1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	2
Семестр (и)	4
Обсяг *(кредити ЄКТС/години)*	5/150
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	20
семінарські заняття (СЗ)	30
практичні заняття (ПЗ)	–
лабораторні заняття (ЛЗ)	
індивідуальні завдання (ІЗ)	
самостійна робота (СР)	100
форма підсумкового контролю *(семестр)*	екзамен

2. Мета та завдання навчальної дисципліни

2.1. Мета та основні завдання вивчення навчальної дисципліни

Мета: формування у студентів ННІ ІБ СК Національної академії СБ України системи концептуальних знань про передумови, тенденції, сутність та зміст інформаційної безпеки, її складові і напрями, в сучасних умовах розвитку інформаційних технологій та суспільної взаємодії, а також компетентностей щодо виокремлення, осмислення і вирішення основних проблем в означеній сфері.

Завдання:

Основними завданнями вивчення навчальної дисципліни «Система забезпечення державної безпеки в інформаційній сфері» є:

- усвідомлення комплексності проблем інформаційної безпеки і шляхів її вирішення;

- з'ясування тенденцій, факторів, чинників, перспектив розвитку уявлень про інформаційну безпеку та її значення для майбутнього людства в національному, регіональному і світовому масштабі;

- осмислення явища інформаційної безпеки в єдності найбільш актуальних складових її осмислення і забезпечення, зокрема в контексті права, медіа, інформаційно-аналітичного забезпечення, інформаційних технологій;

- формування здатностей до індивідуальної і групової творчо-аналітичної діяльності, дослідницьких компетентностей, умінь і навичок представляти результати власної діяльності, аргументувати і захищати власну професійну позицію.

2.2. Результати навчання

Обов'язкова навчальна дисципліна «Система забезпечення державної безпеки в інформаційній сфері» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Організація захисту інформації з обмеженим доступом» (*№29/3/4-408/ві від 12.09.2024року, зміни №29/3-30/ві від 11.02.2025 року),* а саме:

ПРН 3.	Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави, у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.
ПРН 11.	Застосовувати загальну методологію, спеціальні методи і технології для розв'язання професійних задач у визначених законодавством сферах та за напрямами майбутньої діяльності.
ПРН 14.	Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань національної безпеки до фахівців і нефахівців, зокрема до осіб, які навчаються.
ПРН 15.	Управляти проведенням заходів у процесі забезпечення національної безпеки в різних умовах обстановки з використанням нових стратегічних підходів.

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 2						
Змістовий модуль 1. Основні поняття та визначення інформаційної безпеки держави						
Тема 1. Аналіз стану інформаційного простору та інформаційної безпеки держави.	**18**	**2**	**4**			**12**
Лекція 1. Аналіз стану інформаційного простору та інформаційної безпеки держави.		2				
Семінарське заняття 1. Аналіз стану інформаційного простору та інформаційної безпеки держави.			2			
Семінарське заняття 2. Інформаційний суверенітет: визначення, дискусії.			2			
Самостійна робота 1. Основні концепти державної інформаційної політики.						4
Самостійна робота 2. Підходи до дослідження інформаційної безпеки: статичний, діяльнісний, комплексний.						4
Самостійна робота 3. Класифікація національних інтересів, національний інтерес в інформаційній сфері.						4
Тема 2. Сутність інформаційної безпеки держави, суспільства та особи.	**24**	**4**	**4**			**16**
Лекція 1. Сутність інформаційної безпеки держави, суспільства та особи.		2				
Семінарське заняття 1. Інформаційна безпека як складова національної безпеки.			2			
Лекція 2. Принципи інформаційної війни. Логіка інформаційної війни.		2				
Семінарське заняття 2. Моделі інформаційної війни. Різновиди інформаційних воєн.			2			
Самостійна робота 1. Засоби, методи і технології інформаційних воєн.						6
Самостійна робота 2. Різновиди інформаційної безпеки особи, суспільства та держави.						4
Самостійна робота 3. Спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, інформаційні війни.						6
Тема 3. Основи інформаційного протиборства.	**22**	**2**	**4**			**16**
Лекція 1. Основи інформаційного протиборства.		2				
Семінарське заняття 1. Інформаційне протиборство, інформаційна експансія, інформаційна війна, інформаційний тероризм.			2			
Самостійна робота 1. Інтернет-ресурси як об'єкти загроз інформаційній безпеці держави.						4
Семінарське заняття 2. Сучасні інформаційні війни.			2			
Самостійна робота 3. Основи інформаційного протиборства.						4
Самостійна робота 4. Інформаційна акція, інформаційна атака, інформаційна операція, інформаційна кампанія.						4
Самостійна робота 5. Система моніторингу Інтернет-ресурсів.						4
Всього годин за модуль 1	**64**	**8**	**12**			**44**

