Сутність та зміст стратегічних комунікацій*** 1. Поняття стратегічних комунікацій. 2. Основні компоненти стратегічних комунікацій за стандартами НАТО. 3. Завдання національної системи стратегічних комунікацій.	[2.2, 2.3],
		самостійна робота	2	***Стратегічні комунікації як інформаційний інструмент захисту та реалізації інтересів держави*** 1. Еволюція проблематики стратегічних комунікацій. 2. «Стратегічні комунікації» та «пропаганда»: проблемні аспекти сепарації. 3. Проблема визначення наративів стратегічних комунікацій.	[2.2, 2.3],
		самостійна робота	2	***Система формування іміджу організації*** 1. Основні поняття. 2. Зміцнення позитивного іміджу ДПСУ.	[2.2-2.4], [3.1-3.2]
	2	лекція	2	***Засоби масової інформації*** 1. Основні принципи взаємодії із засобами масової інформації. 2. Планування роботи зі ЗМІ. 3. Вирішення конфліктних ситуацій зі ЗМІ.	[2.2-2.4], [3.1-3.2]

1	2	3	4	5	6
		самостійна робота	2	***Співпраця ДПСУ з об'єднаннями громадян*** 1. Об'єднання громадян як цільова аудиторія стратегічних комунікацій. 2. Механізми співпраці з об'єднаннями громадян.	[2.2-2.4], [3.1-3.2]
		індивідуальна робота	14	**ІР – 2** Виконання вибіркового дослідницького завдання за заданою тематикою	[1.1-1.22], [2.1-2.5], [3.1-3.2]
Разом за ІІІ семестр			**54**	**з них 8 аудиторних занять, індивідуальної роботи – 30 год., самостійної роботи – 16 год.**	
IV семестр					
			36	**Інформаційна безпека**	
3	1	лекція	2	***Суспільно-психологічна характеристика інформаційного простору.*** 1. Когнітивні підходи до аналізу інформаційного простору. 2. Особливості захоплення і захисту інформаційного простору. 3. Інформаційно-комунікативні процеси в сучасних суспільствах.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Об'єкти та суб'єкти інформаційної безпеки 2. Види інформаційної безпеки	[2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Основні поняття та зміст категорій інформаційної безпеки держави. 2. Сутність та зміст загроз інформаційній безпеці держави.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Дестабілізуючі фактори інформаційної безпеки. 2. Класифікація загроз інформаційній безпеці. 3. Джерела загроз інформаційній безпеці.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	***Державне управління в умовах інформаційного суспільства.*** 1. Стратегічні, інформаційні і віртуальні потоки. 2. Стратегічні і тактичні , інформаційні та віртуальні потоки. 3. Управління масовою свідомістю та активністю населення в соціосистемах.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Основні принципи забезпечення інформаційної безпеки. 2. Система забезпечення інформаційної безпеки держави. Основні форми і способи забезпечення інформаційної безпеки	[1.1-1.2], [2.1-2.6], [3.1-3.4]

1	2	3	4	5	6
				держави.	
		самостійна робота	2	***Інформаційне протиборство і національна безпека.*** 1. Інформаційне протиборство та операції національної безпеки. 2. Пропаганда та комунікативні складники інформаційно-психологічної боротьби.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Інформаційна війна. 2. Інформаційний тероризм. 3. Інформаційна злочинність.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Визначення інформаційної війни. 2. Концепція інформаційної війни. 3. Органи інформаційної війни.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	1. Визначення форм інформаційної війни. 2. Основні форми інформаційної війни на державному рівні. 3. Основні форми інформаційної війни на воєнному рівні.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	***Інформаційні та віртуальні потоки в соціосистемах.*** 1. Військові дослідження проблем комунікації та мислення. 2. Підготовка спеціалістів у сфері інформаційного протиборства на пострадянському просторі.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		самостійна робота	2	***Інформаційне протиборство: сучасність.*** 1. Росія і Україна у співставленні їх комунікативних пропагандистських можливостей. 2. Особливості пропагандистських механізмів з двох боків російсько-українського конфлікту.	[1.1-1.2], [2.1-2.6], [3.1-3.4]
		індивідуальна робота	12	**ІР – 3** Виконання вибіркового дослідницького завдання за заданою тематикою	[1.1-1.2], [2.1-2.6],[3.1-3.4]
			28	**Основи кібернетичної безпеки**	
4	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]
		самостійна	2	***Національна система кібербезпеки, її структура та***	[1.1-1.3, 1.20]

