НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ОБОРОНИ УКРАЇНИ

Інститут стратегічних комунікацій

Кафедра інформаційної боротьби

ЗАТВЕРДЖУЮ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ІНФОРМАЦІЙНА БЕЗПЕКА
(код ВК 21)

Ступінь вищої освіти	бакалавр
Освітньо-професійна програма	Фізичне виховання і спорт у Збройних Силах
Галузь знань	01 Освіта/Педагогіка
Спеціальність	017 Фізична культура і спорт
Цикл	
Статус навчальної дисципліни:	вибіркова
Форма здобуття освіти:	очна (денна)
Мова навчання:	українська

Київ – 2024

Робоча програма навчальної дисципліни "Інформаційна безпека" каталогу вибіркових дисциплін розроблена за освітньо-професійною програмою "Фізичне виховання і спорт у Збройних Силах" першого (бакалаврського) рівня для підготовки курсантів за спеціальністю 017 "Фізична культура і спорт" спеціалізацією "Фізичне виховання і спорт у Збройних Силах".

Розробники програми:

Розглянуто і схвалено на засіданні кафедри інформаційної боротьби.
Протокол від "28" серпня 2024 року № 1.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td>Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма здобуття освіти</td></tr>
<tr><td rowspan="16">Кількість кредитів – 4 кредити ECTS.

Загальна кількість годин – 120 годин.

Для денної форми здобуття освіти: кількість навчальних занять під керівництвом викладача – 80 год. кількість годин самостійної роботи – 40 год.

Індивідуальні завдання – есе, колективний проект.</td><td>галузь знань:
01 Освіта/Педагогіка</td><td>вибіркова</td></tr>
<tr><td rowspan="5">Спеціальність:
017 Фізична культура і спорт

Спеціалізація:
Фізичне виховання і спорт у Збройних Силах</td><td>Рік підготовки:</td></tr>
<tr><td>4-й</td></tr>
<tr><td>Півріччя</td></tr>
<tr><td>7, 8</td></tr>
<tr><td></td></tr>
<tr><td rowspan="10">освітній ступінь – бакалавр</td><td>Лекції, год.</td></tr>
<tr><td>8</td></tr>
<tr><td>Семінарські заняття (круглий стіл), год.</td></tr>
<tr><td>14</td></tr>
<tr><td>Групові заняття, год.</td></tr>
<tr><td>20</td></tr>
<tr><td>Практичні заняття, год.</td></tr>
<tr><td>22</td></tr>
<tr><td>Групові вправи, год.</td></tr>
<tr><td>14</td></tr>
<tr><td>Самостійна робота, год.</td></tr>
<tr><td>40</td></tr>
<tr><td>Індивідуальні завдання:
2</td></tr>
<tr><td>Підсумковий контроль, год.:
Залік – 2</td></tr>
</table>

2. Мета та заплановані результати навчання

2.1. Метою вивчення навчальної дисципліни “Інформаційна безпека” є формування у курсантів теоретичних знань та практичних навичок щодо основ інформаційної безпеки, оволодіння методами захисту інформації, свідомого підходу до використання сучасних цифрових (інформаційних) технологій та навчання правилам безпеки в цифровому просторі.

2.2. Компетентності, які набуваються під час засвоєння навчальної дисципліни.

Під час засвоєння навчальної дисципліни курсантами набуваються компетентності:

здатність вчитися та оволодівати сучасними знаннями;

здатність працювати в команді;

здатність планувати та управляти часом;

здатність застосовувати знання у практичних ситуаціях;

здатність організовувати та підтримувати зв’язок у підрозділі штатними засобами зв’язку.

2.3. Заплановані результати навчання.

Згідно з вимогами освітньо-професійної програми визначені та сформульовані такі результати навчання:

показувати навички самостійної роботи, демонструвати критичне та самокритичне мислення;

засвоювати нову фахову інформацію, оцінювати й представляти власний досвід, аналізувати й застосовувати досвід колег;

спроможність використовувати штатні засоби зв’язку, які перебувають на озброєнні підрозділу для організації зв’язку;

організовувати заходи із захисту від засобів радіоелектронної боротьби противника під час підготовки та ведення бою.

Курсант повинен бути спроможний:

оцінювати можливості використання штатних засобів зв’язку, які перебувають на озброєнні підрозділу для організації зв’язку;

застосовувати набуті знання і навички та практично використовувати їх в умовах ведення бойових дій.