1	2	3	4	5	6	7
Змістовий модуль 2. Загрози національній безпеці держави та боротьба з ними в інформаційній сфері						
Тема 4. Основні загрози національній безпеці держави в інформаційній сфері.	**22**	**4**	**4**			**14**
Лекція 1. Основні загрози національній безпеці держави в інформаційній сфері.		2				
Семінарське заняття 1. Загрози національній безпеці України в інформаційній сфері.			2			
Лекція 2. Інформаційний тероризм. Комп'ютерна злочинність.		2				
Семінарське заняття 2. Шляхи забезпечення інформаційної безпеки України.			2			
Самостійна робота 1. Конкурентоспроможність вітчизняної продукції, що обслуговує інформаційну сферу.						4
Самостійна робота 2. Розголошення інформації з обмеженим доступом.						4
Самостійна робота 3. Розвідувально-підривна діяльність іноземних спецслужб.						6
Тема 5. Стратегічні цілі та завдання інформаційної боротьби.	**22**	**2**	**4**			**16**
Лекція 1. Стратегічні цілі та завдання інформаційної боротьби.		2				
Семінарське заняття 1. Стратегічні цілі та завдання інформаційної боротьби.			2			
Семінарське заняття 2. Пропаганда та комунікативні складники інформаційно-психологічної боротьби.			2			
Самостійна робота 1. Інформаційна безпека суспільства та держави.						4
Самостійна робота 2. Державне управління в умовах інформаційного суспільства.						4
Самостійна робота 3. Інформаційне протиборство і національна безпека.						4
Самостійна робота 4. Інформаційні ризики від застосування інформаційних технологій.						4
Тема 6. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності.	**20**	**4**	**4**			**12**
Лекція 1. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності.		2				
Семінарське заняття 1. Стан розбудови інформаційного суспільства в Україні. Порівняльний аналіз.			2			
Лекція 2. Основні напрями та першочергові заходи державної політики забезпечення інформаційної безпеки України.		2				
Семінарське заняття 2. Свобода слова в Україні та інформаційна безпека держави.			2			
Самостійна робота 1. Незалежність засобів масової інформації.						4
Самостійна робота 2. Проблеми утвердження свободи слова в Україні.						4
Самостійна робота 3. Інститути забезпечення інформаційної безпеки України.						4
Тема 7. Інформаційні технології та проблеми їхньої	**22**	**2**	**6**			**14**

1	2	3	4	5	6	7
безпеки.						
Лекція 1. Інформаційні технології та проблеми їхньої безпеки.		2				
Семінарське заняття 1. Криптографічний захист інформації.			4			
Семінарське заняття 2. Правові аспекти захисту інформації в автоматизованих системах.			2			
Самостійна робота 1. Критерії безпеки інформаційних технологій.						4
Самостійна робота 2. Інтернет як об'єкт інформаційного права та ІБ.						4
Самостійна робота 3. Досвід забезпечення інформаційної безпеки в державах ЄС, США.						6
Всього годин за модуль 2	**86**	**12**	**18**			**56**
Підсумковий контроль ЕКЗАМЕН						
Всього годин за дисципліну	**150**	**20**	**30**			**100**

4. Основні методи навчання

Методи організації і здійснення навчально-пізнавальної діяльності:

– методи надання і сприйняття навчальної інформації: словесні (лекція, дискусія); наочні (ілюстрація, демонстрація, візуалізація); практичні (міні-дослідження, задачі);

– методи логіки сприйняття навчальної інформації: індуктивний; дедуктивний; аналітичний, моделювання, тощо;

– методи формування знань: репродуктивний; проблемно-пошуковий;

– організаційні методи: навчальна робота під керівництвом викладача; самостійна творчо-пошукова робота з джерельною базою, міні-дослідження.

