Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра інформаційного права та права інтелектуальної власності

ІНФОРМАЦІЙНА БЕЗПЕКА

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни	
Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*Всі галузі знань*
Спеціальність	*Всі спеціальності*
Освітня програма	*Всі ОПП*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (денна)*
Рік підготовки, семестр	*3 курс, осінній або весінній семестр*
Обсяг дисципліни	*2 кредити (60 годин). Лекцій 18 годин, семінарські 18 годин, СРС 24 години*
Семестровий контроль/ контрольні заходи	*Залік, МКР*
Розклад занять	*Лекційні заняття (2 год.) – щотижня* *Семінарські заняття (2 год.) – щотижня*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *доцент, к.т.н, старший науковий співробітник, Фурашев Володимир Миколайович, e-mail: vfurashev@gmail.com.* Практичні / Семінарські**:** *доцент, к.т.н, старший науковий співробітник, Фурашев Володимир Миколайович, e-mail: vfurashev@gmail.com.*
Розміщення курсу	http://ipp.kpi.ua/

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчання та результати навчання

Розвиток сучасних інформаційно-комунікаційних технологій загострює проблеми які пов’язані з негативним впливом інформації на свідомість людини, як на державному так і світовому рівні. Відповідно до положень статті 17 Конституції України, забезпечення інформаційної безпеки України є справою усього українського народу.

Розуміння природи та сутності процесів та процедур, які відбуваються у наступний час в інформаційному просторі, впливу цих процесів та процедур на процеси забезпечення інформаційної безпеки людини, суспільства держави є одним з головних запобіжних шляхів превентивного запобігання інформаційної небезпеки та її наслідків.

Виходячи з цього, головною метою навчальної дисципліни «Інформаційна безпека» є:

- надання основоположних знань щодо сутності, проявів, наслідків та механізмів інформаційної безпеки, виникнення, у зв’язку з цим, особливостей правовідносин в інформаційній сфері;
- опанування базовими знаннями щодо механізмів правового забезпечення запобігання та усунення загроз в інформаційній сфері, спрямованими на формування здатності

розв’язувати складні спеціалізовані задачі та практичні проблеми у сфері поводження з інформацією на всіх етапах забезпечення здійснення її обороту;

- опанування базовими знаннями класифікації та правової оцінки дій суб`єктів суспільних відносин в сфері інформаційної діяльності.

Ключовими аспектами навчальної дисципліни є розуміння:

- природи інформації та її властивостей;
- сутності прийомів та методів маніпулювання свідомістю людини;
- сутності інформаційного насильства та його запобігання;
- ролі інформації та інформаційної безпеки у забезпеченні національної та міжнародної безпеки:

Комунікація з викладачем можлива і заохочуватиметься на навчальних заняттях, а також в межах двох годин консультацій з викладачем, які проводяться за графіком, доступним на сайті кафедри інформаційного права та права інтелектуальної власності.

Відповідно до вимог ОПП **метою дисципліни** є підсилення у студентів наступних здатностей:

- Здатність до абстрактного мислення, аналізу та синтезу.
- Навички використання інформаційних і комунікаційних технологій.
- Здатність вчитися і оволодівати сучасними знаннями (ЗК7).
- Здатність бути критичним і самокритичним.
- Здатність реалізувати свої права і обов’язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
- Повага до честі і гідності людини як найвищої соціальної цінності, розуміння їх правової природи.

Завданням дисципліни є формування таких результатів навчання**:**

1) знань:

- сутності основних понять, їх тотожностей та відмінностей у сфері інформаційної безпеки;
- взаємозв’язки інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;
- основи державної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки;
- реальні та потенційні загрози у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;
- основні методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;

- основні положення юридичної відповідальності за правопорушення в інформаційній сфері;
- зміст основних міжнародних договорів з питань інформаційної безпеки;
- основні проблеми правового забезпечення інформаційної безпеки.

2) уміння:

- Визначати переконливість аргументів у процесі оцінки заздалегідь невідомих умов та обставин.
- Здійснювати аналіз суспільних процесів у контексті аналізованої проблеми і демонструвати власне бачення шляхів її розв'язання.
- Пояснювати характер певних подій та процесів з розумінням професійного та суспільного контексту.
- Вільно використовувати для професійної діяльності доступні інформаційні технології і бази даних.
- Пояснювати природу та зміст основних правових явищ і процесів (УМ20).
- Застосовувати зазначені акти та інформаційно-правові положення у практичній діяльності, у тому числі, і під час розробки, впровадження та використання інформаційних технологій.
- Знаходити протиріччя та не вирішені питання правового регулювання суспільних відносин у сфері забезпечення інформаційної безпеки з метою їх вирішення.
- Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності з урахуванням вимог забезпечення інформаційної безпеки.

В результаті засвоєння дисципліни студенти зможуть:

- Здійснювати аналіз суспільних процесів у контексті аналізованої проблеми і демонструвати власне бачення шляхів її розв'язання.
- Проводити збір і інтегрований аналіз матеріалів з різних джерел.
- Формулювати власні обґрунтовані судження на основі аналізу відомої проблеми.
- Давати короткий висновок щодо окремих фактичних обставин (даних) з достатньою обґрунтованістю.
- Оцінювати недоліки і переваги аргументів, аналізуючи відому проблему.
- Використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин.
- Доносити до респондента матеріал з певної проблематики доступно і зрозуміло.
- Пояснювати характер певних подій та процесів з розумінням професійного та суспільного контексту.
- Застосовувати набуті знання у різних правових ситуаціях, виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки, які виникають під час здійснення процесів та процедур основної виробничої діяльності.

2. Пререквізити та постреквізити дисципліни (місце в структурно-логічній схемі навчання за відповідною освітньою програмою)

Для вивчення дисципліни від студента не вимагається знання визначених юридичних або інших спеціалізованих знань.