1	2	3	4	5	6
		робота		***функціонування*** 1. Об’єкти кібербезпеки та кіберзахисту. Суб’єкти забезпечення кібербезпеки. 2. Об’єкти критичної інфраструктури. 3. Структура системи кібербезпеки.	
		самостійна робота	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	***Інформаційні системи, як об'єкти інформаційної безпеки*** 1. Інформація, її види та властивості. 2. Інформаційні системи як об'єкти захисту.	[1.3-1.7], [2.1]
		самостійна робота	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. Ранжирування джерел загроз. 2. Класифікація уразливостей безпеці. 3. Ранжирування уразливостей. 4. Класифікація актуальних загроз.	[1.7], [2.2, 2.3]
		самостійна робота	2	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	***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]

1	2	3	4	5	6
		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]
		індивідуальна робота	10	**ІР – 4** Виконання вибіркового дослідницького завдання за заданою тематикою	[1.1-1.20], [2.1-2.7],[3.1-3.4]
Диференційований залік			**2**		
Разом за IV семестр			**66**	**з них 6 аудиторних занять, індивідуальної роботи – 22 год., самостійної роботи – 38 год.**	
Разом за II курс			**120**	**з них 14 аудиторних занять, індивідуальної роботи – 52 год., самостійної роботи – 38 год.**	
Усього за дисципліну			**120**		

ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Перелік орієнтовних тем вибіркового дослідницького завдання:

1. Державне регулювання інформаційної сфери (телекомунікації, Інтернет, ЗМІ тощо).
2. Державне управління інформаційною сферою: зарубіжний і вітчизняний досвід.
3. Державна інформаційна політика в Україні.
4. Досвід Європейського Союзу щодо налагодження комунікацій влади з громадськістю.
5. Інтелектуальна власність в сфері інформаційної політики України
6. Побудова інформаційного суспільства в Україні: державно - управлінський аспект.
7. Інформаційна політика ООН.
8. Інформаційна структура сучасного суспільства.
9. Інформаційне суспільство: українські перспективи (теоретико-методологічні, практичні, правові, культурні аспекти).
10. Комунікації в органах Держприкордонслужби.
11. Комунікативна політика: зарубіжний і вітчизняний досвід.
12. Консультування з громадськістю.
13. Механізми забезпечення прозорості і відкритості Держприкордонслужби.
14. Преса в інформаційній політиці України.
15. Телебачення в інформаційній політиці України.
16. Пропаганда: відродження старого інструментарію в нових умовах.
17. Путінська пропаганда: методика роботи.
18. Російський тренд відродження СРСР.
19. Інформаційно-психологічні операції «Крим».
20. Інформаційно-психологічна операція «Новоросія».
21. Інформаційно-психологічна операція «Юго-восток» («Донбас»).
22. Інформаційно-психологічна операція «Україна», «Захід».
23. Помилки інформаційно-психологічної політики в період російсько-українського конфлікту.
24. Гібридна війна: інформаційно-психологічна складова.
25. Історико-політичні передумови російсько-українського протиборства.
26. Маси та масова свідомість у контексті суспільної еволюції.
27. Маси як соціально-психологічний та політичний феномен: історія і сучасність.
28. Психологія масових настроїв.
29. Методи впливу та прийоми управління масами.
30. Натовп: типологія натовпу.
31. Механізми та закономірності утворення натовпу, сценарії еволюції.
32. Масова комунікація і громадська думка.