3. СТРУКТУРА ТА ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

3.1. Структура навчальної дисципліни

Номери та назви тем	Усього годин	З них		У т. ч. за видами навчальних занять					Індивідуальні завдання	Контрольні заходи
		Навчальних занять	Самостійна робота	Лекції	Семінарські заняття, (круглі столи)	Групові заняття	Практичні заняття	Групові вправи		
1	2	3	4	5	6	7	8	9	10	11
4 курс										
І півріччя										
Тема 1. Теоретичні основи забезпечення інформаційної безпеки держави	30	20	10	2	4	12	2			
Тема 2. Виклики та загрози інформаційній безпеці держави	30	20	10	2	4	4	10			
Всього за І півріччя	**60**	**40**	**20**	**4**	**8**	**16**	**12**			
ІІ півріччя										
Тема 3. Інформаційна безпека військовослужбовця	26	18	8	2	2	4	10			
Тема 4. Колективний проект. Розроблення пропозицій щодо протидії інформаційним загрозам	30	20	10	2	4			14		
Залік	**4**	**2**	**2**							**2**
Всього за ІІ півріччя	**60**	**40**	**20**	**4**	**6**	**4**	**10**	**14**		**2**
Всього за 4 курс	**120**	**80**	**40**	**8**	**14**	**20**	**22**	**14**		**2**
Всього за навчальну дисципліну	**120**	**80**	**40**	**8**	**14**	**20**	**22**	**14**		**2**

3.2. Зміст навчальної дисципліни

№ з/п	Вид навчального заняття	Кількість годин	Із них		Півріччя (курс навчання), номери та назва тем і навчальних занять, навчальні питання заняття, завдання для самостійної роботи	Матеріально-технічне забезпечення	Рекомендована література
			Навчальних занять під керівництвом викладача	Самостійної роботи			
1	2	3	4	5	6	7	8
		60	**40**	**20**	**І півріччя 4 курсу**		
		30	**20**	**10**	**Тема 1. Теоретичні основи забезпечення інформаційної безпеки держави.**		
1.	Л (Б)	2	2		*Тема 1. Заняття 1.* **Інформаційна безпека держави: сутність та складові**. 1. Інформаційна безпека: ключові визначення та поняття 2. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Самостійна робота:* Вивчення Стратегії інформаційної безпеки України.	ПЕОМ, проектор, тощо	[1, 2, 3-10]
2.	ГЗ	6	4	2	*Тема 1. Заняття 2*. **Інформаційна безпека в умовах російсько-української війни.** 1. Основні напрями забезпечення інформаційної безпеки в умовах російсько-української війни. 2. Стратегічні цілі та пріоритети забезпечення інформаційної безпеки держави з урахуванням досвіду російсько-української війни. *Самостійна робота:* Вивчення Закону України “Про інформацію”.	ПЕОМ, проектор, тощо	[1, 2, 3-10]

3.	ГЗ	6	4	2	*Тема 1. Заняття 3.* **Система забезпечення інформаційної безпеки держави**. 1. Складові системи забезпечення інформаційної безпеки держави. 2. Завдання та повноваження суб'єктів забезпечення інформаційної безпеки. *Самостійна робота:* Дублювання повноважень в системі забезпечення інформаційної безпеки та шляхи вирішення проблеми.	ПЕОМ, проектор, тощо	[1, 2, 3-10, 11]
4.	ГЗ	6	4	2	*Тема 1. Заняття 4.* **Кібербезпека як складова інформаційної безпеки держави**. 1. Сутність поняття кібербезпеки держави. 2. Виклики та загрози в сфері кібербезпеки держави з урахуванням досвіду російсько-української війни. *Самостійна робота:* Стратегія кібербезпеки України	ПЕОМ, проектор, тощо	[1, 2, 3-10, 11, 12]
5.	ПЗ	4	2	2	*Тема 1. Заняття 5.* **Інформаційна безпека Збройних Сил України**. 1. Система забезпечення інформаційної безпеки Збройних Сил України. 2. Механізми забезпечення інформаційної безпеки Збройних Сил України. *Самостійна робота:* Зарубіжний досвід забезпечення інформаційної безпеки Збройних Сил.	ПЕОМ, проектор, тощо	[2, 3-10, 14, 15]
6.	КС	6	4	2	*Тема 1. Заняття 6.* **Ключові напрями удосконалення забезпечення інформаційної безпеки держави в умовах російсько-української війни.** 1. Основні недоліки функціонування системи забезпечення інформаційної безпеки держави та шляхи їх подолання. 2. Шляхи удосконалення нормативно-правової бази з забезпечення інформаційної безпеки України в умовах РУВ гібридної війни. *Самостійна робота:* Повторення пройденого матеріалу за першою темою.	ПЕОМ, проектор	[1, 2, 5-10, 15, 16]
		30	**20**	**10**	**Тема 2. Виклики та загрози інформаційній безпеці держави.**		
7.	Л	2	2		*Тема 2. Заняття 1*. **Сучасні виклики та загрози інформаційній безпеці держави.** 1. Визначення та сутність загроз інформаційній безпеці України. 2. Характеристика основних загроз інформаційній безпеці України в	ПЕОМ, проектор	[2, 5-10, 15, 16]

