НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Кафедра інформаційної безпеки держави

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Організаційно-правові основи забезпечення інформаційної безпеки»

Освітня програма	«Право інформаційної безпеки»
Рівень вищої освіти	перший (бакалаврський)
Форма навчання	денна
Статус навчальної дисципліни	обов'язкова
Мова викладання	українська

КИЇВ – 2025

Робочу програму навчальної дисципліни розглянуто та затверджено на засіданні КІБД ННІ ІБ СК НА СБ України від «02» 12 2025 року, протокол № 14.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	4
Семестр (и)	7
Обсяг *(кредити ЄКТС/години)*	5/150
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	30
семінарські заняття (СЗ)	14
практичні заняття (ПЗ)	30
лабораторні заняття (ЛЗ)	
індивідуальні завдання (ІЗ)	
самостійна робота (СР)	76
форма підсумкового контролю	екзамен

2. Мета та завдання навчальної дисципліни

2.1. Мета – набуття здобувачем освіти компетенцій, знань, умінь і навичок для подальшого використання у практичній діяльності із організаційно-правового забезпечення інформаційної безпеки України в умовах розвитку інформаційного суспільства.

2.2. Завдання:

Основними завданнями вивчення дисципліни «Організаційно-правові основи забезпечення інформаційної безпеки» є:

- отримання базових знань з основ організаційно-правового забезпечення інформаційної безпеки;
- набуття вмінь використовувати законодавство, підзаконні нормативно-правові акти, вітчизняний та зарубіжний досвід при аналізі сфери інформаційної безпеки;
- набуття вмінь визначати життєво важливі інтереси людини, суспільства та держави в інформаційній сфері;
- отримання навичок здійснення науковий аналіз сучасного стану забезпечення інформаційної безпеки;
- розширення та систематизація знань щодо загроз безпеці держави в інформаційній сфері;
- отримання знань щодо визначення загроз інформаційній безпеці;
- набуття знань щодо визначення стану інформаційної безпеки держави.

2.3. Результати навчання

Обов'язкова навчальна дисципліна «Організаційно-правові основи забезпечення інформаційної безпеки» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної програми «Право інформаційної безпеки» *(від 30.08.2024 № 29/1/7-7380/ві)*, а саме:

РН1	Визначати переконливість аргументів у процесі оцінки заздалегідь невідомих умов та обставин.
РН3	Проводити збір і інтегрований аналіз матеріалів з різних джерел.
РН6	Оцінювати недоліки і переваги певних правових аргументів, аналізуючи відому проблему.
РН9	Самостійно визначати ті обставини, у з'ясуванні яких потрібна допомога, і діяти відповідно до отриманих рекомендацій.
РН12	Доносити до респондента матеріал з певної проблематики доступно і зрозуміло.
РН15	Вільно використовувати для правничої діяльності доступні інформаційні технології і бази даних.
РН16	Використовувати комп'ютерні програми, необхідні у правничій діяльності.
РН18	Застосовувати в професійній діяльності основні сучасні правові доктрини, цінності та принципи функціонування національної правової системи.
РН19	Пояснювати природу та зміст основних правових явищ і процесів.
РН23	Демонструвати розуміння напрямів забезпечення інформаційної безпеки, зокрема з використанням різних правових механізмів.
РН24	Забезпечувати власну інформаційну безпеку у процесі здійснення правничої діяльності.

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*
Змістовий модуль 1.						
Тема 1. Теоретичні та правові засади інформаційної безпеки.	**22**	**4**	**4**	**2**		**12**
Лекція 1. Поняття та зміст інформаційної безпеки.		**2**				
Самостійна робота 1. Сучасні підходи до визначення поняття інформаційна безпека.						**4**
Семінарське заняття 1. Підходи до концептуалізації та ідентифікатори визначення основних понять інформаційної безпеки.			**2**			
Самостійна робота 2. Співвідношення безпеки держави, суспільства та особи в інформаційній сфері.						**4**
Лекція 2. Інформаційна безпека як складова національної безпеки.		**2**				
Семінарське заняття 2. Інформаційна безпека - визначальний компонент національної безпеки України.			**2**			
Самостійна робота 3. Правові засади організації системи інформаційної безпеки в Україні.						**4**
Практичне заняття 1. Інформаційний суверенітет - важлива умова забезпечення інформаційної безпеки України.				**2**		
Тема 2. Державна інформаційна політика.	**38**	**6**	**2**	**8**		**22**
Лекція 1. Основні засади державної інформаційної політики України.		**2**				
Практичне заняття 1. Особливості державної інформаційної політики в умовах війни.				**2**		
Лекція 2. Формування та розвиток інформаційного суспільства в Україні.		**2**				
Самостійна робота 1. Міжнародні нормативно-правові документи, що визначають основні стратегічні цілі та напрямки розвитку глобального інформаційного суспільства.						**4**
Практичне заняття 2. Інформаційне суспільство як головний пріоритет перспективного розвитку держави.				**2**		
Самостійна робота 2. Інформаційна складова науково-технологічного розвитку держави.						**4**
Лекція 3. Система забезпечення інформаційної безпеки України.		**2**				
Самостійна робота 3. Механізм забезпечення інформаційної безпеки держави.						**4**
Семінарське заняття 1. Основні суб'єкти та заходи із забезпечення інформаційної безпеки держави.			**2**			
Самостійна робота 4. Кібербезпека та нові виклики для інформаційного суспільства України в умовах війни.						**5**
Практичне заняття 3. Забезпечення кібербезпеки - запорука успішного розвитку інформаційного суспільства в Україні.				**4**		
Самостійна робота 5. Міжнародна співпраця України в галузі забезпечення інформаційної та кібербезпеки.						**5**
Тема 3. Загрози інформаційній безпеці держави.	**20**	**4**	**2**	**4**		**10**