33. Феномен чуток: фундаментальні та сприятливі фактори виникнення чуток.
34. Мода як масове соціально-психологічне явище.
35. Українські психологічні типи.
36. Порівняльна характеристика психології українців та інших етносів.
37. Європейські критерії безпеки інформаційних технологій.
38. Федеральні критерії безпеки інформаційних технологій.
39. Канадські критерії безпеки комп'ютерних систем.
40. Потенційні загрози безпеці та типові завдання захисту.
41. Політика безпеки.
42. Продукт інформаційних технологій.
43. Профіль захисту.
44. Проект захисту.

МЕТОДИ ФОРМУВАННЯ ТА КОНТРОЛЮ ДОСЯГНЕННЯ ПРОГРАМНИХ РЕЗУЛЬТАТІВ НАВЧАННЯ

Форми (методи) навчання: лекції (з використанням методів проблемного навчання і дослідницького методу), групові заняття (з використанням лекційного методу з елементами практичної роботи), самостійна робота, виконання індивідуальних завдань.

Форми оцінювання результатів навчання: усне опитування та доповіді на групових заняттях, групових вправах, тестування, захист практичних індивідуальних робіт. Вид семестрового контролю: диференційований залік.

Результати навчання	Зміст результатів навчання	Метод формування	Методи контролю досягнення
ПРН 4 Розробляти інформаційно-аналітичні матеріали, доповіді та інші службові (службово-бойові) документи.	**Знати:** зміст вимог нормативно-правових актів з питань ІП та ІБ; основні положення ІП та ІБ; основні принципи інформаційних відносин; основні принципи, напрями, механізми формування та реалізації державної інформаційної політики України; основні принципи взаємодії керівника організації із засобами масової інформації; основні напрями здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки; основи теорії інформаційної боротьби; основні поняття та зміст інформаційно-психологічного протиборства; **Розуміти:** комунікативної взаємодії структур ДПСУ з громадськістю; основні аспекти зарубіжного	Лекції, групові заняття (з використанням методів проблемного і дослідницького навчання та візуалізації), практична робота, групові вправи в рамках оперативно-тактичних задач, самостійна та індивідуальна робота. Навчання здійснюється через активну практичну діяльність.	Контроль досягнення ПРН 4 здійснюється за результатами виконання вибірково-го дослідницького завдання та усного опитування з теми №1, 2. В ході підсумкового контролю.

	досвіду регулювання інформаційної сфери; **Застосовувати:** методи і засоби забезпечення інформаційної безпеки; результати аналізу відповідної інформації щодо розв'язувати ситуаційні проблеми, які виникають в органах охорони державного кордону, у межах своєї; комунікативні та інформаційні технології у процесі підготовки, прийняття і впровадження управлінських рішень; нормативно-правові документи, що регулюють здійснення державної інформаційної політики в Україні; загальні методи забезпечення інформаційної безпеки України; громадську підтримку управлінських рішень шляхом участі у брифінгах, прес-конференціях, інших заходах для оприлюднення прийнятих рішень, їх донесення до широкого загалу; **Аналізувати:** стан забезпечення безпеки інформації та інформаційних ресурсів; основні напрямками здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки; **Синтезувати:** стан зв'язку із громадськістю з метою підтримки управлінських рішень шляхом участі у брифінгах, прес-конференціях, інших заходах для оприлюднення прийнятих рішень, їх донесення до широкого загалу.		
ПРН 5 Виявляти та прогнозувати ризики від впливу реальних та потенційних загроз безпеці державного кордону, обґрунтовувати заходи щодо їх мінімізації на місцевому рівні, застосовуючи технологію аналізу ризиків та кримінального аналізу.	**Знати:** основні поняття та зміст ІП та ІБ; основні принципи інформаційних відносин; основні принципи, напрями, механізми формування та реалізації державної інформаційної політики України; основні напрями здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки; основні поняття та зміст інформаційно-психологічного протиборства; **Розуміти:** шляхи уникнення конфлікту із засобами масової інформації. основні принципи і методи комунікативної взаємодії структур ДПСУ з громадськістю;	Досягається використання таких методів викладання і навчання - пояснювально-ілюстративний метод, метод проблемного викладу навчального матеріалу, активні методи навчання. Для ознайомлення та засвоєння навчального матеріалу використовуються також словесні, практичні та наочні методи з використанням новітніх мультимедійних та комп'ютерних технологій, робота з науковою літературою, джерелами і електронними ресурсами, методи організації самостійно роботи (розв'язання завдань, виконання проектів,	Контроль досягнення ПРН 4 здійснюється за результатами виконання вибірково-дослідницького завдання та усного опитування з теми № 3, 4. В ході підсумкового контролю.