					умовах російсько-української війни. *Самостійна робота:* Відображення загроз інформаційній безпеці України в чинному законодавстві.		
8.	ГЗ	6	4	2	*Тема 2. Заняття 2*. **Національний інформаційний простір**. 1. Поняття національного інформаційного простору, його складові. 2. Інформаційний простір як середовище поширення інформаційних загроз. *Самостійна робота*: механізми конструювання інформаційного простору.	ПЕОМ, проектор	[5-10, 15-26]
9.	ПЗ	4	2	2	*Тема 2. Заняття 3*. **Внутрішні інформаційні загрози.** 1. Інформаційні загрози в різних сферах життєдіяльності суспільства. 2. Виявлення джерел внутрішніх інформаційних загроз. *Самостійна робота:* способи нейтралізації внутрішніх інформаційних загроз.	ПЕОМ, проектор	[5-10, 15-26]
10.	ПЗ	6	4	2	*Тема 2. Заняття 4*. **Зовнішні інформаційні загрози.** 1. Джерела зовнішніх інформаційних загроз з урахуванням досвіду російсько-української війни. 2. Оцінювання зовнішніх інформаційні загрози державі в умовах російсько-української війни. *Самостійна робота:* способи нейтралізації зовнішніх інформаційних загроз.	ПЕОМ, проектор	[5-12, 15-28]
11.	ПЗ	6	4	2	*Тема 2. Заняття 5*. **Витік інформації як загроза національній безпеці держави.** 1. Поняття та канали витоку інформації. 2. Методи та засоби захисту від витоку інформації. *Самостійна робота*: види інформації відповідно до чинного законодавства та особливості роботи з нею.	ПЕОМ, проектор	[5-12, 15-28]
12.	С	6	4	2	*Тема 2. Заняття 6*. Проблеми оцінювання інформаційних загроз державі в умовах російсько-української війни. 1. Критерії оцінювання інформаційних загроз. 2. Способи протидії інформаційним загрозам в умовах російсько-української війни. *Самостійна робота*: підготовка есе за обраною темою.	ПЕОМ, проектор	[1-12, 15-30]

		60	**40**	**20**	**ІІ півріччя**		
		26	18	8	**Тема 3. Інформаційна безпека військовослужбовця.**		
13.	Л	2	2		*Тема 3. Заняття 1.* **Інформаційна безпека військовослужбовців в умовах російсько-української війни**. 1. Когнітивна складова російсько-української війни. 2. Сутність та зміст поняття інформаційної безпеки військовослужбовця. *Самостійна робота:* Зарубіжний досвід забезпечення когнітивної безпеки військовослужбовців у країнах-членах НАТО.	ПЕОМ, проектор	[1-12, 15-30]
14.	ГЗ	5	4	1	*Тема 3. Заняття 2.* **Деструктивні інформаційні впливи в умовах російсько-української війни.** 1. Деструктивні інформаційні впливи на військовослужбовців ЗС України в умовах російсько-української війни. 2. Механізми захисту військовослужбовців ЗС України від деструктивних інформаційних впливів. *Самостійна робота:* Ключові наративи російської пропаганди та дезінформації.	ПЕОМ, проектор	[1-12, 15-30]
15.	ПЗ	6	4	2	*Тема 3. Заняття 3.* **Інформаційна безпека військовослужбовців у соціальних мережах**. 1. Приклади дослідження соціальних мереж військовослужбовцями. 2. Механізми забезпечення інформаційної безпеки військовослужбовців під час використання соціальних мереж. *Самостійна робота*: алгоритми роботи соціальних мереж.	ПЕОМ, проектор	[15-30]
16.	ПЗ	6	4	2	*Тема 3. Заняття 4.* **Медіа та інформаційна грамотність військовослужбовців**. 1. Способи аналізу понять медіа, інформаційна та цифрова грамотність. 2. Доповідь висновків з аналізу понять медіа, інформаційна та цифрова грамотність. інформаційний простір, інформаційна бульбашка та механізми її формування. *Самостійна робота*: підходи щодо свідомого споживання інформації.	ПЕОМ, проектор	[15-40]