3. Зміст навчальної дисципліни

Денна форма навчання

№ п\п	Змістовні модулі	Кількість годин				
		Всього	Лекції	Практ. занят.	Індив. занят.	Самост. робота
1	**2**	**3**	**4**	**5**	**6**	**7**
	Розділ 1. Основи інформаційної безпеки					
1.1.	Інформація як джерело небезпеки. ❑	4	2	2	-	-
1.2.	Інформаційна діяльність як об'єкт небезпеки. ❑	10	2	4	-	4
1.3.	Кібернетична безпека як складова інформаційной безпеки. ❑	6	2	2	-	2
1.4.	Інтернет та інформаційна безпека. ❑	6	2	2	-	2
1.5.	Інформаційна безпека в системі забезпечення національної та міжнародної безпеки. ❑	4	2	-	-	2
	МКР	-	-	-	(1)	-
	Всього за розділом:	**30**	**10**	**10**	**(1)**	**10**
	Розділ 2. Правове забезпечення інформаційної безпеки					
2.1.	Законодавче забезпечення безпекового обороту інформації. ❑	8	2	2	-	4
2.2.	Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.❑	6	2	2	-	2
2.3.	Основні законодавчі положення у сфері забезпечення інформаційної безпеки, кібербезпеки. ❑	8	2	2	-	4
2.4.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки. ❑	6	2	2	-	2
	МКР				(1)	
	Всього за розділом:	**28**	**8**	**8**	**(1)**	**12**
	Залік:	2	-	(2)	-	2
	Разом:	**60**	**18**	**18**	**(3)**	**24**

❑ Лекція та семінарське заняття проводяться із застосуванням мультимедійних засобів навчання.

Заочна форма навчання

п\п	Змістовні модулі	Кількість годин				
		Всього	Лекції	Практ. занят.	Індив. занят.	Самост. робота
1	**2**	**3**	**4**	**5**	**6**	**7**
	Розділ 1. Основи інформаційної безпеки					
1.1.	Інформація як джерело небезпеки. ❑	4	2	-	-	2
1.2.	Інформаційна діяльність як об'єкт небезпеки. ❑	10	-	2	-	8
1.3.	Кібернетична безпека як складова інформаційной безпеки. ❑	6	-	-	-	6
1.4.	Інтернет та інформаційна безпека. ❑	6	2	-	-	4
1.5.	Інформаційна безпека в системі забезпечення національної та міжнародної безпеки. ❑	4	-	-	-	4
	Всього за розділом:	**30**	**4**	**2**	-	**24**
	Розділ 2. Правове забезпечення інформаційної безпеки					
2.1.	Законодавче забезпечення безпекового обороту інформації. ❑	8	-	-	-	8
2.2.	Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.❑	6	-	-	-	6
2.3.	Основні законодавчі положення у сфері забезпечення інформаційної безпеки, кібербезпеки. ❑	8	2	-	-	6
2.4.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки. ❑	6	-	-	-	6
	МКР				(3)	
	Всього за розділом:	**28**	**2**	**-**	-	**26**
	Залік:	2	-	(**2**)	-	2
	Разом:	**60**	**6**	**2**	**(3)**	**52**

❑ Лекція та семінарське заняття проводяться із застосуванням мультимедійних засобів навчання.

4. Навчальні матеріали та ресурси

Для успішного вивчення дисципліни достатньо опрацьовувати навчальний матеріал, який викладається на лекціях та наведений у «Конспекті лекції», а також доцільно ознайомитися з:

1. Додонов А.Г. Распознавание информационных операций / А.Г. Додонов, Д.В.Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. – К.: ООО «Инжиниринг» , 2017. – 282 с. – URL: http://dwl.kiev.ua/art/riop/riop.pdf
2. Фурашев В.М. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє / Фурашев В.М., Ланде Д.В., Григор'єв О.М., Фурашев О.В. - К.: Преса України, 2005. - 166 с. - URL: http://dwl.kiev.ua/art/monogr/vs_ukr.pdf
3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII / Верховна Рада України. *Відомості Верховної Ради України.* 2017. № 45. Ст.403.
4. Стратегія національної безпеки України : Указ Президента України від 26.05.2015 р. № 287/2015/ Президент України. *Офіційний вісник України*. 2015. № 43. С. 14. Ст. 1353.
5. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017 / Президент України. *Офіційний вісник Президента України.* 2017. № 5. С. 15. Ст. 102.

Для пошуку необхідної літератури та НПА необхідно використовувати офіційні інтернет-портали:

- https://www.rada.gov.ua/
- https://www.library.kpi.ua/resources/
- http://ippi.org.ua/golovne-menyu/vidannya

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

5.1 Денна форма навчання

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань (завдання на СРС)
1	**Тема 1.1. Інформація як джерело небезпеки.** Основні загальносвітові тенденції розвитку суспільства та їх вплив на напрями розвитку українського суспільства. Основні причини та механізми міждержавних, міжблокових та міжрегіональних сучасних протистоянь. Природа та визначення інформації. Носії інформації. Засоби передачі та сприйняття інформації. Властивості інформації. Сутність та визначення поняття «безпека інформації» та «безпечність інформації». Сутність та визначення поняття «інформаційна безпека». Критерії визначення об'єктів інформаційної небезпеки та їх обґрунтування. Ієрархія об'єктів інформаційної небезпеки. Реальні та потенційні загрози в інформаційній сфері. Сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя».
2	**Тема 1.2. Інформаційна діяльність як об'єкт небезпеки.**