	основні аспекти зарубіжного досвіду регулювання інформаційної сфери; основні проблеми сучасної інформаційної політики і розвитку інформаційного суспільства в Україні; **Застосовувати:** результати аналізу відповідної інформації щодо розв'язування ситуаційних проблем, які виникають в органах охорони державного кордону, у межах своєї; загальні методи забезпечення інформаційної безпеки України; інформаційно-психологічну складову інформаційної безпеки у оперативно-службовій діяльності; **Аналізувати:** основні стан забезпечення безпеки інформації та інформаційних ресурсів; основні напрямками здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки; **Синтезувати:** стан зв'язку із громадськістю з метою підтримки управлінських рішень шляхом участі у брифінгах, прес-конференціях, інших заходах для оприлюднення прийнятих рішень, їх донесення до широкого загалу. **Оцінювати:** рівень інформаційної безпеки держави; стан зв'язку із засобами масової інформації; стан інформованості громадськості про діяльність ДПСУ;	індивідуальних і творчих завдань тощо) та індивідуальна науково-дослідна робота тощо.	
ПРН 7 Виконувати функції управління (прийняття рішення, планування, організація, мотивація та контроль) прикордонною діяльністю в різних режимах функціонування та умовах обстановки.	**Знати:** зміст вимог нормативно-правових актів з питань ІП та ІБ; основні поняття та зміст інформаційної політики та інформаційної безпеки; основні положення інформаційної політики, інформаційної безпеки; основні принципи інформаційних відносин; основні принципи, напрями, механізми формування та реалізації державної інформаційної політики України; основні напрями здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки; основи теорії інформаційної боротьби; **Розуміти:**	Лекційний метод, метод проблемних ситуацій, групові вправи, практичні заняття, у тому числі в рамках оперативно-тактичних задач, виконання індивідуальних завдань, самостійна робота з навчальною літературою.	Контроль досягнення ПРН 7 здійснюється за результатами виконання практичних індивідуальних завдань. В ході підсумкового контролю.

	основні принципи і методи комунікативної взаємодії структур ДПСУ з громадськістю; основні аспекти зарубіжного досвіду регулювання інформаційної сфери; основні проблеми сучасної інформаційної політики і розвитку інформаційного суспільства в Україні; **Застосовувати:** методи і засоби забезпечення інформаційної безпеки; результати аналізу відповідної інформації щодо розв'язування ситуаційних проблем, які виникають в органах охорони державного кордону, у межах своєї компетенції; комунікативні та інформаційні технології у процесі підготовки, прийняття і впровадження управлінських рішень; загальні методи забезпечення інформаційної безпеки України; громадську підтримку управлінських рішень шляхом участі у брифінгах, прес-конференціях, інших заходах для оприлюднення прийнятих рішень, їх донесення до широкого загалу; інформаційно-психологічну складову інформаційної безпеки у оперативно-службовій діяльності; **Аналізувати:** основні стан забезпечення безпеки інформації та інформаційних ресурсів; основні напрямками здійснення державної інформаційної політики в Україні й забезпечення інформаційної безпеки; **Синтезувати:** стан зв'язку із громадськістю з метою підтримки управлінських рішень шляхом участі у брифінгах, прес-конференціях, інших заходах для оприлюднення прийнятих рішень, їх донесення до широкого загалу. **Оцінювати:** рівень інформаційної безпеки держави; стан зв'язку із засобами масової інформації; стан інформованості громадськості про діяльність ДПСУ;		