17.	ПЗ	3	2	1	*Тема 3. Заняття 5.* **Способи пошуку та перевірки інформації.** 1. Пошук та перевірка текстової інформації. 2. Пошук та перевірка аудіо та відео файлів. *Самостійна робота*: використання інструментів ШІ для пошуку, перевірки та створення інформації.	ПЕОМ, проектор	[15-30, 40, 42, 45]
18.	С	4	2	2	*Тема 3. Заняття 6.* **Проблеми забезпечення інформаційної безпеки військовослужбовців Збройних Сил України в умовах російсько-української війни.** 1. Особливості забезпечення інформаційної безпеки Збройних Сил України в умовах російсько-української війни. 2. Шляхи удосконалення інформаційної безпеки військовослужбовців Збройних Сил України. *Самостійна робота*: опрацювання пройденого матеріалу за третьою темою.	ПЕОМ, проектор	[25-40, 43, 44]
		30	20	10	**Тема 4. Колективний проект. Розроблення пропозицій командира тактичного рівня щодо протидії інформаційним загрозам.**		
19.	Л (Б)	2	2		*Тема 4. Заняття 1.* **Постановка завдання на підготовку колективного проекту**. 1. Приклад підготовки колективного проєкту з виявлення і протидії інформаційним загрозам. Вручення завдань. 2. Методика підготовки колективного проекту з виявлення і протидії інформаційним загрозам. *Самостійна робота:* особливості моніторингу інформаційного простору.	ПЕОМ, проектор	[40, 42, 45-50]
20.	ГВ	6	4	2	*Тема 4. Заняття 2.* **Моніторинг інформаційного простору та виявлення інформаційних загроз**. 1. Особливості моніторингу інформаційного простору в інтересах виявлення інформаційних загроз. 2. Формування актуального переліку інформаційних загроз *Самостійна робота:* моніторинг інформаційного простору.	ПЕОМ, проектор	[40, 42, 45-52]
21.	ГВ	6	4	2	*Тема 4. Заняття 3.* **Оцінювання інформаційних загроз**. 1. Критерії оцінювання інформаційних загроз. 2. Методика оцінювання інформаційних загроз.	ПЕОМ, проектор	[40, 42, 45-52]

					Самостійна робота: моніторинг інформаційного простору.		
22.	ГВ	6	4	2	*Тема 4. Заняття 4.* **Прогнозування сценаріїв розвитку інформаційних загроз.** 1. Розробка сценаріїв інформаційних загроз. 2. Вибір найбільш імовірного варіанту розвитку ситуації. *Самостійна робота:* моніторинг інформаційного простору.	ПЕОМ, проектор	[40, 42, 45-52]
23.	ГВ	4	2	2	*Тема 4. Заняття 5.* **Вироблення шляхів протидії інформаційних загроз**. 1. Способи реагування на інформаційні загрози. 2. Вироблення механізму реагування на виявлені інформаційні загрози. *Самостійна робота:* моніторинг інформаційного простору.	ПЕОМ, проектор	[40, 42, 45-62]
24.	КС	6	4	2	*Тема 4. Заняття 6.* **Захист колективного проекту**. 1. Представлення результатів колективного проекту. 2. Обговорення переваг та недоліків *Самостійна робота:* підготовка до заліку.	ПЕОМ, проектор	[40, 42, 43, 45-62]
25.	Залік	4	2	2	Залік.	Комплект тестів	Література згідно тем.
Усього за навчальну дисципліну		**120**	**80**	**40**	Л – 8 год., С (КС) – 14 год., ГЗ – 20 год., ГВ – 14 год., ПЗ – 22 год., Залік – 2 год.		[1-65]

4. Індивідуальні завдання

Робочою програмою навчальної дисципліни передбачено такі індивідуальні завдання: есе.

5. Методи навчання

У ході вивчення дисципліни використовуються такі методи навчання:

1. За джерелом інформації:

словесні: лекція (традиційна, проблемна тощо) із застосуванням комп'ютерних інформаційних технологій (презентація PowerPoint), семінари, пояснення;

наочні: ілюстрація, демонстрація;

практичні: задачі, вправи.