	Сутність, поняття та правове визначення поняття «інформаційна діяльність». Складові інформаційної діяльності. Засоби та їх структура здійснення інформаційної діяльності. Взаємозв'язок інформаційної діяльності та інформаційної безпеки. Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства. Маніпулювання свідомістю, сутність та види маніпуляції. Роль та місце маніпулювання в національних системах державного управління та політичних системах, а також у формуванні та здійсненні міжнародних стосунків. Сутність та прояви інформаційного насильства. Проблемні питання правового запобігання здійсненню інформаційного насильства.
3	**Тема 1.3. Кібернетична безпека як складова інформаційної безпеки.** Кібернетика як джерело небезпеки. Процеси створення та впровадження інформаційно-комунікаційних технологій (ІКТ) як об'єкт і предмет правового регулювання. Безпека глобальних інформаційних систем та мереж. Визначення поняття «кібернетична безпека» (кібербезпека). Сутність та поняття інтернет-речей, DL-технологій, GRID, «блокчейн» та крипто-технології вільного доступу. Трансформація кіберзагроз в сучасних умовах. Об'єкти інформаційних загроз. Об'єкти кіберзагроз. Сутність зв`язку інформаційної безпеки та кібербезпеки.
4	**Тема 1.4. Інтернет та інформаційна безпека.** Особливості встановлення та проблеми реалізації інформаційних правовідносин в мережі Інтернет. Сутність, витоки та механізми трансформаційних процесів забезпечення національної та міжнародної безпеки. Сутність, витоки та механізми глобалізації інформаційного простору. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері. Поняття та сутність інформаційного суверенітету. Сучасні та потенційні проблемні питання правового забезпечення інформаційного суверенітету та можливі шляхи їх вирішення. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення. Витоки та сутність кіберсоціалізації. Соціальні мережі. Мережева мобілізація: питання демократії та безпеки. Наслідки кіберсоціалізації. Сутність поняття «кіберцивілізація». Потенційні загрози кіберцивілізації для людства. Поняття кіберзлочинності. Про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. № 994-575. Сутність та визначення поняття «кібертероризм». Відображення кібертероризму в законодавстві України.
5	**Тема 1.5. Інформаційна безпека в системі забезпечення національної та міжнародної безпеки.** Спрямованість та зміст законодавчих змін у сфері забезпечення національної безпеки. Причинно-наслідкові зв'язки, види та правові засади регіональних та міжнародних систем колективної безпеки. Права і свобода людини, громадянина та їх обов'язки в інформаційній сфері. Права суспільства та обов'язки держави в інформаційній сфері. Дилема забезпечення прав і свобод людини, громадянина та прав суспільства із забезпеченням інформаційної безпеки. Транскордонність забезпечення інформаційної безпеки.

	Корупція як головна загроза забезпечення інформаційної безпеки на всіх рівнях – національному, регіональному та міжнародному.
6	**Тема 2.1. Законодавче забезпечення безпекового обороту інформації.** Сутність поняття «правове забезпечення». Складові правового забезпечення та їх зміст. Зміст правового забезпечення інформаційної безпеки та її складової – кібербезпеки. Роль та значення категорійно-понятійного апарату в системі правового забезпечення інформаційної безпеки. Правові гарантії безпекового обороту інформації. Правові обмеження щодо створення, поширення, збереження, обробки та знищення інформації. Інформаційний ресурс як об'єкт інформаційної небезпеки.
7	**Тема 2.2. Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.** Основні ознаки відмінностей індустріального та постіндустріального суспільств. Тенденції розвитку постіндустріального суспільства. Трансформація правовідносин у постіндустріальному суспільстві. Реальні та потенційні загрози в інформаційній сфері у постіндустріальному суспільстві. Характеристика основних положень: - Воєнної доктрини України; - Доктрини інформаційної безпеки України; - Концепції розвитку сектору безпеки і оборони України. - Стратегії національної безпеки України; - Стратегії кібербезпеки України Характеристика основних положень Закону України «Про основні засади забезпечення кібербезпеки України».
8	**Тема 2.3. Основні законодавчі положення у сфері забезпечення інформаційної безпеки, кібербезпеки.** Основні законодавчі положення у сфері: - забезпечення захисту інформації; - убезпечення від «шкідливої» інформації людину, суспільство, державу; захисту персональних даних.
9	**Тема 2.4. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки.** Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.

Семінарські (практичні) заняття

Основними завданнями циклу практичних (семінарських) занять є:

- оцінка засвоєння студентами лекційного матеріалу;
- оцінка виконання студентами завдань на СРС;
- набуття досвіду підтримування на фаховому рівні дискусій щодо актуальних питань інформаційної безпеки, а також особливостей правового регулювання суспільни**х** відносин в сфері забезпечення інформаційної безпеки.

№ з/п	Назва теми заняття та перелік основних питань (перелік дидактичного забезпечення, питання для поточного контролю та завдання на СРС)
1	**Тема 1.1. Інформація як джерело небезпеки.** *Питання для розгляду:* 1. Основні трансформаційні процеси сучасності з точки зору безпеки людини. 2. Основні трансформаційні процеси сучасності з точки зору безпеки суспільства. 3. Основні трансформаційні процеси сучасності з точки зору безпеки держави. 4. Що таке війна? 5. Чім війна відрізняється від збройного конфлікту? 6. Основні види війн. 7. Основні цілі та завдання сучасних війн. 8. У зв'язку з чим відбуваються трансформаційні процеси організації та проведення локальних і регіональних конфліктів та війн. 9. Характерні ознаки гібридних війн. 10. Основна спрямованість трансформаційних процесів організації та проведення локальних та регіональних конфліктів і війн. 11. Предмет інформаційної безпеки. 12. Основні завдання інформаційної безпеки. 13. Природа та сутність інформації. Визначення поняття «інформація» з точки зору інформаційної безпеки. 14. Законодавче визначення поняття «інформація». 15. Основні властивості інформації з позиції інформаційної безпеки. 16. Сутність та визначення поняття «безпека інформації». 17. Сутність та визначення поняття «безпечність інформації». 18. Сутність та визначення поняття «захист інформації». 19. Сутність та визначення поняття «інформаційна безпека». 20. Об'єкти інформаційної небезпеки та їх ієрархія. 21. Сутність поняття «загроза». 22. Сутність поняття «загроза» в інформаційної сфері. 23. Сутність понять «інформаційний вплив», «інформаційна війна», «інформаційна зброя». 24. Сутність поняття «інформаційна операція». Наведіть приклади. 25. Сутність поняття «спеціальна інформаційна операція». Наведіть приклад. 26. Сутність поняття «експансія». 27. Сутність поняття «інформаційна експансія». Наведіть приклади. 28. Сутність понять «насильство», «жорстокість», «порнографія». 29. Основні загрози національної та міжнародної безпеці в сфері інформаційнії безпеки.
2-3	**Тема 1.2. Інформаційна діяльність як об'єкт небезпеки.** *Питання для розгляду:* 1. Розкриття сутності інформаційної діяльності. 2. Законодавче визначення поняття «інформаційна діяльність».