Методи стимулювання і мотивації навчально-пізнавальної діяльності та розвитку soft skills:

– стимулювання інтересу до дослідницької діяльності;

– створення навчально-наукової дискусії;

– моделювання проблемних ситуацій правової сфери, що потребують наукового вирішення;

– колективна робота малими групами;

– модерування групової роботи;

– створення презентації, інфографіки;

– кейс-метод;

– створення ситуацій зайнятості і пізнавальної новизни;

– заохочення до самонавчання і дослідницької творчості.

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	-
Робота на лабораторних заняттях	-
Виконання завдань для самостійної роботи	1
Виконання індивідуальних та/або групових завдань	-
Виконання модульної контрольної роботи	-

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. Актуальні проблеми інформаційної безпеки : навч. посіб. / О. О. Тихомиров, А. В. Ватраль, Д. С. Мельник та ін. Київ : НА СБУ, 2024. 264 с.
2. Баранов О. А. Соціальні та цифрові трансформації: нова парадигма кібербезпеки. Монографія. Київ: 2021. 86 с.
3. Горбулін В.П. Як перемогти росію у війні майбутнього / В.Горбулін. Київ: Брайт Букс, 2021. 248 с.
4. Енциклопедія соціогуманітарної інформології / коорд. проєкту та заг. ред. проф. К.І. Бєляков. Одеса: Видавничий дім «Гельветика». 2021. Т. 2. 432 с.
5. Енциклопедія соціогуманітарної інформології / коорд. проєкту проф. К.І. Бєляков. Київ: Видавничий дім «Гельветика», 2020. Т. 1. 472 с.
6. Золотар О.О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
7. Інформаційна безпека. Підручник / В.В. Остроухов, М.М. Присяжнюк, О.І. Фармагей, М.М. Чеховська та ін.; за ред. В.В. Остроухова. Київ: Видавництво Ліра-К, 2021. 412 с.
8. Інформаційне протиборство: навчальний посібник / І.М. Ничитайло, Л.В. Єрьоміна, В.Л. Тиква, Г.М. Чіпуріна, В.М. Шемаєв; Київ: Наук.-вид. відділ НА СБ України, 2023. 263 с.
9. Організаційно-правові основи забезпечення кібербезпеки: підручник / М.М. Присяжнюк, А.І. Марущак, Д.С. Мельник, В.В. Остроухов, М.В. Гуцалюк, О.П. Ткаченко; за заг. ред. М.М. Присяжнюка. Київ: Вид-во «Ліра-К», 2023. 320 с.
10. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ: НІСД, 2017. 496 с.
11. Стратегічний, оперативний, ситуаційний аналіз у сфері національної безпеки (основні підходи і методики) : оглядове видання / уклад. Д. В. Талалай, О. О. Тихомиров. Київ : НА СБУ, 2023. 76 с.
12. Стратегія розвитку штучного інтелекту в Україні: монографія / А. І. Шевченко, С. В. Барановський, О. В. Білокобильський, Є. В. Бодянський та ін. [За заг. ред. А. І. Шевченка]. Київ: ІПШІ, 2023. 305 с.
13. Сугестивні технології маніпулятивного впливу: навч. посіб. / М.М. Присяжнюк, Л.Ф. Компанцева, Є.Д. Скулиш [та ін.]; ред.: Є.Д. Скулиша; Київ: Нац. акад. СБУ, 2010. 247 с.
14. Тихомиров О. О., Тугарова О. К. Юридична відповідальність за правопорушення в інформаційній сфері: навч. посіб. Київ: Нац. акад. СБУ, 2015. 172 с.
15. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І.В. Арістова, О.А. Баранов, О.П. Дзьобань та ін.; за заг. ред. проф. К. І. Бєлякова. Київ: КВІЦ, 2019. 344 с.

Допоміжна література:

1. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах. Юридична Україна. 2018. № 5-6. С. 75–95.
2. Баранов О.А. Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом. Інформація і право. 2018. № 4(27). С. 46–70.
3. Бєляков К.І., Онопрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір. Монографія. Київ: КВІЦ, 2018. 168 с.
4. Грабар І.Г., Грищук Р.В., Молодецька К.В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир, 2019. 279 с.
5. Деструктивні впливи та негативні наративи: інструменти виявлення та протидії: метод.мат. / Д.В. Дубов, А.В. Баровська, Ю.К. Каздобіна. Київ: УФБС, 2020. 60 с.
6. Дзьобань О.П., Мануйлов Є.М. Інформаційна безпека в контексті інформаційної культури. Інформація і право. 2017. № 1(20). С. 74–81.
7. 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.
8. Костенко О.В. Електронна юрисдикція, метавсесвіт, штучний інтелект, цифрова особистість, цифровий аватар, нейронні мережі: теорія, практика, перспективи. Наукові інновації та передові технології. 2022. № 2(4). С. 54-78.
9. Кулеба Д.І. Війна за реальність. Як перемагати у світі фейків, правд і спільнот. Київ: Книголав, 2023. 480 с.
10. Ланде Д.В., Фурашев В.М. Парламентський контроль із застосуванням генеративного штучного інтелекту : монографія / Ланде Д.В., Фурашев В.М. Київ: ТОВ «Інжиніринг», 2023. 202 с.
11. Мельник Д.С. Комп'ютерні злочини: проблеми виділення та кваліфікації. Міжнародний науковий журнал «Інтернаука». Київ, 2021, вип. 4 (104), С. 59-62. URL: htttps://doi.org/10.25313/2520-2057-2021-4-7055
12. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
13. Почепцов Г.Г. Когнітивні війни у соцмедіа, масовій культурі та масових комунікаціях. Харків: Фоліо, 2019. 314 с.
14. Почепцов Г.Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Київ: Vivat, 2021. 384 с.
15. Размєтаєва Ю.С. Цифрові права людини та проблеми екстратериторіальності в їх захисті. Право та державне управління. 2020. № 4. С. 12–23.
16. Сенченко М. Мас-медіа, піар, як засоби маніпуляції. Київ: Ліра К, 2022. 200 с.
17. Стрельбицька Л.М. Стрельбицький М.П., Пальчик М.Л. Організаційно-правові засади управління інформаційною та кібернетичною безпекою як складових національної безпеки України. Київ: НА СБУ, 2022. 65 с.

18. Тихомиров О.О. Еволюція інформаційних прав людини. Інформація і право. 2023. № 1 (44). С. 50–57.
19. Тихомиров О.О. Права людини: інформаційний вимір : монографія Одеса : Видавництво «Юридика», 2023. 304 с.
20. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.
21. Clarke A.E., Washburn R., Friese C. (Eds.). Situational Analysis in Practice: Mapping Relationalities Across Disciplines (2nd ed.). New York: Routledge. 2022. 378 p. DOI: https://doi.org/10.4324/9781003035923
22. Hassan M. Framework Analysis – Method, Types and Examples. October 1, 2023. URL: https://researchmethod.net/framework-analysis/.
23. Tykhomyrov O.O., Bieliakov K.I., Kostenko O.V., Radovetska L.V. Digital rights in the human rights system. InterEULawEast. 2023. Vol. X (1). P. 183–207. DOI: https://doi.org/10.22598/iele.2023.10.1.10; URL: https://hrcak.srce.hr/file/440551
24. Tykhomyrov O.O, Kostenko O.M., Bieliakov K.I., Aristova I.V. «Legal personality» of artificial intelligence: methodological problems of scientific reasoning by Ukrainian and EU experts. AI & SOCIETY. February 2023. DOI: https://doi.org/10.1007/s00146-023-01641-0

Нормативно-правові джерела:

1. Загальна декларація прав людини: Міжнародний документ від 10.12.1948. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_015
2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Міжнародний документ від 28.01.1981. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_326
3. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини): міжнародний документ від 04.11.1950. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_004
4. Конвенція про кіберзлочинність: міжнародний документ. Ратифікація від 07.09.2005. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575
5. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр
6. Міжнародний пакт про громадянські і політичні права: міжнародний документ. Прийнято Генеральною Асамблеєю ООН 16 грудня 1966 року. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_043
7. Про інформацію: Закон України від 02.10.1992 № 2657-XII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12
8. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: http://zakon2.rada.gov.ua/laws/show/2163-19

10. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/389-19
11. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 2.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80
12. Про Цілі сталого розвитку України на період до 2030 року: Указ Президента України №722/2019 від 30.09.2019. Президент України. URL: https://www.president.gov.ua/documents/7222019-29825
13. Стратегія інформаційної безпеки : затверджено Указом Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021
14. Стратегія кібербезпеки України : затверджено Указом Президента України від 26.08.2021 № 447/2021. URL: https://www.rnbo.gov.ua/ua/Ukazy/4974.html
15. Стратегія національної безпеки України «Безпека людини – безпека країни» : затверджено Указом Президента України від 14.09.2020 № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020

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.