2. За логікою передачі і сприйняття навчальної інформації: індуктивні, дедуктивні, аналітичні, синтетичні.

3. За ступенем самостійності мислення: репродуктивні, пошукові, дослідницькі.

4. За ступенем керування освітньою діяльністю: під керівництвом викладача; самостійна робота курсантів із науковим матеріалом; самостійне розв'язання додаткових задач підвищеної складності.

6. Контроль успішності навчання

Протягом навчання проводяться такі види контролю: поточний, самоконтроль, підсумковий.

Формами контролю знань є: усне та письмове опитування, тестові завдання (у тому числі, комп'ютерне тестування), захист стажування (практики), есе, реферат, екзамен, захист кваліфікаційної роботи магістра.

Поточний контроль проводиться під час всіх видів занять у формі: контрольних опитувань, летючок, співбесід з окремих питань. Засоби поточного контролю: тестові завдання, виступи на семінарах, круглих столах, групових заняттях.

Підсумковий контроль за навчальну дисципліну проводиться у формі заліку.

7. Критерії оцінювання результатів навчання

Рейтингова оцінка навчальної дисципліни.

Рейтингова оцінка навчальної дисципліни **(R)** формується як сума всіх рейтингових балів курсанта:

денна форма здобуття освіти:

за відповіді на групових заняттях **($R_{ГЗ}$)** та групових вправах **($R_{ГВ}$)**, виконання завдань на практичних заняттях **($R_{ПЗ}$)**, виконання індивідуального завдання **($R_{ІЗ}$),** складання заліку $R_{ДЗ}$:

$$R = R_{ГЗ} + R_{Гв} + R_{ПЗ} + R_{ІЗ} + R_{ДЗ}$$

Для визначення оцінки за національною шкалою рейтингова оцінка (в балах) навчальної дисципліни (R) переводиться згідно з таблицею:

Значення R	**Оцінка за національною шкалою**
90 – 100	“відмінно”
80 – 89	“дуже добре”
65 – 79	“добре”
55 – 64	“задовільно”
50 – 54	“достатньо”
1 – 49	“незадовільно” з можливістю повторного складання

Результати заліку оцінюються в діапазоні від 0 до 100 балів. В разі, коли відповіді за всі завдання курсанта оцінені менше ніж в 50 балів, він отримує незадовільну оцінку за результатами заліку. Курсант має 2 можливості повторно скласти залік, при цьому для другої спроби, рішенням начальника кафедри, створюється комісія кафедри.

Критерії оцінювання заліку:

90 – 100 – курсант має глибокі, міцні і систематичні знання всіх положень теорії, може не тільки вільно сформулювати, але й самостійно застосовує здобуті знання і вміння в нестандартних ситуаціях, здатний вирішувати проблемні питання. Відповідь курсанта відрізняється точністю формулювань, логікою, достатнім рівнем узагальненості знань.

80 – 89 – курсант знає і може самостійно сформулювати основні визначення та пов'язати їх з реальними явищами, може привести вербальне формулювання основних положень теорії, навести приклади їх застосування в практичній діяльності. Курсант може самостійно застосовувати знання в стандартних ситуаціях, його відповідь логічна.

65 – 79 – курсант знає і може самостійно сформулювати основні визначення та пов'язати їх з реальними явищами, може привести вербальне формулювання основних положень теорії, навести приклади їх застосування в практичній діяльності, але не завжди може їх обґрунтувати. Курсант може самостійно застосовувати знання в стандартних ситуаціях, його відповідь логічна, але розуміння не є узагальненим.

55 – 64 – курсант володіє більшою частиною навчального матеріалу, але викладає його не досить послідовно і логічно, не завжди вміє інтегровано

застосувати набуті знання для аналізу конкретних ситуацій, нечітко формулює основні теоретичні положення та причинно-наслідкові зв'язки.

50 – 54 – курсант володіє більшою частиною навчального матеріалу, але викладає його не досить послідовно і логічно, допускає істотні пропуски у відповіді, не завжди вміє інтегровано застосувати набуті знання для аналізу конкретних ситуацій, нечітко, а інколи й невірно формулює основні теоретичні положення та причинно-наслідкові зв'язки.

1 – 49 – відповідь курсанта при відтворенні навчального матеріалу елементарна, фрагментарна, зумовлена нечіткими уявленнями про систему інформаційної безпеки. У відповіді цілком відсутня самостійність.