	3. Суб'єкти здійснення інформаційної діяльності. 4. Засоби здійснення інформаційної діяльності та їх структура. 5. Розуміння поняття «інформаційна інфраструктура». 6. Основні напрями інформаційної діяльності. 7. Основні види інформаційної діяльності. 8. Чинники, які визначають ступінь ефективності проведення інформаційної діяльності. 9. Сутність інформаційного моделювання. 10. Зміст інформаційної експертизи. 11. Складові інформаційної діяльності. 12. Сутність інформаційного виробництва. 13. Основні елементи інформаційного виробництва. 14. Поняття інформаційного забруднення. 15. Поняття інформаційного середовища. 16. Ієрархічні рівні інформаційного середовища. 17. Основні функції інформаційного середовища. 18. Поняття інформаційного продукту. 19. Взаємозв'язок інформаційної діяльності та інформаційної безпеки. 20. Характерні риси постіндустріального суспільства з точки зору здійснення інформаційної діяльності. 21. Перспективи та напрями розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки. 22. Сутність поняття «маніпуляція». 23. Види маніпуляції та розкриття їх сутність. 24. Роль та місце маніпулювання в системі державного управління (з наведенням конкретних прикладів). 25. Роль та місце маніпулювання в політичних системах (з наведенням конкретних прикладів). 26. Роль та місце маніпулювання у здійсненні міжнародних стосунків (з наведенням конкретних прикладів). 27. Сутність інформаційного насильства. 28. Прояви інформаційного насильства (з наведенням конкретних прикладів). 29. Тотожності та відмінності процесів маніпулювання свідомістю людини та інформаційного насильства. 30. Чинники, які створюють проблемні питання правового запобігання здійсненню інформаційного насильства.
4	**Тема 1.3. Кібернетична безпека, як складова інформаційної безпеки.** *Питання для розгляду:* 1. Кібернетика як джерело небезпеки. 2. Визначення поняття «кібернетична безпека» (кібербезпека). 3. Сутність та визначення поняття «система». Наведіть приклади. 4. Сутність та визначення поняття «інформаційна система». Наведіть приклади. 5. Сутність та визначення поняття «технологія». Наведіть приклади. 6. Сутність поняття «комунікація». Наведіть приклади. 7. Сутність поняття «комунікаційна система». Наведіть приклади. 8. Сутність та визначення поняття «інформаційно-комунікаційна система». 9. Сутність та визначення поняття «інформаційна технологія». Наведіть приклади. 10. Чинники, які вказують на особливості сучасних інформаційних відносин. 11. Чинники, які вказують на об'єктність та предметність правового регулювання ІКТ. 12. Сутність процесів забезпечення безпеки глобальних інформаційних систем та мереж. 13. Сутність та поняття «Інтернет речей». 14. Що розуміємо під словосполученням «взаємодія M2M»? 15. Які основні недоліки породжує взаємодія M2M?

	16. Сутність технології «блокчейн». 17. Сутність DL-технології. 18. Дефініція поняття «інформаційна діяльність». 19. Суб'єкти здійснення інформаційної діяльності. 20. Засоби здійснення інформаційної діяльності. 21. Структура засобів здійснення інформаційної діяльності. 22. Дефініція поняття «інформаційна безпека» та її основні об'єкти. 23. Дефініція поняття «кібербезпека» та її основний об'єкти. 24. У чому полягають основні тотожності та відмінності процесів забезпечення інформаційної безпеки та кібербезпеки.
5	**Тема 1.4. Інтернет та інформаційна безпека.** *Питання для розгляду:* 1. Сутність та витоки глобалізації. 2. Сутність та витоки глобалізації інформаційного простору. 3. Сутність поняття «суверенітет». 4. Види суверенітету. 5. Сутність (принципи) інформаційного суверенітету. 6. Законодавче визначення поняття «інформаційний суверенітет держави». 7. Складові здійснення інформаційного суверенітету України. 8. Шляхи забезпечення інформаційного суверенітету України. 9. Проблемні питання забезпечення інформаційного суверенітету України. 10. Сутність та визначення поняття «соціалізація». 11. Сутність та визначення поняття «цивілізація». 12. Сутність поняття «кіберсоціалізація». 13. Сутність поняття «кіберцивілізація». 14. Витоки загроз для особистості в умовах кіберсоціалізації. 15. Загрози для суспільства, держави, соціалізації особистості в умовах кіберцивілізації. 16. Сутність та визначення поняття «кіберзлочин». 17. Сутність та визначення поняття «кіберзлочинність». 18. Сутність та визначення поняття «кіберпростір». 19. Дефініція поняття «тероризм». 20. Природа тероризму. 21. Дефініція поняття «терористичний акт». 22. Дефініція поняття «кіберпростір». 23. Чим приваблює кіберпростір терористів? Відображення кібертероризму в законодавстві України
6	**Тема 2.2. Законодавче забезпечення безпекового обороту інформації.** *Питання для розгляду:* 1. Сутність поняття «правове забезпечення» та його складові. 2. Розкриття сутності поняття «безпековий оборот інформації». 3. Що означає поняття «життєвий цикл інформації»? 4. Що розуміємо під поняттям «правові гарантії обороту інформації»? 5. У зв`зку з чим існують правові обмеження збір, зберігання та поширення певної інформації? 6. Інформація якої спрямованості обмежується у поширенні, збиранні та зберігання на законодавчому рівні? 7. Яка мотивація обмеження обороту певної інформації?Сутність та визначення поняття «інформаційний ресурс». 9. Які властивості притаманні інформресурсам?