Оцінювання знань, вмінь та навичок слухачів здійснюється за методикою, визначеною «**Положенням** про систему поточного і підсумкового оцінювання

результатів навчання курсантів (слухачів, студентів) Національної академії Державної прикордонної служби україни імені Б. Хмельницького

Оцінювання індивідуальних завдань здійснюється диференційовано за традиційною (національною) шкалою. Меже бути застосована бальна оцінка для підвищення точності та об'єктивності оцінювання. Оформлення індивідуальних завдань здійснюється відповідно до вимог, визначених у джерелі Підготовка та оформлення індивідуальних завдань з навчальних дисциплін : методичні рекомендації / укладач Д. А. Купрієнко. – Хмельницький : Електронне видання ФПКК НАДПСУ, 2019. – 47 с.

Слухач може обрати тему реферату чи індивідуального завдання з переліку, або обґрунтовано запропонувати власну тему в контексті виконання курсової роботи (проекту) або кваліфікаційної випускної роботи, що узгоджується з викладачем, який веде навчальну дисципліну.

Під час оцінювання есе враховують:

здатність слухача критично й незалежно оцінювати наявні дані, погляди, позиції, аргументи;

здатність розуміти, оцінювати та встановлювати зв'язки між фактами та оцінками;

уміння висловлювати власні погляди, обґрунтовувати й доводити свої думки.

Шкала оцінювання індивідуальних завдань

За традиційною шкалою	За шкалою ECTS	За 100-бальною шкалою	Характеристика
5 (відмінно)	A	90…100 (відмінно)	Роботу виконано на високому науково-теоретичному рівні, грамотно та логічно викладено. Слухач успішно та творчо застосовує теоретичні знання на практиці. В методиці аналізу враховано достатню кількість факторів, шкали вимірювання побудовані адекватні параметру, який вимірюється, розрахунки проведені правильно, інтерпретація результатів аналізу здійснена правильно, що дозволило сформувати обґрунтовані висновки та рекомендації. Кожна складова оцінюється 25 балів.
4 (добре)	B	82…89 (дуже добре)	Робота виконана на високому науково-теоретичному рівні, але допущені несуттєві помилки. Слухач в основному успішно застосовує теоретичні знання на практиці. В методиці не враховано несуттєві факторів, шкали вимірювання побудовані в цілому адекватні параметру, який вимірюється, розрахунки проведені з помилками,, які не суттєво вплинули на результат оцінювання, інтерпретація результатів аналізу здійснена в цілому правильно, що дозволило сформувати в цілому обґрунтовані висновки та рекомендації.
	C	75…81 (добре)	Роботу виконано на достатньому науково-теоретичному рівні із несуттєвими помилками. Слухач в основному успішно застосовує теоретичні знання на практиці, мав окремі несуттєві труднощі. В методиці не враховано несуттєві факторів, шкали

За традиційною шкалою	За шкалою ECTS	За 100-бальною шкалою	Характеристика
			вимірювання побудовані в цілому адекватні параметру, який вимірюється, розрахунки проведені з помилками,, які не суттєво вплинули на результат оцінювання, інтерпретація результатів аналізу здійснена в цілому правильно, що дозволило сформувати в цілому обґрунтовані висновки та рекомендації.
3 (задовільно)	D	67…74 (задовільно)	У роботі є суттєві помилки і неточності. Слухач застосовує теоретичні знання на практиці в типових ситуаціях, мав окремі суттєві труднощі. В методиці не враховано суттєві факторів, шкали вимірювання не враховують суттєві складові параметру, який вимірюється, розрахунки проведені з помилками, які вплинули на результат оцінювання, інтерпретація результатів аналізу здійснена не достатньо обґрунтовано , що призвело до помилкових висновків та рекомендації.
	E	60…66 (достатньо)	Робота виконана в цілому правильно на рівні мінімальних критерії, допущені грубі помилки. Слухач з певними труднощами застосовує теоретичні знання на практиці в типових ситуаціях, мав помилки в роботі.
2 (незадовільно)	FX	35…49 (незадовільно з можливістю повторного складання)	Допущено велику кількість грубих помилок. Слухач не може застосовувати одержані знання на практиці.
	F	1…34 (незадовільно з обов'язковим повторним виконанням)	Індивідуальне завдання не виконано.

