

НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ

Кафедра інформаційної безпеки держави

**РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Актуальні проблеми інформаційної безпеки»**

Освітня програма	«Кіберзахист у сфері інформаційних технологій та кіберпросторі»
Рівень вищої освіти	другий (магістерський)
Форма навчання	денна
Статус навчальної дисципліни	обов'язкова
Мова викладання	українська

КИЇВ – 2025

721 ноз401

Робочу програму навчальної дисципліни розглянуто та схвалено на засіданні кафедри ІБД ННІ ІБ СК НА СБ України від «06» 01 2025 року, протокол № 1.

1. Опис навчальної дисципліни

Показник	Значення показника
Курс (и)	1
Семестр (и)	2
Обсяг (<i>кредити ЄКТС/години</i>)	5/150
Кількість змістових модулів	2
Розподіл годин за видами навчальної діяльності:	
лекції (Л)	18
семінарські заняття (СЗ)	38
практичні заняття (ПЗ)	-
індивідуальні завдання (ІЗ)	-
самостійна робота (СР)	94
форма підсумкового контролю (<i>семестр</i>)	диф. залік

2. Мета та завдання навчальної дисципліни

2.1. 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.

2.2. Завдання:

Основними завданнями опанування навчальної дисципліни «Актуальні проблеми інформаційної безпеки» 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.

2.3. Результати навчання

Обов'язкова навчальна дисципліна «Актуальні проблеми інформаційної безпеки» спрямована на досягнення програмних результатів навчання, які в інтегрованому (синтезованому) вигляді визначені у профілі освітньо-професійної / освітньо-наукової програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» (від 11.09.2024 № 29/3/1/1-1276/ві), а саме:

ПРН-02	Застосовувати вітчизняний та зарубіжний досвід забезпечення національної безпеки з урахуванням теорії національної безпеки під час здійснення професійної діяльності.
ПРН-03	Приймати обґрунтовані рішення з питань забезпечення національної безпеки держави (кіберзахист, забезпечення державної безпеки в інформаційній сфері), у тому числі в умовах багатокритеріальності, неповних чи суперечливих інформації та вимог.
ПРН-05	Розробляти та реалізовувати інноваційні проекти у сфері національної безпеки з урахуванням правових, соціальних, економічних та етичних аспектів.
ПРН-07	Аналізувати та оцінювати потенційний вплив розвитку технологій на сучасний стан безпекового середовища.
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-16	Організовувати та спрямовувати діяльність фахівців з кіберзахисту у сфері інформаційних технологій та кіберпросторі; розробляти та впроваджувати заходи із кіберзахисту у сфері інформаційних технологій та кіберпросторі, самостійно та у взаємодії з контролюючими органами.
ПРН-20	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
ПРН-23	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

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
Змістовний модуль 1. Засади розуміння інформаційної безпеки та їх правове відображення в сучасних умовах						
Тема 1. Теорія і філософія інформаційної безпеки	18	2	4			12
Лекція 1. Генеза розуміння інформаційної безпеки в науці і практиці		2				
Семінар 1. Сучасні тренди інформаційної безпеки			2			
Самостійна робота 1. Цінність інформаційної безпеки в інформаційному суспільстві						6
Семінар 2. Параметри інформаційної безпеки в основних вимірах її забезпечення			2			
Самостійна робота 2. Вплив агресивної інформаційної політики рф на інформаційну безпеку європейському і світовому рівні						6
Тема 2. Правові аспекти інформаційної безпеки	50	6	12			32
Лекція 1. Правове регулювання інформаційної безпеки: національний, міжнародний регіональний і глобальний рівні		2				
Семінар 1. Інформаційна безпека в системі національної безпеки			2			
Самостійна робота 1. Розвиток положень про інформаційну безпеку в українському законодавстві						4
Семінар 2. Інформаційна безпека в міжнародному контексті			2			
Самостійна робота 2. Міжнародні стандарти управління інформаційною безпекою						4
Лекція 2. Інформаційні права людини як стратегічний пріоритет інформаційної безпеки		2				
Семінар 3. Інформаційні права людини в міжнародних стандартах прав людини і національному законодавстві			2			
Самостійна робота 3. «Інформація» як критерій інформаційних прав людини						6
Семінар 4. Цифрові права людини в реаліях і перспективах інформаційної безпеки			2			
Самостійна робота 4. Європейські ініціативи щодо						6

Назви змістових модулів, тем навчальних занять	Кількість годин					
	Усього	Л	СЗ	ПЗ	ЛЗ	СР
1	2	3	4	5	6	7
цифрових прав та їх розвиток						
Лекція 3. Інформаційні делікти як чинник інформаційної безпеки		2				
Семінар 5. Поняття, види, особливості інформаційних деліктів			2			
Самостійна робота 5. Причини виникнення і поширення інформаційних деліктів						6
Семінар 6. Юридична відповідальність за інформаційні делікти			2			
Самостійна робота 6. Юридична відповідальність в системі механізмів забезпечення інформаційної безпеки						6
Модульний контроль 1			2			
Всього годин за модуль 1	70	8	18			44
Змістовний модуль 2. Медіа, аналітична та технологічна складова інформаційної безпеки						
Тема 3. Медійний вимір інформаційної безпеки	24	4	4			16
Лекція 1. Розвиток медіапростору як чинник інформаційної безпеки		4				
Семінар 1. Соціальні медіа та їх вплив на інформаційну безпеку			2			
Самостійна робота 1. Правові та морально-етичні засади регулювання медіа в сучасних умовах						8
Семінар 2. Технології маніпулятивних інформаційних впливів в медіапросторі			2			
Самостійна робота 2. Протидія дезінформації в медіапросторі як напрям забезпечення інформаційної безпеки						8
Тема 4. Аналітична складова інформаційної безпеки	18	2	4			12
Лекція 1. Інформаційно-аналітичне забезпечення в системі забезпечення інформаційної безпеки		2				
Семінар 1. Види, рівні, форми аналізу у сфері національної безпеки			2			
Самостійна робота 1. Стандарти і особливості інформаційно-аналітичного забезпечення в різних видах соціально значущої діяльності						6
Семінар 2. Основні аналітичні рамки та можливості їх використання в контексті інформаційної безпеки			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. Альтернативні формати інформаційно-аналітичного забезпечення						6
Тема 5. Інформаційні технології і перспективи інформаційної безпеки	34	4	8			22
Лекція 1. Кібербезпека в сучасних умовах: проблеми розуміння, чинники, перспективи		2				
Семінар 1. Складові, напрями, суб'єкти, стратегічні цілі забезпечення кібербезпеки України			2			
Самостійна робота 1. Міжнародне регулювання кібербезпеки						6
Семінар 2. Характеристика основних проявів кіберзлочинності			2			
Самостійна робота 2. Подолання кіберзлочинності в кібербезпекових стратегіях провідних країн світу						6
Лекція 2. Інформаційні технології та перспективи їх розвитку в безпековому вимірі		2				
Семінар 3. Актуальні тренди інформаційних технологій в контексті безпеки: проблеми, загрози та шляхи їх подолання			2			
Самостійна робота 3. Властивості середовища індустрії 4.0 та його вплив на безпеку						4
Семінар 4. Штучний інтелект як чинник формування сучасного середовища забезпечення інформаційної безпеки			2			
Самостійна робота 4. Перспективи зміни парадигми інформаційної безпеки в умовах розвитку Metaverse						6
Модульний контроль 2			2			
Всього годин за модуль 2	78	10	18			50
Підсумковий контроль (диференційований залік)			2			
Всього годин за навчальну дисципліну	150	18	38			94

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 (участь в обговоренні актуальних питань; власні пропозиції, зауваження тощо)	1
Робота на семінарських заняттях	5
Робота на практичних заняттях	5
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	<i>Відмінно – відмінне виконання лише з незначною кількістю помилок.</i> Здобувач вищої освіти виявляє особливі творчі здібності, вмє самостійно здобувати знання, без допомоги викладача знаходить та опрацьовує необхідну інформацію, вмє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні обдарування і нахили.
B	84-89	<i>Дуже добре – вище середнього рівня, але з кількома помилками.</i> 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	<i>Добре – загалом правильна робота, але з певною кількістю помилок.</i> Здобувач вищої освіти вмє 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	<i>Задовільно – непогано, але зі значною кількістю недоліків.</i> 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	<i>Достатньо – виконання задовольняє мінімальні вимоги.</i> Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.
FX	35-59	<i>Незадовільно – потрібна додаткова робота.</i> Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу
F	1-34	<i>Незадовільно – потрібна значна додаткова робота.</i> 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. проекту та заг. ред. проф. К.І. Беляков. Одеса: Видавничий дім «Гельветика». 2021. Т. 2. 432 с.
5. Енциклопедія соціогуманітарної інформології / коорд. проекту проф. К.І. Беляков. 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: ППШ, 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. Белякова. 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. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія. Київ: Едельвейс, 2014. 497 с.
4. Беляков К.І. Інформація в праві: теорія і практика. Київ: КВІЦ, 2006. 118 с.
5. Беляков К.І. Інформатизація в Україні: проблеми організаційного, правового та наукового забезпечення. Монографія. Київ: КВІЦ, 2008. 574 с.
6. Беляков К.І., Онопрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір. Монографія. Київ: КВІЦ, 2018. 168 с.
7. Грабар І.Г., Гришук Р.В., Молодецька К.В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. Житомир, 2019. 279 с.
8. 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.
9. Дзьобань О.П., Мануйлов Є.М. Інформаційна безпека в контексті інформаційної культури. Інформація і право. 2017. № 1(20). С. 74–81.
10. 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.
11. Кастельс М., Хіманен П. Інформаційне суспільство та держава добробуту. Фінська модель: пер. з англ. Київ: Ваклер, 2006. 230 с.
12. 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.
13. Кулеба Д.І. Війна за реальність. Як перемагати у світі фейків, правд і спільнот. Київ: Книголав, 2023. 480 с.
14. 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.
15. Мельник Д.С. Комп'ютерні злочини: проблеми виділення та кваліфікації. Міжнародний науковий журнал «Інтернаука». Київ, 2021, вип. 4 (104), С. 59-62. URL: <https://doi.org/10.25313/2520-2057-2021-4-7055>
16. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.
17. Почепцов Г.Г. Когнітивні війни у соцмедіа, масовій культурі та масових комунікаціях. Харків: Фоліо, 2019. 314 с.
18. Почепцов Г.Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Київ: Vivat, 2021. 384 с.
19. Разметаєва Ю.С. Цифрові права людини та проблеми екстратериторіальності в їх захисті. Право та державне управління. 2020. № 4. С. 12–23.
20. Сенченко М. Мас-медіа, піар, як засоби маніпуляції. Київ: Ліра К, 2022. 200 с.
21. 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.

22. Тихомиров О.О. Еволюція інформаційних прав людини. Інформація і право. 2023. № 1 (44). С. 50–57.

23. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави: монографія; заг. ред. Р. А. Калюжний. Київ: Центр навч.-наук. та наук. практ. видань НА СБ України, 2014. 196 с.

24. Тихомиров О.О. Інформаційна безпека: соціотехнічна парадигма. Інформаційна безпека людини, суспільства, держави. 2014. №1. С. 13-20.

25. Тихомиров О.О. Права людини: інформаційний вимір : монографія Одеса : Видавництво «Юридика», 2023. 304 с.

26. Тоффлер Е. Третя Хвиля / 3 англ. пер. А. Євса. Київ: Вид. дім «Всесвіт», 2000. 480 с.

27. Федчак І.А. Основи кримінального аналізу: навчальний посібник. Львів: Львівський державний університет внутрішніх справ, 2021. 288 с.

28. Фігель Ю.О. Проблеми обмеження права на доступ до інформації. Вісник ЛТЕУ. Юридичні науки. 2015. № 1. С. 132–139.

29. 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>

30. Hassan M. Framework Analysis – Method, Types and Examples. October 1, 2023. URL: <https://researchmethod.net/framework-analysis/>.

31. 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>

32. 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>

Інші джерела:

1. Керівні принципи у сфері прав людини для інтернет-провайдерів. URL: <https://tm.coe.int/1680599368>
2. Майбутнє, якого ми хочемо, Організація Об'єднаних Націй, яка нам потрібна. Оновлена інформація про роботу Канцелярії Спеціального радника з підготовки заходів з приводу 75-річчя ООН. Вересень 2020 року. URL: https://sozi.com.ua/image/catalog/home/laws/the_future_we_want.pdf
3. Національна доповідь «Цілі Сталого Розвитку: Україна». / Кабінет Міністрів України. URL: <https://www.kmu.gov.ua/storage/app/sites/1/natsionalna-dopovid-csr-Ukrainy.pdf>
4. Основи відновлення: Зміцнення інституційної спроможності. URL: <https://recovery.gov.ua/project/program/strengthening-institutional-capacity>
5. Основи відновлення: Цифрова держава. URL: <https://recovery.gov.ua/project/program/digital-government>
6. План Відновлення України. URL: <https://recovery.gov.ua/>
7. 10 Internet Rights & Principles. URL: <https://internetrightsandprinciples.org/campaign/>

8. Carta Portuguesa de Direitos Humanos na Era Digital. Lei n.º 27/2021, de 17 de maio. URL: https://www.parlamento.pt/Legislacao/Paginas/Educacao_Carta-Portuguesa-de-Direitos-Humanos-na-Era-Digital.aspx

9. Declaration of Principles Building the Information Society: a global challenge in the new Millennium. URL: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

10. Declaration on Human Rights and the Rule of Law in the Information Society. May, 13, 2005. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805da1a0

11. Digital democracy with a purpose. Lisbon declaration. URL: <https://www.lisbondeclaration.eu/>

12. European Declaration on Digital Rights and Principles for the Digital Decade. Brussels, 26.1.2022 COM(2022) 28 final. URL: <https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration>

13. The promotion, protection and enjoyment of human rights on the Internet. UN. General Assembly Resolution A/HRC/RES/32/13 URL: https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/32/13

14. The right to Internet access. Parliamentary Assembly Resolution 1987 (2014). Final version. URL: <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=20870&lang=en>

15. Transforming our world: the 2030 Agenda for Sustainable Development. General Assembly Resolution. 25 September 2015. URL: https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_70_1_E.pdf

16. Ukraine Reform Tracker. URL: <https://impact.economist.com/projects/ukraine-reform-tracker/>

17. World Summit on the Information Society. General Assembly Resolution. 31 January 2002. URL: https://digitallibrary.un.org/record/455403/files/A_RES_56_183-EN.pdf

18. World Summit on the Information Society. General Assembly Resolution. 22 December 2004. URL: https://digitallibrary.un.org/record/538071/files/A_RES_59_220-EN.pdf

Офіційні інформаційні ресурси:

1. Верховна Рада України – www.rada.gov.ua
2. Президент України – www.president.gov.ua
3. Кабінет Міністрів України – www.kmu.gov.ua
4. European Commission – <https://commission.europa.eu>
5. Council of Europe – <https://www.coe.int>

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

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