	10. Основні функції інформресурсів.
7	**Тема 2.3. Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.** *Питання до розгляду:* 1. Поняття «індустріальне суспільство» та його характерні ознаки. 2. Поняття «постіндустріальне суспільство» та його характерні ознаки. 3. Основні тенденції розвитку постіндустріального суспільства та їх вплив на трансформацію суспільних відносин. 4. Характер реальних та потенційних загрозз в інформаційній сфері у постіндустріальному суспільстві. 5. Дефініція поняття «доктрина». 6. Актуальні воєнні загрози для України з використанням властивостей інформації, які знайшли своє відображення у Воєнної доктрині України. 7. Воєнно-політичні виклики із застосуванням властивостей інформації, які можуть перерости в загрозу застосування воєнної сили проти України. 8. Сценарії реалізації загроз воєнної безпеці України із застосуванням властивостей інформації за версією Воєнної доктрини України. 9. Мета Доктрини інформаційної безпеки України. 10. Національні інтереси України в інформаційній сфері, які відображені у Доктрині інформаційної безпеки України. 11. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері відповідно до положень Доктрини інформаційної безпеки України. 12. Пріоритети державної політики в інформаційній сфері у частині забезпечення інформаційної безпеки. 13. Дефініція поняття «концепція». 14. Що визначає Концепція розвитку сектору безпеки і оборони України та її мета? 15. Які безпекові виклики що можуть посилювати загрозу застосування воєнної сили проти України розглядає Концепція розвитку сектору безпеки і оборони України? 16. Дефініція поняття «стратегія». Механізми реалізації стратегії. 17. Основні цілі Стратегії національної безпеки України та Які основні загрози у сфері забезпечення інформаційної безпеки та кібербезпеки, а також безпеці інформаційних ресурсів, визначає Стратегія національної безпеки. 18. Які пріоритети у сфері забезпечення інформаційної безпеки відповідно до Стратегії національної безпеки?
8	**Тема 2.4. Основні законодавчі положення у сфері забезпечення інформаційної безпеки, кібербезпеки.** *Питання до розгляду:* 1. Основоположні положення Конституції України щодо поводження з інформацією. 2. Основні принципи інформаційних відносин. 3. Що означає режим доступу до інформації? 4. Які права мають громадяни щодо збору інформації про них? 5. Які документи та інформація не підлягають обов'язковому наданню для ознайомлення за інформаційними запитами? 6. У чому полягає неприпустимість зловживання правом на інформацію? 7. Дефініція поняття «персональні дані». Об'єкти захисту у сфері персональних даних? 8. Сутність поняття «інформаційні правовідносини»? 9. Сутність поняття «інформаційно-інфраструктурні відносини». 10. З чим пов’язані інформаційно-інфраструктурні відносини? 11. Статус та основні завдання Державної служби спеціального зв’язку та захисту

	інформації України? 12. Яким нормативно-правовим актом регулюються відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах? 13. Об'єкти захисту в телекомунікаційних та інформаційно-телекомунікаційних системах?
9	**Тема 2.4. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки.** *Питання до розгляду:* 1. Сутність поняття «соціальна відповідальність». Дефініція поняття «юридична відповідальність». 2. Сутність поняття «цивільно-правова відповідальність». 3. Основні напрями дій, які віднесені до правопорушень в інформаційної сфері відповідно до положень Господарського кодексу України. 4. Види адміністративних стягнень. 5. Основні напрями дій, які віднесені до правопорушень в інформаційної сфері відповідно до положень Цивільного кодексу України. 6. Основні напрями дій, які віднесені до правопорушень в інформаційної сфері відповідно до положень Кодексу України про адміністративні правопорушення. 7. Сутність поняття «кримінальна відповідальність». 8. Сутність поняття «кримінальне покарання». 9. Основні напрями дій, які віднесені до правопорушень в інформаційної сфері відповідно до положень Кримінального кодексу України. 10. Власна оцінка ступеня повноти та адекватності відображення у національному законодавстві правопорушень в сфері забезпечення інформаційної безпеки та кібербезпеки.

6. Самостійна робота студента

Самостійна робота студента (СРС) передбачає самостійне, на основі зазначених питань віднесених до розгляду на практичному (семінарькому) занятті, з використанням лекційного матеріалу і рекомендованої літератури.

Особливу увагу слід звернути на підготовку практичних (семінарських) занять за тематикою, яка, відповідно до положень розділу 3 «Зміст навчальної програми», не передбачає проведення лекційного заняття. У даному випадку, студенти, орієнтуючись на перелік питань до розгляду на даному практичному (семінарському) заняттю та тих, що віднесені до завдань на СРС, використовуючи конспект лекцій та рекомендовану літературу з даної тематики, а також будь-які інші джерела інформації, повністю самостійно готуються до проведення заняття.

У разі виникнення складнощів під час підготовки до проведення практичного (семінарського) заняття студент повідомляє про це викладача, а останній проводить індивідуальну або групову консультацію. Консультація може проводитися як очно, та й заочно з використанням засобів інформаційно-комунікаційних технологій.