ПОЛІТИКА КУРСУ

Курс передбачає аудиторні заняття, індивідуальну роботу і роботу у складі групи, а також самостійне вивчення матеріалу з використанням консультації викладача.

Середовище навчання є творчим та відкритим.

Відвідування лекційних та групових занять у зборовий період є обов'язковим. Всі групові заняття оцінюються за результатами виконання індивідуальних завдань. Через поважні причини (наприклад, хвороба, міжнародне стажування) навчання може відбуватись в он-лайн формі за погодженням із керівни-ком курсу. Заняття, які слухач пропустив без поважних причин, відпрацьовуються за погодженням з викладачем.

Порушення кінцевих термінів подання роботи на перевірку та перескладання: Усі завдання, передбачені програмою, мають бути виконані у встановлені терміни.

Роботи, які здаються на перевірку із порушенням кінцевих термінів без поважних причин, оцінюються нижче на 10 балів (один рівень за національною шкалою).

Якщо здобувач вищої освіти був відсутній на заняттях, обов'язкових для оцінювання з будь-якої причини, він/вона відпрацьовують навчальні питання та завдання в часи самостійної підготовки та у встановлені викладачем терміни.

Під час навчання не допустимо порушення академічної доброчесності.

Забезпечення дотримання академічної доброчесності здобувачами вищої освіти (у т.ч. створення і забезпечення функціонування ефективної системи запобігання та виявлення академічного плагіату) є важливими складовими *системи забезпечення закладами вищої освіти якості освітньої діяльності та якості вищої освіти* (системи внутрішнього забезпечення якості)

Дотримання академічної доброчесності слухачами передбачає :

самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;

посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

дотримання норм законодавства про авторське право і суміжні права;

надання достовірної інформації про результати власної навчальної (наукової) діяльності, використані методики досліджень і джерела інформації.

Порушенням академічної доброчесності вважається:

обман – надання завідомо неправдивої інформації щодо власної діяльності. Формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;

академічний плагіат – оприлюднення (частково або повністю) х результатів, отриманих іншими особами, як результатів власного дослідження та/або відтворення опублікованих текстів інших авторів без зазначення авторства;

фабрикація – вигадування даних чи фактів, що використовуються в роботах;

фальсифікація – свідома зміна чи модифікація вже наявних даних;

списування – виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;

хабарництво – надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;

необ'єктивне оцінювання – свідоме завищення або заниження оцінки результатів навчання здобувачів освіти.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА
Нормативно-правові акти

До теми 1, 2:

1.1. Конституція України

1.2. Закон України «Про Державну прикордонну службу України»

1.3. Закон України «Про Державний кордон України»

1.4. Закон України «Про інформацію»

1.5. Закон України «Про друковані засоби масової інформації (пресу) в Україні»
1.6. Закон України «Про науково-технічну інформацію»
1.7. Закон України «Про захист інформації в автоматизованих системах»
1.8. Закон України «Про інформаційні агентства»
1.9. Закон України «Про державну таємницю»
1.10. Закон України «Про зв'язок»
1.11. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації»
1.12. Закон України «Про електронний цифровий підпис»
1.13. Закон України «Про телекомунікації»
1.14. Закон України «Про доступ до публічної інформації»
1.15. Закон України «Про захист персональних даних»
1.16. Закон України «Про авторське право і суміжні права»
1.17. Закон України «Про звернення громадян»
1.18. Закон України «Про інформаційні агентства»
1.19. Закон України «Про телебачення і радіомовлення»
1.20. Постанова Кабінету Міністрів України «Про заходи щодо подальшого забезпечення відкритості у діяльності органів виконавчої влади»
1.21. Указ Президента України «Про вдосконалення діяльності органів виконавчої влади з питань інформування населення»
1.22. Указ Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади»

До теми 3:
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

До теми 4:
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-ХП 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.

Базова

До теми 1, 2:

2.1. Макаренко Є.А. Європейська інформаційна політика: Монографія. – К.: Наша культура і наука, 200. – 368 с.
2.2. Почепцов Г. Сучасні інформаційні війни. – К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.
2.3. Почепцов Г.Г., Чукут С.А. Інформаційна політика. Навч.посіб. – К.: Вид-во «Знання», 2006. – 665 с.
2.4. Шинкарук О. М., Криворучко І. Я., Дем’янюк М. Б., Ставицький О. М. , Купрієнко Д. А. Корпоративна культура в системі управління персоналом

Державної прикордонної служби України. Навчальний посібник. – Хмельницький : Видавництво НАДПСУ, 2018. – 357 с.
2.5. Чукут С.А., Джига Т.В. Опорний конспект лекцій з курсу «Інформаційна політика в Україні». – К.: Вид-во НАДУ, 2007. – 72 с.

До теми 3:

2.1. Юдін О.К., Богуш В.М. Інформаційна безпека держави. – Харків: Консум, 2004. — 508 с.
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. 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.
2.4. Почепцов Г. Сучасні інформаційні війни. – К.: Вид. дім «Києво-Могилянська академія», 2015. 497 с.
2.5. Почепцов Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах. – К.: .: Вид. дім «Києво-Могилянська академія», 2016. 316 с.
2.6. 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.

До теми 4:

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.

Допоміжна

До теми 1, 2:

3.1. Методичні рекомендації працівникам прес-служб та офіцерам ДПСУ, уповноваженим до співпраці зі ЗМІ : Методичні рекомендації / Міжнародна організація з міграції. – Київ : 2014. – 91 с.
3.2. Зміцнення позитивного іміджу відділу прикордонної служби : Рекомендації та практичні поради / Міжнародна організація з міграції. – Київ : 2015. – 91 с.

До теми 3:

3.1. 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

До теми 4:

3.1. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. — М.: ИНФРА-М, 200ІЮ — 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

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ (ІНТРАНЕТІ)

До теми 1, 2:

1. Офіційний веб-портал ВРУ. – Режим доступу : http://rada.gov.ua
2. Наукова електронна бібліотека періодичних видань Національної академії наук України. – Режим доступу : http://dspace.nbuv.gov.ua/
3. Електронна бібліотека Національного інституту стратегічних досліджень при Президентові України. – Режим доступу : http://www.niss.gov.ua/catalogue/6/.
4. Електронна бібліотека інституту соціології Національної академії наук України. – Режим доступу : http://i-soc.com.ua/institute/el_library.php.
5. Електронна бібліотека “psylib” (психологія, філософія, релігія, культурологія, методологія та ін.). – Режим доступу : http://www.psylib.kiev.ua.
6. Державний комітет телебачення і радіомовлення України: http://www.sciptrb.gov.ua/
7. Державний комітет зв'язку та інформатизації України: http://www.stc.gov.ua/_info/
8. Інститут масової інформації: http://www.imi.com.ua
9. Кабінет Міністрів України: http://www.kmu.gov.ua/
10. Комітет Верховної Ради України з питань свободи слова та інформації: http://www.rada.gov.ua/svobodaslova/
11. Національний інститут стратегічних досліджень: http://www.niss.gov.ua
12. Національна рада України з питань телебачення і радіомовлення: http://www.nradatvr.kiev.ua/
13. Український центр економічних і політичних досліджень ім. Олександра Разумкова: http://www.uceps.com.ua

До теми 3:

1. Автоматизована електрона система навчання, режим доступу - http://10.241.24.9/.
2. Методичне забезпечення дисципліни «Інформаційна безпека», режим доступу - http://10.241.24.235/kaf18.

До теми 4:

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.