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Лекція 1. Глобальні та національні загрози інформаційній безпеці України.		2				
Самостійна робота 1. Наукові підходи до визначення видів загроз інформаційній безпеці.						5
Практичне заняття 1. Оцінка загроз інформаційній безпеці.				2		
Практичне заняття 2. Актуальні питання протидії деструктивним інформаційним впливам рф.				2		
Лекція 2. Національні механізми протидії інформаційним загрозам.		2				
Самостійна робота 2. Механізми державного реагування на сучасні виклики та загрози інформаційній безпеці.						5
Семінарське заняття 1. Стратегічні цілі та завдання з протидії інформаційним загрозам в умовах гібридної війни рф проти України.			2			
Всього годин за модуль І.	80	14	8	14		44
Змістовий модуль 2.						
Тема 1. Стратегічні засади системи забезпечення інформаційної безпеки України в сучасних умовах.	44	8	4	8		24
Лекція 1. Роль та місце правоохоронних органів та спеціальних служб в системі забезпечення інформаційної безпеки України в сучасних умовах.		2				
Самостійна робота 1. Діяльність суб'єктів формування і реалізації політики державної безпеки в інформаційній сфері України.						4
Семінарське заняття 1. Завдання та функції органів державної влади у сфері забезпечення інформаційної безпеки України.			2			
Лекція 2. Правопорушення у сфері інформаційної безпеки.		2				
Практичне заняття 1. Актуальні питання протидії правопорушенням в інформаційній сфері.				2		
Самостійна робота 2. Міжнародна інформаційна безпека.						4
Лекція 3. Зарубіжний досвід забезпечення інформаційної безпеки.		2				
Практичне заняття 2. Розбудова системи міжнародної інформаційної безпеки в сучасних умовах.				2		
Самостійна робота 3. Взаємодія України в сфері забезпечення інформаційної безпеки держави з країнами-членами ЄС та НАТО.						2
Семінарське заняття 2. Аналіз та шляхи впровадження передового зарубіжного досвіду забезпечення інформаційної безпеки держави.			2			
Самостійна робота 4. Вплив інформації на прогресивний розвиток суспільства.						2
Лекція 4. Інформаційні права і свободи людини та громадянина як основа формування інформаційного суспільства.		2				
Самостійна робота 5. Забезпечення інформаційних прав та свобод людини в умовах воєнного стану.						4

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	*2*	*3*	*4*	*5*	*6*	*7*
Практичне заняття 3. Інформаційна гігієна та кібергігієна як необхідна умова діяльності сучасної людини.				2		
Самостійна робота 6. Інформаційна та кібербгігієна в органах державної влади.						4
Практичне заняття 4. Основи управління інформаційною безпекою.				2		
Самостійна робота 7. Публічне управління інформаційною безпекою в умовах цифровізації.						4
Тема 2. Забезпечення інформаційної безпеки в умовах війни.	26	8	2	8		8
Лекція 1. Медійний простір як середовище для маніпулятивних впливів на масову свідомість.		2				
Самостійна робота 1. Нормативно-правове забезпечення національного медійного простору.						4
Семінарське заняття 1. Особливості формування та сучасний стан національного медійного простору України.			2			
Практичне заняття 1. Соціальні медіа в сучасному інформаційному просторі.				2		
Лекція 2. Деструктивні інформаційні впливи рф як складова гібридної війни проти України.		4				
Практичне заняття 2. Виявлення дезінформації, маніпуляцій та пропаганди в інформаційному середовищі України.				4		
Лекція 3. Медіакультура та медіаграмотність в протидії деструктивним інформаційним впливам.		2				
Практичне заняття 3. Медіакультура та медіаграмотність - основа формування інформаційного суспільства.				2		
Самостійна робота 2. Медіаосвіта як запорука розвитку демократії в умовах інформаційного суспільства.						4
Всього годин за модуль ІІ.	70	16	6	16		32
Підсумковий контроль ЕКЗАМЕН						
Всього годин за навчальну дисципліну.	150	30	14	30		76

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	-
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

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

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.