Перевірка рівня засвоєння матеріалу для самостійного опрацювання проводиться в процесі обговорення питань із близьких до визначеної теми на аудиторних заняттях.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Порушення термінів виконання завдань та заохочувальні бали

Ключовими заходами при викладанні дисципліни є ті, які формують семестровий рейтинг студента.
Штрафних балів з дисципліни не передбачається.
Заохочувальні бали у розмірі 10 балів студент може отримати за підготовку тез виступу на наукової конференції за тематикою навчальної дисципліни.

Відвідування занять
Відвідування лекційних та семінарських занять є обов`язковим, за виключенням поважних причин. Бали за присутність на лекціях не додаються. За відвідування семінарських занять студенти також не отримують бали, але головна частина рейтингу студента формується через активну участь у семінарських заняттях й підготовленість до них.

Пропущені контрольні заходи оцінювання
Пропущені заходи оцінювання знань студентом(ами) по темі навчальної дисципліни вирішується шляхом домовленості між викладачем та студентами щодо порядку здійснення усунення заборгованості.

Календарний контроль
Метою проведення календарного контролю є підвищення якості навчання студентів та моніторинг виконання графіка освітнього процесу студентами.

Критерій	Перший календарний контроль	Другий календарний контроль
Термін календарного контролю	8-ий тиждень	14-ий тиждень
Умови позитивного отримання	≥ 20 балів	≥ 45бал

Академічна доброчесність
Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

Норми етичної поведінки
Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: https://kpi.ua/code.

8. Види контролю та рейтингова система оцінювання результатів навчання (РСО)

Поточний контроль: оцінка знань за кожною темою заняття, оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу по кожному розділу навчальної дисципліни (частини 1 та 2 МКР).

Оцінювання якості та глибини розкриття поставленого питання під час проведення практичних занять здійснюється відповідно до наступних положень:

активна участь у проведенні заняття; надання повної і аргументованої, логічно викладеної доповіді, відповіді, висловлення власної позиції з дискусійних питань або повністю правильне вирішення задачі з відповідним	8

обґрунтуванням, у поєднанні зі слушними доповненнями відповідей інших студентів у процесі дискусії	
активна участь у проведенні заняття; надання правильних відповідей або правильне вирішення задач з незначними неточностями	7
суттєве доповнення відповідей студентів	6
надання відповідей з чисельними значними похибками	4
неспроможність надання відповіді на поставлене питання	0

Програмою навчальної дисципліни передбачено проведення модульної контрольної роботи (МКР) з двох частин. Частина перша МКР виконується по розділу 1, частина друга – по розділу 2.

Написання МКР має на меті перевірку рівня засвоєння студентами матеріалів, отриманих на момент її проведення.

Головною метою МКР є визначення ступеня розуміння студентом природи, сутності, визначення того чи іншого явища, процесу, процедури у сфері інформаційної безпеки на основі отриманого навчального матеріалу, а також визначення здібності студента до чіткості та лаконічності формулювання власної думки у розкритті поставленого питання.

Написання частини МКР передбачає письмове викладення у довільної формі одного з питань визначеного викладачем за тематикою відповідного розділу навчальної дисципліни. Тематика визначеної частини МКР надається викладачем індивідуально кожному студенту під час проведення контрольної перевірки рівня засвоєння пройденого матеріалу.

Перелік питань, які пропонуються студентам у якості тематики МКР, формується на основі переліку тематичних питань до лекційних занять та питань для самоперевірки.

Написання МКР здійснюється протягом академічної години під час проведення передостаннього практичного (семінарського) заняття за даним розділом навчальної дисципліни.

Під час написання МКР суворо забороняється використання будь-яких засобів сучасних інформаційно-комунікаційних технологій (ІКТ). Порушення цього положення веде до автоматичного не розгляду та не зарахування даної МКР.

Під час однієї академічної години останнього практичного (семінарського) заняття за даним розділом навчальної дисципліни відбувається розгляд та обговорення виконаних МКР. Студенти мають можливість звернути увагу на ті питання, розв’язання яких викликало у них певні складності. Викладач має можливість дати студенту конкретне індивідуальне завдання на відпрацювання недостатньо засвоєного матеріалу.

Оцінювання якості та глибини розкриття поставленого питання здійснюється відповідно до наступних положень:

письмове тестування ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням повної і аргументованої, логічно викладеної відповіддю на поставлене питання	18
письмове тестування ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням відповіді на поставлене питання з незначними неточностями або порушеннями логіки	16
письмове тестування ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням неповної відповіді на поставлене питання	12
письмове тестування ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням відповіді на поставлене питання з чисельними	9

значними похибками	
письмове тестування ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням не повної відповіді на поставлене питання з чисельними значними похибками	0

Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.
Семестровий контроль: залік.
Умови допуску до семестрового контролю: необхідною умовою допуску до заліку є підсумковий рейтинг за семестр не менше 40 балів.
При наявності підсумкового рейтингу рівного або більше 60 балам та згоди студента підсумкова оцінка формується у автоматичному режимі.

Система оцінювання

№ з/п	Контрольний захід оцінювання	%	Ваговий бал	Кіл-ть	Всього
1.	Оцінювання знань студентів по кожної темі навчального плану	64	8	8	64
2.	Оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу по кожному розділу навчальної дисципліни	36	18	2	36
	Всього				100

При наявності підсумкового рейтингу у межах 40-59 балів або висловлені студентом бажання підвищення кількості балів залік відбувається у режимі жорсткого РСО (попередні бали анулюються)
Залік складається з двох самостійних етапів.

Вид завдання	Статус	Бали
Відповідь на п`ять теоретичних питань в аудиторному режимі.	Обов`язкове	85
Вирішення ситуаційного завдання	факультативно	15

Теоретичне питання
Викладач може поставити до 2-ох уточнюючих запитань.

Ваговий бал	Критерій оцінювання
8-17	Студент розкрив тему на високому рівні. Володіє основними поняттями, класифікацією які охоплюються змістом питання. Може навести порівняльно-правову характеристику. Знає нормативно-правове регулювання. Відповідав

	логічно та послідовно, продемонстрував вміння застосовувати наукові методи, відповідь містить обґрунтовані висновки.
10-16	Студент розкрив тему на задовільному рівні. Здобувач вказав основні поняття та нормативно-правові акти. У відповіді висновки обґрунтовано неповністю.

Вирішення ситуаційного завдання

Ваговий бал	Критерій оцінювання
15	Здобувач розкрив завдання на високому рівні. Самостійно і логічно структурував відповідь, вірно визначив суб'єктів правовідносин, класифікував запропоновані у завданні процеси, питання виклав послідовно, продемонстрував вміння застосовувати наукові методи, у роботі є самостійні, обґрунтовані висновки. Здобувач вірно визначив правовідносини, сформулював предмет, поняття та окреслив права та обов'язки сторін в межах фабули.
12-14	Студент розкрив тему на достатньому та задовільному рівні. Матеріал викладено логічно у відповіді висновки обґрунтовано неповністю. Здобувач вірно визначив правовідносини, частково сформулював предмет, поняття та окреслив права та обов'язки сторін в межах фабули.
5-11	Студент не розкрив задачу (кейс) на достатньому рівні, відповідь не містить посилань на нормативно-правові акти. Робота не містить обґрунтованих висновків.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	*Оцінка*
100-95	Відмінно
94-85	Дуже добре
84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

Орієнтовні питання до заліку

1. Основні трансформаційні процеси сучасності з точки зору інформаційної безпеки.
2. Тотожності та відмінності сутностей війни та збройного конфлікту. Основні види війн. Основні цілі та завдання сучасних війн.
3. Витоки трансформаційних процесів організації та проведення локальних та регіональних конфліктів та війн. Характерні ознаки гібридних війн.
4. Основна спрямованість трансформаційних процесів організації та проведення локальних та регіональних конфліктів та війн.

5. Основні базові положення Доктрини інформаційної безпеки України, які відображають трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн.
6. Предмет та основні завдання інформаційної безпеки.
7. Природа та сутність інформації. Визначення поняття «інформація» з точки зору інформаційної безпеки. Законодавче визначення поняття «інформація».
8. Основні властивості інформації з позиції інформаційної безпеки. Сутність та визначення понять «безпека інформації» та «захист інформації».
9. Сутність та визначення поняття «інформаційна безпека». Об'єкти інформаційної небезпеки та їх ієрархія.
10. Сутність понять «права людини», «свобода людини» та «обов'язок людини».
11. Спрямованість законодавче визначені обмеження прав людини та громадянина в інформаційної сфері.
12. Сутність прав людини та прав суспільства в інформаційної сфері.
13. Обов'язки держави в інформаційної сфері. Сутність та поняття цензури.
14. Чому говоримо про права і свободи людини, але не говоримо про свободу суспільства, а по відношенню до держави – лише про обов'язки?
15. Взаємозв'язок між забезпеченням прав і свобод людини, громадянина в інформаційної сфері та забезпеченням інформаційної безпеки.
16. Відображення терміну «інформаційна безпека» у законодавстві України. Законодавче визначення поняття «інформаційна безпека».
17. Зв'язок сутності понять «кібернетика» та «небезпеки».
18. Сутність поняття «інформаційний простір» та його властивості.
19. Сутність поняття «кібернетичний простір» («кіберпростір») та його властивості.
20. Сутність та визначення поняття «кібербезпека».
21. Взаємозв'язок інформаційної безпеки та кібербезпеки. Ознаки коректності застосування термінів «інформаційна безпека» та «кібербезпека».
22. Сутність та законодавче визначення поняття «інформаційна діяльність». Основні види та напрями інформаційної діяльності.
23. Чинники які визначають ступінь ефективності проведення інформаційної діяльності.
24. Сутність інформаційного моделювання. Зміст інформаційної експертизи.
25. Складові інформаційної діяльності. Сутність інформаційного виробництва. Основні елементи інформаційного виробництва.
26. Взаємозв'язок інформаційної діяльності та інформаційної безпеки.
27. Характерні риси постіндустріального суспільства з точки зору здійснення інформаційної діяльності.
28. Перспективи та напрями розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки.
29. Сутність поняття «маніпуляція». Види маніпуляції та їх характерні прийоми.
30. Роль та місце маніпулювання в системі державного управління та політичних системах (з наведенням конкретних прикладів).
31. Роль та місце маніпулювання у здійсненні міжнародних стосунків (з наведенням конкретних прикладів).
32. Сутність інформаційного насильства. Прояви інформаційного насильства (з наведенням конкретних прикладів).
33. Тотожності та відмінності процесів маніпулювання свідомістю людини та інформаційного насильства. Чинники, які створюють проблемні питання правового запобігання здійснення інформаційного насильства.

