НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Інформаційна безпека»

Освітня програма	«Кіберзахист інформаційних ресурсів»
Рівень вищої освіти	перший (бакалаврський)
Форма навчання	денна
Статус навчальної дисципліни	обов'язкова
Мова викладання	українська

КИЇВ – 2024

Робочу програму навчальної дисципліни розглянуто та затверджено на засіданні КІБД ННІ ІБ СК НА СБ України від «14» 10 2024 року, протокол № 11.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	3
Семестр (и)	5
Обсяг *(кредити ЄКТС/години)*	4/120
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
семінарські заняття (СЗ)	16
практичні заняття (ПЗ)	14
лабораторні заняття (ЛЗ)	
індивідуальні завдання (ІЗ)	
самостійна робота (СР)	60
форма підсумкового контролю *(семестр)*	екзамен

2. Мета та завдання навчальної дисципліни

2.1. Мета – набуття здобувачами освіти компетенцій, знань, умінь і навичок для подальшого використання у практичній діяльності із забезпечення інформаційної безпеки.

Завдання:

Основними завданнями вивчення дисципліни «Інформаційна безпека» є:

- отримання базових знань з концептуальних засад інформаційної безпеки;
- отримання знань щодо основних загроз інформаційній безпеці;
- здобуття знань щодо комплексу завдань з управління у сфері інформаційної безпеки, методів, заходів та засобів щодо їх реалізації на різних організаційних рівнях;
- отримання знань щодо загальних форм та методів попередження та припинення діяльності на шкоду безпеці держави в інформаційній сфері;
- здобуття практичних навичок з виявлення ознак маніпулювання, СІО та СІА;
- формування уявлення здобувачів освіти щодо системи міжнародної інформаційної безпеки, а також зарубіжних підходів до забезпечення інформаційної безпеки.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Інформаційна безпека» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Кіберзахист інформаційних ресурсів» *(від 11.09.2024 №29/3/113-127.6а* саме:

ПРН-09	Вміти здійснювати комплексний аналіз загроз національній безпеці, розробляти та реалізовувати ефективні стратегії їх нейтралізації, застосовуючи знання з основ теорії національної безпеки та синтезуючи різнопланову інформацію.
ПРН-10	Вміти пояснювати роль, місце та призначення політичних та безпекових інститутів України для ефективного здійснення заходів при виконання обов'язків з питань забезпечення національної безпеки.
ПРН-12	Планувати та організовувати особисту діяльність в умовах протиборства в інформаційній сфері та кіберпросторі для забезпечення інформаційної безпеки та кібербезпеки держави та організації.
ПРН-13	Оцінювати стан безпеки особистості, суспільства та держави за окремими сферами забезпечення і видами діяльності на основі положень теорії безпеки окремих сфер забезпечення національної безпеки і видів діяльності.
ПРН-16	Розробляти основні положення методів та заходів забезпечення інформаційної безпеки та кібербезпеки держави у різноманітних сферах життєдіяльності.
ПРН-19	Демонструвати здатність розробляти та впроваджувати комплексні стратегії управління інформаційною та кібербезпекою на різних рівнях, що охоплюють окремі організації, державні і міжнародні структури, спираючись на глибоке розуміння теоретичних основ та застосовуючи набуті практичні навички аналізу, дослідження та підготовки відповідної документації.
ПРН-25	Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки для розслідування внутрішніх та зовнішніх інцидентів в сфері кібербезпеки.

3. Програма та структура навчальної дисципліни

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Семестр 5						
Змістовий модуль 1.						
Тема 1. Теоретичні та правові засади інформаційної безпеки.	**24**	**8**	**8**			**8**
Лекція 1. Поняття та зміст інформаційної безпеки.		2				
Семінарське заняття 1. Інформаційна безпека як фундаментальна складова життєво важливих інтересів людини, суспільства та держави.			2			
Самостійна робота 1. Співвідношення безпеки держави, суспільства та особи в інформаційній сфері.						2
Лекція 2. Інформаційна безпека як складова національної безпеки.		2				
Семінарське заняття 2. Інформаційна безпека - визначальний компонент національної безпеки України.			2			
Самостійна робота 2. Інформаційний суверенітет - важлива умова забезпечення інформаційної безпеки Украини.						2
Лекція 3. Основні засади державної інформаційної політики України.		2				
Семінарське заняття 3. Основні концепти державної інформаційної політики.			2			
Лекція 4. Інформаційне суспільство – стратегічна ціль розвитку держави.		2				
Самостійна робота 3. Міжнародні нормативно-правові документи, що визначають основні стратегічні цілі та напрямки розвитку глобального інформаційного суспільства.						4
Семінарське заняття 4. Формування та розвиток інформаційного суспільства в Україні.			2			
Тема 2. Стратегічні засади системи забезпечення інформаційної безпеки України в сучасних умовах.	**28**	**6**	**6**			**16**
Лекція 1. Система забезпечення інформаційної безпеки України.		2				
Самостійна робота 1. Роль і місце кібербезпеки у розвитку сучасного інформаційного суспільства.						4
Семінарське заняття 1. Основні суб'єкти та заходи із забезпечення інформаційної безпеки держави.			2			
Лекція 2. Загрози інформаційній безпеці держави.		2				
Самостійна робота 2. Російсько-українська інформаційна війна: історичний контекст.						4
Семінарське заняття 2. Глобальні та національні загрози інформаційній безпеці України, стратегічні цілі держави з протидії інформаційним загрозам			2			
Лекція 3. Інформаційний делікт як чинник інформаційної безпеки.		2				
Самостійна робота 3. Взаємодія України в сфері забезпечення інформаційної безпеки та кібербезпеки держави з країнами-						4