Під час визначення рейтингової оцінки навчальної дисципліни **(R),** отримані бали за залік враховуються з коефіцієнтом 0,4.

Розподіл балів, які отримують курсанти:

Максимальна/мінімальна оцінка в балах							
Поточне оцінювання та самостійна робота						Залік	Всього
У тому числі за темами				Есе	Всього		
Тема 1	Тема 2	Тема 3	Тема 4				
15	15	15	15	10	70	30	100

Умови допуску до заліку

Курсант допускається до заліку, якщо він до підсумкового контролю ліквідував заборгованість за всіма видами робіт, які передбачені індивідуальним навчальним планом (робочою програмою навчальної дисципліни) та набрав не менше ніж 50 % балів (30 балів) від суми рейтингових балів контрольних заходів протягом вивчення тем навчальної дисципліни.

Курсант який набрав протягом вивчення тем навчальної дисципліни та виконання індивідуального завдання рейтингову оцінку менше за 50 % від максимальної кількості балів (30 балів), до заліку не допускається.

8. Методичне забезпечення

8.1. Методичне забезпечення навчальної дисципліни включає:

8.1.1. Конспект опорних лекцій всіх тем курсу.

8.1.2. Організаційно-методичні вказівки щодо відпрацювання курсових робіт (рефератів, есе).

8.2. Варіанти індивідуальних завдань.

8.2.1. Перелік типових тем для написання курсантами есе.

1. Роль і місце інформаційної безпеки військовослужбовця в системі забезпечення національної безпеки держави.
2. Міфодизайн та конструювання інформаційного простору в умовах широкомасштабної збройної агресії росії проти України.

8.3. Перелік типових питань для проведення підсумкового контролю:

Перше питання:

1. Особливості управління інформаційним простором Збройних Сил України.
2. Визначення та сутність інформаційної безпеки в сучасному світі.
3. Визначення та сутність загроз інформаційній безпеці України.
4. Фізичний, когнітивний та віртуальний виміри інформаційного простору.
5. Основні чинники, що впливають на систему управління інформаційним простором.
6. Сутність та зміст інформаційної політики держави.
7. Особливості реалізації інформаційної політики держави в умовах особливого періоду.
8. Суб'єкти забезпечення інформаційної безпеки України.
9. Організація скоординованої роботи різних суб'єктів забезпечення інформаційної безпеки України.
10. Сутність комунікативних кампаній ЗС України.

Друге питання:

1. Основні етапи підготовки інформаційної кампанії Збройних Сил України.
2. Сутність та зміст завдань моніторингу інформаційного простору в процесі підготовки інформаційної кампанії Збройних Сил України.
3. Основні завдання та функції суб'єктів забезпечення кібербезпеки України.
4. Особливості визначення цільових аудиторій та підготовки меседжів інформаційної кампанії Збройних Сил України.
5. Єдиний інформаційний простір у сфері оборони та його складові.
6. Організація системи моніторингу інформаційного простору, виявлення та оцінювання складових загальної проблеми.
7. Особливості підготовки і ведення інформаційної кампанії Збройних Сил України.
8. Характеристика напрямів забезпечення кібербезпеки України.
9. Проблемні питання підготовки і ведення інформаційних кампаній Збройних Сил України.
10. Кризові ситуації в інформаційному просторі.

Рекомендована література

1. Військова концепція стратегічних комунікацій НАТО від 18 серпня 2010 року. DSG (2010) 0528.

2. Військовий стандарт 01.004.004 (Видання 1) Воєнна політика, безпека та стратегічне планування: Інформаційна безпека держави у воєнній сфері. Київ : ЦУМС Збройних Сил України, 2014.

3. Військово-політичні вказівки щодо формування та реалізації воєнної політики в Міністерстві оборони України та у Збройних Силах України в 2017 році, 2018 та двох наступних роках, 683дск від 13.12.2016 року.

4. Директива Генерального штабу Збройних Сил України від 02.09.2016 р. № Д-20 "Про організацію стратегічних комунікацій у Збройних Силах України".

5. Доктрина з інформаційної операції Збройних Сил України, затверджена Наказом Генерального штабу Збройних Сил України від 30.12.2020 р. № 262/НВГШ.

6. Доктрина з психологічних операцій Збройних Сил України, затверджена Наказом Генерального штабу Збройних Сил України від 25.05.2021 р. № 74/НВГШ.