34. Сутність поняття «національна безпека». Законодавчі акти в системі забезпечення національної безпеки.
35. Сутність поняття «міжнародна безпека». Міжнародні системи колективної безпеки та їх сутності. Наведіть приклади.
36. Чинники від яких залежить ефективність системи міжнародної безпеки. Спрямованість трансформаційних процесів в системах міжнародної безпеки.
37. Роль та місце інформаційної безпеки у системі національної безпеки.
38. Роль та місце інформаційної безпеки в системах міжнародної безпеки.
39. Сутність понять «загроза» в інформаційної сфері та «інформаційна операція».
40. Сутність поняття «спеціальна інформаційна операція». Наведіть приклади.
41. Сутність поняття «інформаційна експансія». Наведіть приклади.
42. Сутність понять «насильство», «жорстокість», «порнографія».
43. Розуміння поняття «інформаційна інфраструктура».
44. Доктринальні та стратегічні нормативно-правові акти України в сфері забезпечення інформаційної безпеки, які визначають сучасні реальні та потенційні загрози в інформаційної сфері.
45. Основні загрози міжнародній безпеці в сфері інформаційної безпеки.
46. Сутність та визначення понять «інформаційна система», «комунікаційна система» та «інформаційно-комунікаційна система». Наведіть приклади.
47. Сутність та визначення поняття «технологія». Наведіть приклади.
48. Чинники, які вказують на об’єктність та предметність правового регулювання ІКТ.
49. Сутність процесів забезпечення безпеки глобальних інформаційних систем та мереж.
50. Сутність та визначення поняття «соціалізація» та «кіберсоціалізація».
51. Сутність та визначення поняття «цивілізація» та «кіберцивілізація».
52. Витоки загроз для особистості в умовах кіберсоціалізації.
53. Загрози для суспільства, держави соціалізації особистості в умовах кіберцивілізації.
54. Основні положення Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки», які стосуються питань забезпечення інформаційної безпеки.
55. Спрямованість правових основ розвитку інформаційних технологій та забезпечення інформаційної безпеки.
56. Витоки та сутність глобалізації інформаційного простору.
57. Принципи та механізми глобалізації інформаційного простору.
58. Наслідки глобалізації інформаційного простору у наступний час.
59. Сутність, цілі, завдання та можливості соціальних мереж .
60. Наслідки функціонування та розширення соціальних мереж.
61. Чинники які визначають особливості та проблеми реалізації інформаційних правовідносин в мережі Інтернет.
62. Сутність та визначення поняття «кіберзлочин» та «кіберзлочинність».
63. Сутність, мотивація та визначення поняття «кібертероризм».
64. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Україні.
65. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Європейському Союзі.
66. Сутність, прояви та наслідки кібертероризму.
67. Відображення у законодавстві України юридичної відповідальності за спробу здійснення або здійснення кібертероризму.
68. Сутність понять «права людини», «свобода людини», «обов’язок» людини.
69. Законодавче визначені обмеження прав людини та громадянина в інформаційній сфері.

70. Сутність прав суспільства. Права суспільства в інформаційної сфері.
71. Обов’язки держави в інформаційної сфері. Сутність та поняття цензури.
72. Взаємозв’язок між забезпеченням прав і свобод людини, громадянина в інформаційної сфері та забезпечення інформаційної безпеки.
73. Основні положення Стратегії кібербезпеки України.
74. Основні положення Воєнної доктрина України в частині забезпечення інформаційної та кібернетичної безпеки.
75. Основні положення Концепції розвитку сектору безпеки і оборони України в частині забезпечення інформаційної та кібернетичної безпеки.
76. Основні положення Конституції України в частині забезпечення інформаційної безпеки. Концепція розвитку сектору безпеки і оборони України.
77. Основні положення Закону України «Про засади внутрішньої і зовнішньої політики» в частині забезпечення інформаційної та кібернетичної безпеки.
78. Основні положення Закону України «Про інформацію» в частині забезпечення інформаційної безпеки.
79. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» в частині забезпечення інформаційної безпеки.
80. Основні положення Закону України «Про основні засади забезпечення кібербезпеки України» в частині забезпечення кібернетичної безпеки.
81. Основні положення Закону України «Про телекомунікації» в частині забезпечення інформаційної та кібернетичної безпеки.
82. Основні положення Закону України «Про захист персональних даних» в частині забезпечення інформаційної та кібернетичної безпеки.
83. Сутність поняття «правове забезпечення». Складові процесу правового забезпечення та їх зміст. Об`єкти та суб`єкти складових системи правового забезпечення.
84. Відмінності та тотожності понять «правове забезпечення» та «законодаче забезпечення».
85. Поняття «індустріальне суспільство» та його характерні ознаки. Поняття «постіндустріальне суспільство» та його характерні ознаки. Основні ознаки відмінностей індустріального та постіндустріального суспільств.
86. Тенденції розвитку постіндустріального суспільства. Спрямованість трансформаційних процесів правовідносин у постіндустріальному суспільстві.
87. Характер та спрямованість реальних та потенційних загроз в інформаційній сфері у постіндустріальному суспільстві.
88. Сутність та витоки глобалізації. Сутність та витоки глобалізації інформаційного простору.
89. Сутність поняття «суверенітет». Види суверенітету. Сутність (принципи) інформаційного суверенітету. Законодавче визначення поняття «інформаційний суверенітет держави».
90. Складові здійснення інформаційного суверенітету України. Шляхи забезпечення інформаційного суверенітету України. Проблемні питання забезпечення інформаційного суверенітету України.
91. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері.
92. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення.
93. Правові обмеження щодо створення, поширення, збереження, обробки та знищення інформації.

94. Сутність поняття «інформаційний ресурс». Інформаційний ресурс як об`єкт інформаційної небезпеки.
95. Основоположні положення Конституції України щодо поводження з інформацією.
96. Сутність поняття «соціальна відповідальність». Дефініція поняття «юридична відповідальність». Сутність поняття «цивільно-правова відповідальність».
97. Основні напрями дій, які віднесені до правопорушень в інформаційної сфері відповідно до положень Кримінального кодексу України.

Робочу програму навчальної дисципліни (силабус):

Складено доцент, к.т.н, старший науковий співробітник, Фурашев Володимир Миколайович

Ухвалено кафедрою інформаційного права та права інтелектуальної власності (протокол № 12 від 18 червня 2020 року).

Погоджено Методичною радою університету (протокол №6 від 25.02.2021 року)