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
членами ЄС та НАТО.						
Семінарське заняття 3. Правопорушення в інформаційній сфері - аналіз проблемних питань правового забезпечення, запобігання та протидії. **Модульний контроль 1.**			2			
Самостійна робота 4. Зарубіжний досвід забезпечення інформаційної безпеки.						4
Всього годин за змістовий модуль 1.	**52**	**14**	**14**			**24**
Змістовий модуль 2.						
Тема 1. Сучасні деструктивні впливи в інформаційно комунікативному просторі.	**28**	**6**	**2**	**4**		**16**
Лекція 1. Інформаційні війни - джерело загроз в сфері забезпечення інформаційної безпеки.		2				
Самостійна робота 1. Поняття, зміст та історія інформаційно-психологічного протиборства.						4
Семінарське заняття 1. Сучасні форми та методи ведення інформаційних війн.			2			
Самостійна робота 2. Інформаційний тероризм як сучасна загроза інформаційній безпеці людини, суспільства, держави.						4
Лекція 2. Спеціальні інформаційні операції та акції інформаційного впливу як загроза інформаційній безпеці держави.		2				
Самостійна робота 3. Пропаганда та її місце в інформаційній війні: засоби та технології розповсюдження, форми та методи протидії.						4
Практичне заняття 1. Етапи та методи проведення спеціальних інформаційних операції та акцій інформаційного впливу.				2		
Лекція 3. Інформаційні впливи на психіку людини.		2				
Практичне заняття 2. Фізичні фактори інформаційного впливу на психіку людини.				2		
Самостійна робота 4. Ідеологія «руского міра» як ідейна основа російської агресії проти України.						4
Тема 2. Медійний вимір інформаційної безпеки.	**42**	**10**		**10**		**20**
Лекція 1. Медійний простір як середовище для поширення негативних інформаційних впливів.		2				
Практичне заняття 1. Особливості формування та сучасний стан національного медійного простору України.				2		
Лекція 2. Соціальні медіа в сучасному інформаційному просторі.		2				
Практичне заняття 2. Соціальні медіа як інструмент інформаційного впливу на особу, суспільство.				2		
Самостійна робота 1. Характеристики та тенденції розвитку сучасної Інтернет-спільноти України.						4
Лекція 3. Маніпулятивні комунікації в медіа.		2				
Практичне заняття 3. Реалізація маніпулятивних технологій в соціальних медіа.– основні види та їх характеристика.				2		

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Самостійна робота 2. Факт чекінг та OSINT у боротьбі з дезінформацією.						**4**
Лекція 4. Маніпуляції як засіб інформаційно-психологічного впливу у інформаційній війні.		**2**				
Самостійна робота 3. Соціальна інженерія: теоретичні та практичні засади.						**4**
Практичне заняття 4. Технології маніпулювання в інформаційній війні.				**2**		
Самостійна робота 4. Медіакультура та медіаграмотність - основа розвитку інформаційного суспільства.						**4**
Лекція 5. Сугестивні технології маніпулятивного впливу та їх використання в інформаційній сфері.		**2**				
Самостійна робота 5. Сучасні технології нейролінгвістичного програмування та їх використання в інформаційній сфері.						**4**
Практичне заняття 5. Інформаційно-комунікативне суспільство як об'єкт сугестивних маніпулятивних впливів. **Модульний контроль 2.**				**2**		
Всього годин за змістовий модуль ІІ.	**68**	**16**	**2**	**14**		**36**
Підсумковий контроль *(екзамен).*						
Всього годин за навчальну дисципліну.	**120**	**30**	**16**	**14**		**60**

4. Основні методи навчання

І. Методи організації та здійснення навчально-пізнавальної діяльності:

1. За джерелом інформації:

словесні: лекція (традиційна, проблемна) із застосуванням комп'ютерних інформаційних технологій, семінари, пояснення, розповідь, бесіда;

наочні: спостереження, ілюстрація, демонстрація.