7. Доктрина ЗС США JP 3-12 Cyberspace Operations, 8 June 2018.

8. Доктрина ЗС США JP 3-13.3 Operations Security, 04 January 2015.

9. Доктрина об'єднаних сил НАТО щодо інформаційних операцій AJP-10.1. Edition A Version 1. Січень 2023 року.

10. Закон України "Про військово-цивільні адміністрації" від 3 лютого 2015 року № 141-VIII.

11. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 5 липня 1994 року № 80/94-ВР.

12. Закон України "Про інформацію" від 2 жовтня 1992 року № 2657-XII.

13. Закон України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII.

14. Закон України "Про оборону України" № 1932-XII від 6 грудня 1991 року.

15. Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року № 2163-VIII.

16. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки" від 9 січня 2007 року № 537-V.

17. Закон України "Про правовий режим воєнного стану" від 12 травня 2015 року № 389-VIII.

18. Збірник № 3 матеріалів вивчення бойового досвіду російсько-української війни 2022 року. К.: ГУДтаП ГШ Збройних Сил України. – 179 арк.

19. Збірник № 4 матеріалів вивчення бойового досвіду російсько-української війни 2022 року. Київ : ГУДтаП ГШ Збройних Сил України. 224 арк.

20. Зеленін В. В. Основи міфодизайну. Психотехнології керування медіареальністю. Навчально-метолічний посібник. Київ : Вид-во "Гнозіс", 2017. 168 с.

21. Інформаційна безпека держави у воєнній сфері: Навч. посібник / В. О. Кацалап. Київ : НУОУ, 2020. 301 с.

22. Інформаційна безпека та кібербезпека держави: навчальний посібник / [Н. М. Титова, Н. М. Рідей, В. П. Настрадін, М. М. Присяжнюк, С. М. Мамченко, С. В. Артюх, Р. О. Яворська]; за заг. ред. М. М. Присяжнюка. Київ : Видавництво Ліра-К, 2024. 224 с.

23. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чховська та ін.; під. ред. В. В. Остроухова. Київ : Видавництво Ліра-К, 2021. 412 с.

24. Кацалап В.О. Планування інформаційної операції за стандартами НАТО: навч. посіб. / В. О. Кацалап, Ю. В. Цурко. Київ : НУОУ, 2021. 160.

25. Кацалап В.О., Прима М.В., Рахімов В.В. Метод моніторингу інформаційного простору воєнної сфери в інтересах забезпечення дій військ (сил)// Сучасні інформаційні технології у сфері безпеки і оборони, № 38 (2), 2020. [Електронний ресурс] Режим доступу: https://sit.nuou.org.ua/article/view/207647

26. Конституція України.

27. Концепція забезпечення інформаційної безпеки Міністерства оборони України та Збройних Сил України, затверджена Наказом Міністерства оборони України № 10 від 10.01.2014 р.

28. Концепція інформаційної операції Збройних Сил України, затверджена спільним Наказом Міністерства оборони України та Збройних Сил України № 948 від 31.12.2014 р.

29. Концепція стратегічних комунікацій Міністерства оборони України та Збройних Сил України, затверджена Наказом Міністерства оборони України від 22 листопада 2017 року № 612.

30. Меленко О.С. Стратегічні комунікації і комунікативні стратегії: еволюція співвідношення / Юридичний науковий електронний журнал, 2023// [Електронний ресурс]. Режим доступу: http://www.lsej.org.ua/2_2023/168.pdf

31. Меленко О.С. Стратегічні комунікації як правова категорія / О. С. Меленко // Правова система: теорія і практика [Електронний ресурс]. Режим доступу: http://www.sulj.oduvs.od.ua/archive/2023/3/15.pdf

32. Методи експертних оцінок: теорія, методологія, напрямки використання: монографія/ Б.Є. Грабовецький. Вінниця : ВНТУ, 2010. 171 с.

33. Микусь С.А., Мацько О.Й., Войтко О.В. та ін. Бойовий досвід з питань інформаційної безпеки отриманий під час російсько-української війни. Частина перша (лютий 2014 – березень 2022 року) : збірник інформаційно-аналітичних матеріалів. Київ : НУОУ, 2022. 135 с.

34. Микусь С.А., Мацько О.Й., Войтко О.В. та ін. Бойовий досвід з питань кібербезпеки отриманий під час російсько-української війни (аналіз та уроки). Частина перша (січень – травень 2022 року) : збірник інформаційно-аналітичних матеріалів. Київ : НУОУ, 2022. 90 с.