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

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

4. За ступенем керування навчальною діяльністю: під керівництвом викладача; самостійна робота студентів: з книгою; виконання індивідуальних навчальних проектів.

ІІ. Методи стимулювання інтересу до навчання і мотивації навчально-пізнавальної діяльності:

навчальні дискусії;

створення ситуації пізнавальної новизни;

створення ситуацій зацікавленості (метод цікавих аналогій тощо);

складання конспекту з теми модуля за заданим, або самостійно складеним планом;

підготовка доповідей з теми модуля;

розробка тестових завдань з теми модуля;
добір додаткового теоретичного та ілюстративного матеріалу;
розробка презентацій з теми модуля;
написання самостійної роботи з теми модуля.

5. Оцінювання результатів навчання

5.1 Результати навчання здобувача вищої освіти з навчальної дисципліни оцінюються за 100-бальною шкалою як сума балів поточного та підсумкового контролю із застосуванням наступних вагових коефіцієнтів, загальна сума яких дорівнює 1:

Вид контролю	Ваговий коефіцієнт
Поточний контроль (К)	**0.6**
Підсумковий контроль (ПК)	**0.4**

Підсумкова семестрова оцінка (ПСО) обчислюється за формулою: ПСО=К+ПК

5.2. Складниками для обчислення балу поточного контролю здобувача вищої освіти є:

Види навчальної діяльності	Кількість балів (максимальна)
Робота на лекціях (ведення конспекту лекцій або інше)	1
Робота на семінарських заняттях	5
Робота на практичних заняттях	5
Робота на лабораторних заняттях	-
Виконання завдань для самостійної роботи	1
Виконання індивідуальних та/або групових завдань	-
Виконання модульної контрольної роботи	5

Мінімальна кількість балів для допуску до підсумкового контролю 36

5.3. Шкала оцінювання здобувача вищої освіти

Оцінка за шкалою ЄКТС	Оцінка за 100-бальною шкалою	Значення оцінки
A	90-100	*Відмінно – відмінне виконання лише з незначною кількістю помилок.* Здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	*Дуже добре – вище середнього рівня, але з кількома помилками.* Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.
C	75-83	*Добре – загалом правильна робота, але з певною кількістю помилок.* Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких

		є суттєві, добирати аргументи для підтвердження думок.
D	65-74	*Задовільно – непогано, але зі значною кількістю недоліків.* Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.
E	60-64	*Достатньо – виконання задовольняє мінімальні вимоги.* Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	*Незадовільно – потрібна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	*Незадовільно – потрібна значна додаткова робота.* Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.

6. Ресурсне забезпечення навчальної дисципліни.

Основна література:

1. Інформаційна безпека: підручник / [В. В. Остроухов, М. М. Присяжнюк, О.І.Фармагей, М.М.Чеховська та ін.]; під ред. В.В.Остроухова. – К.: Ліра-К, 2021. – 412 с.

2. Інформаційне протиборство: навчальний посібник / І.М. Ничитайло, Л.В. Єрьоміна, В.Л. Тиква, Г.М. Чіпуріна, В.М. Шемаєв; – К.: Наук.-вид. відділ НА СБ України, 2023. – 263 с.

3. Забезпечення інформаційної та кібербезпеки в умовах військової агресії рф проти України: аналітичний огляд/ Л.М. Стрельбицька, М.П. Стрельбицький, М.Л. Пальчик. – Київ: НА СБУ, 2022. – 56 с.

4. Сугестивні технології маніпулятивного впливу: навчальний посібник / [В. М. Петрик, М. М. Присяжнюк, Л. Ф. Компанцева, Є. Д. Скулиш, О. Д. Бойко, В. В. Остроухов]; за заг. ред. Є. Д. Скулиша. — 2-ге вид.— Київ: Вид. Дім. «СКІФ», 2023. —248 с.

5. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: моногр./ О.О. Тихомиров; заг. ред. Р.А. Калюжний. – Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.

6. Інформаційно-психологічне протиборство: підручник. Видання друге перекладене, доповнене та перероблене / [В.М. Петрик, В.В. Бедь, М.М. Присяжнюк та ін.]; за заг. ред. В.В. Бедь, В. М. Петрика. — К.: ПАТ «ВІПОЛ», 2018. – 386 с.

Допоміжна література:

1. Горбулін В.П. Як перемогти росію у війні майбутнього / В.Горбулін – Київ: Брайт Букс, 2021. – 248 с.

2. Почепцов Г. Г. Токсичний інфопростір / Г. Почепцов - Харків: Віват, 2022. - 384 с.

3. Почепцов Г.Г. Когнітивні війни у соцмедіа, масовій культурі та масових комунікаціях/ Г. Почепцов – Харків: Фоліо, 2019. – 314 с.

4. Кулеба Д.І. Війна за реальність. Як перемагати у світі фейків, правд і спільнот/ Д.Кулеба – Київ: Книголав, 2023. – 480 с.

5. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод.мат. / Д.В. Дубов, А.В. Баровська, Ю.К. Каздобіна. – К.:УФБС, 2020. – 60 с.

6. Сенченко М. Мас-медіа, піар, як засоби маніпуляції/ М.І. Сенченко, О.М. Сенченко. – Київ: Ліра К, 2022. – 200 с.

7. Світова гібридна війна: український фронт: монографія / за заг. Ред. В.П. Горбуліна. – К.: НІСД, 2017. - 496 с.

8. Тоффлер, Елвін. Третя Хвиля / Е. Тоффлер ; пер. з англ. А. Євса ; ред. пер. ШоВ. Шовкун. - К. : Видавничий дім "Всесвіт", 2000. - 475 с.

9. Правові засади розвитку інформаційного суспільства в Україні: [моногр.] / В. А. Ліпкан, І. М. Сопілко, В. О. Кір'ян / за заг. ред. В. А. Ліпкана. - К. : ФОП О. С. Ліпкан, 2015. -664 с.

10. Тихомиров О.О. Права людини: інформаційний вимір: монографія / О.О. Тихомиров.- Одеса: Видавництво «Юридика», 2023. – 304 с.

11. Рекомендації та кращі кейси реалізації стратегічних комунікацій в умовах війни : практичний довідник / [В. Азарова та ін.; за заг. ред. Л. Компанцевої]. Київ : БЦ, 2023. 232 с.

Нормативно-правові акти:

1. Конституція України (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141)

2. Закон України "Про Службу безпеки України" від 25 березня 1992 року № 2229-XII

3. Закон України "Про національну безпеку України" від 21.06.2018р. № 2469 - VIII

4. Закон України "Про інформацію" від 02.10.1992 р. № 2457 - XII

5. Закон України «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI

6. Закон України "Про державну таємницю" від 21.01.1994р. № 3855- XII

7. Закон України «Про Національну програму інформатизації» від 1 грудня 2022 року № 2807-IX

8. Закон України «Про медіа» від 13 грудня 2022 року № 2849-IX

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

10. Закон України «Про Раду національної безпеки і оборони України» від 5 березня 1998 року № 183/98-ВР.

11. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 року № 3475-IV.

12. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 5 липня 1994 року № 80/94-ВР.

13. Закон України "Про основні засади державної політики у сфері утвердження української національної та громадянської ідентичності" від 13 грудня 2022 року № 2834-IX.

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

15. Кодекс України про адміністративні правопорушення. (Редакція від 09.08.2024). Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10#Text

16. Цивільний кодекс України. (Редакція від 03.09.2024). Режим доступу: https://zakon.rada.gov.ua/laws/show/435-15#Text

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

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

19. Указ Президента України №56/2022 Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про Стратегію забезпечення державної безпеки»

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

21. Указ Президента України 242/2016 «Про Національний координаційний центр кібербезпеки».

22. Постанова Кабінету Міністрів України від 15 грудня 2023 р. № 1322 «Про схвалення Стратегії утвердження української національної та громадянської ідентичності на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2023-2025 роках».

23. Постанова Кабінету Міністрів України від 12 березня 2022 р. № 263 «Деякі питання забезпечення функціонування інформаційно- комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану».

24. Окінавська хартія глобального інформаційного суспільства [Електронний ресурс]. – Режим доступу: https://ips.ligazakon.net/document/MU00269

25. Європейська конвенція про кіберзлочинність. Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text

Електронні ресурси:

1. Офіційна сторінка Верховної Ради України: www.zakon.rada.gov.ua
2. Офіційна сторінка Президента України: www.president.gov.ua
3. Офіційна сторінка Центру протидії дезінформації: https://cpd.gov.ua
4. Офіційна сторінка Центру стратегічних комунікацій та інформаційної безпеки: https://spravdi.gov.ua
5. Офіційна сторінка Національного інституту стратегічних досліджень: https://niss.gov.ua

Адреса розміщення робочої програми навчальної дисципліни

_____

(офіційний вебсайт НА СБУ / платформа дистанційного навчання / електронний ресурс навчально-наукового інституту, кафедри, бібліотеки тощо)

7. Дані про перегляд робочої програми навчальної дисципліни[1]

№ п/п	Дата, номер протоколу засідання кафедри (спільного засідання кафедр)	Рішення за результатами перегляду	Підпис керівника кафедри

[1] Перегляд робочої програми навчальної дисципліни відбувається щорічно, з урахуванням результатів моніторингу та періодичного перегляду освітньої програми і, зокрема, отриманих від здобувачів вищої освіти та інших стейкхолдерів побажань та зауважень.

29/3/3-504/6
18.10.2024