35. Наказ Генерального штабу Збройних Сил України від 07.10.2016 р. № 374 “Про затвердження Інструкції з реалізації стратегічних комунікацій у Збройних Силах України”.

36. Основи забезпечення інформаційної безпеки держави у воєнній сфері: навч. посібник / О.В.Войтко, С.А.Микусь, К.В.Єргідзей. Київ : НУОУ ім. І. Черняховського, 2022. 400 с.

37. Основи стратегічних комунікацій у сфері забезпечення національної безпеки та оборони: навч. посіб. Київ : НУОУ імені Івана Черняховського, 2020. 86 с.

38. Планування психологічної операції за стандартами НАТО : навч. посіб. / О. В. Войтко. Київ : НУОУ, 2024. 280 с.

39. Почепцов Г.Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії / Георгій Георгійович Почепцов. Харків : Віват, 2022. 384 с.

40. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28 грудня 2021 року № 685/2021.

41. Публікація ЗС США JP 3-13.4 Military Deception, 26 January 2018.

42. Публікація НАТО Bi-SC NATO Information Operation Reference Book, 05 May 2020.

43. Публікація НАТО CJCSI 3370.01A Target Development Standards.

44. Публікація НАТО NATO Operations Assessment Handbook, 01 July 2015.

45. Публікація СВ США ATP 2-01.3 Intelligence Preparation of the Battlefield, March 2019.

46. Публікація СВ США Cyberspace and Electronic Warfare Operations, 11 April 2017.

47. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017.

48. Словник основних термінів у галузі інформаційної безпеки держави у воєнній сфері. Київ : НУОУ, 2014.

49. Стороженко Л., Петькун С. (2021). Стратегічні комунікації: концептуальні підходи та базові принципи. Society. Document. Communication. Соціум. Документ. Комунікація, (11), 386-403. https://doi.org/10.31470/2518-7600-2021-11-386-403.

50. Стратегічні комунікації в міжнародних відносинах. Монографія. Київ : Вадекс, 2019. 442 с.

51. Стратегічні комунікації: [словник] / Т. В. Попова, В. А. Ліпкан / за заг. ред. В. А. Ліпкана. Київ : ФОП О. С. Ліпкан, 2016. 400 с.

52. Стратегія воєнної безпеки України : Указ Президента України № 121/2021 від 25 березня 2021 року "Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України".

53. Теорія та практика проведення сучасного інформаційно-психологічного протиборства : навчальний посібник / В. М. Петрик, В. В. Бедь, М. М. Присяжнюк, та ін.; за заг. ред. В. В. Бедь, В. М. Петрика. Київ : ПАТ "ВІПОЛ", 2019. 400 с.

54. Ткаченко А.Л., Пилипчук Ю.В., Троцько Л.Г. Інформаційний вплив та його складові // Інформаційний вимір гібридної війни: досвід України: матеріали міжнародної науково-практичної конференції. Київ : НУОУ ім. Івана Черняховського, 2017. С. 89–55. [Електронний ресурс]. Режим доступу: https://nuou.org.ua/assets/documents/zbirn-gibr-mizhn-konf.pdf

55. Указ Президента України від 14 вересня 2020 року № 392/2020 "Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України".

56. Указ Президента України від 17 вересня 2021 року № 473/2021"Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України".

57. Указ Президента України від 25 березня 2021 року № 121/2021 "Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України".

58. Указ Президента України від 25 лютого 2017 року № 47/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України".

59. Указ Президента України від 26 серпня 2021 року № 447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України".

60. Flood Andrew and Keegan J. Richard Cognitive resilience to Psyhological Stress in Military Personnel. Frontiers in Psyhology, March 2022.

61. 4. Bartone, P. T. (2006). Resilience under military operational stress: can leaders influence hardiness? Mil. Psychol. 18, P. 131–148. doi: 10.1207/ s15327876mp1803s_10

62. 5. Wiederhold, B. K., and Wiederhold, M. D. (2008). Virtual reality for posttraumatic stress disorder and stress inoculation training. J. Cyber Ther. Rehabil. 1, 23–35.

63. Управління інформаційним простором Збройних Сил України : курс лекцій / [М.В.Авраменко, В.О.Кацалап, Ю.І.Міхеєв, В.В.Наместнік, Ю.Б.Прібилєв]. Київ: НУОУ, 2024. 30 с.

Розробник: