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

Кафедра інформаційного, господарського та адміністративного права

ІНФОРМАЦІЙНА БЕЗПЕКА

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*Всі галузі знань (крім 081 Право)*
Спеціальність	*Всі спеціальності (крім 081 Право)*
Освітня програма	*Всі ОПП (крім 081 Право)*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (денна), заочна*
Рік підготовки, семестр	*3 курс, осінній або весняний семестр*
Обсяг дисципліни	*60 годин /2 кредити (лекції - 18 годин, семінарські (практичні) заняття - 18 годин, СРС - 24 години (денна форма навчання)* *60 годин/2 кредити (лекції - 6 годин, семінарські (практичні) заняття - 4 години, СРС - 50 годин (заочна форма навчання))*
Семестровий контроль/ контрольні заходи	*Залік/ МКР (ДКР)*
Розклад занять	*http://rozklad.kpi.ua/*
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**:** *старший викладач, Солончук Ірина Вікторівна, e-mail: ivsolonchuk@gmail.com;* *старший викладач, к.ю.н., старший дослідник Радзієвська Оксана Григорівна, e-mail: radeoksa@gmail.com* *Консультації: щопонеділка, 16:00-17:00*
Розміщення курсу	https://kigap.kpi.ua/navchannia/

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 нинішній час в інформаційному просторі, механізму їх впливу на процеси забезпечення інформаційної безпеки людини, суспільства і держави є одним з головних превентивних шляхів запобігання інформаційної небезпеки та її наслідків.

Виходячи з цього, **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 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 основами знань 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, господарського та адміністративного права та, за необхідністю, у взаємно погоджений час.

Метою дисципліни є підсилення у студентів наступних здатностей:

- здатність до абстрактного мислення, аналізу та синтезу.
- здатність вчитися і оволодівати сучасними знаннями.
- 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'язку інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;
- основ державної політики у сфері забезпечення інформаційної безпеки та змісту основних положень нормативно-правових актів у сфері інформаційної безпеки;
- реальних та потенційних загроз у сфері інформаційної безпеки та нормативно-правових шляхів їх запобігання;
- основних методів маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;
- основних положень юридичної відповідальності за правопорушення в інформаційній сфері;
- змісту основних міжнародних договорів з питань інформаційної безпеки;
- основних проблем нормативно-правового забезпечення інформаційної безпеки.

2) **умінь:**

- 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.
- пояснювати природу та зміст основних правових явищ і процесів.
- застосовувати отримані знання та інформаційно-правові положення у практичній діяльності, у тому числі, і під час розробки, впровадження та використання складових компонентів та елементів 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, синтез 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 достатньо опанованих знань за обраною спеціальністю.

3. Зміст навчальної дисципліни

3.1. Денна форма навчання

№ з\п	Змістовні модулі	Кількість годин				
		Всього	Лекції	Практ. занят.	Індив. занят.	Самост. робота
1	**2**	**3**	**4**	**5**	**6**	**7**
	Розділ 1. Природні та суспільні витоки інформаційної небезпеки					
1.1.	Інформаційна безпека як навчальна дисципліна. Інформація як джерело небезпеки. *	4	2	2	-	-
1.2.	Інтернет та інформаційна безпека.□	6	2	2	-	2
1.3.	Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки.*	6	2	2	-	2
1.4.	Інформаційна діяльність як об'єкт небезпеки. *	14	4	4	-	6
1.5.	Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки, кібербезпеки. *	8	2	2	-	4
	Всього за розділом:	**38**	**12**	**12**	-	**14**
	Розділ 2. Нормативно-правове забезпечення інформаційної безпеки					
2.1.	Поняття «нормативно-правове забезпечення» Законодавче забезпечення безпечного обігу інформації. *	8	2	2	-	4
2.2.	Доктринальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.*	6	2	2	-	2
2.3.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки. *	6	2	2	-	2
	МКР				(1)	
	Всього за розділом:	**20**	**6**	**6**	**(1)**	**8**
	Залік:	2	-	-	(2)	2
	Разом:	**60**	**18**	**18**	**(3)**	**24**

* Лекція та семінарське (практичне заняття) заняття проводяться із застосуванням мультимедійних засобів навчання.

3.2. Заочна форма навчання

з\п	Змістовні модулі	Кількість годин				
		Всього	Лекції	Практ. занят.	Індив. занят.	Самост. робота
1	**2**	**3**	**4**	**5**	**6**	**7**
	Розділ 1. Природні та суспільні витоки інформаційної небезпеки					
1.1.	Інформаційна безпека як навчальна дисципліна. Інформація як джерело небезпеки. *	8	2	-	-	6
1.2.	Інтернет та інформаційна безпека. *	4	-	-	-	4
1.3.	Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки. *	4	-	-	-	4
1.4.	Інформаційна діяльність як об'єкт небезпеки. *	14	2	2	-	10
1.5.	Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки, кібербезпеки. *	8	-	-	-	8
	Всього за розділом:	**38**	**4**	**2**	-	**32**
	Розділ 2. Нормативно-правове забезпечення інформаційної безпеки					
2.1.	Поняття «нормативно-правове забезпечення». Законодавче забезпечення безпечного обігу інформації. *	12	2	2	-	8
2.2.	Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.*	4	-	-	-	4
2.3.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки. *	4	-	-	-	4
	МКР				(1)	
	Всього за розділом:	**20**	**2**	**2**	-	**16**
	Залік:	2	-	-	(**2**)	2
	Разом:	**60**	**6**	**4**	**(3)**	**50**

* Лекція та семінарське (практичне заняття) 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 конспекти яких одразу після завершення заняття надсилаються на електронну адресу навчальної групи та старості цієї групи, а також доцільно ознайомитися з тематичними розділами наступних джерел інформації:

Базова література

1. Інформаційна безпека держави: навч. посіб. Для студ. спец. 6.170103 «Управління інформаційною безпекою» / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. – Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
   URL: http://ir.stu.cn.ua/bitstream/handle/123456789/19246/Інформ. безпека держ. New booklet 1.pdf?sequence=1&isAllowed=y
2. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і праваНАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2021. № 6 (червень). 261с - URL: http://ippi.org.ua/sites/default/files/2021-6.pdf
3. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і праваНАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2021. № 5(травень). 304с. URL: http://ippi.org.ua/sites/default/files/2021-5.pdf

4. Основи демократичного цивільного контролю над сектором безпеки і оборони: навчально-методичні матеріали (для тренінгу) / Ященко В.А., Пилипчук В.Г., Довгань О.Д., Лебединська О.В. К.: Видавничий дім «АртЕк». 2019. 106 с. URL: http://www.ippi.org.ua/osnovi-demokratichnogo-tsivilnogo-kontrolyu-nad-sektorom-bezpeki-i-oboroni-navchalno-metodichni-mate
5. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології. /Арістова І.В., Баранов О.А., Дзьобань О.П. та ін.; за заг. ред. проф. К.І. Бєлякова: монографія. Київ: КВІЦ, 2019. 344 с. (Розділ 4. Характеристика галузевих видів юридичної відповідальності за інформаційні делікти.)
URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf

Допоміжна література
(факультативно / ознайомлення)

1. Систематизація і розвиток теоретичних основ трансформації інформаційних відносин на шляху до кіберцивілізації: наук. доп. / Фурашев В.М., Петряєв С.Ю., Поперечнюк В.М. К.: ФСП НТУУ «КПІ», 2016. 55 с. URL: http://ippi.org.ua/sites/default/files/dop._2016.pdf
2. В.П. Горбулін, О.Г. Додонов , Д.В. Ланде. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В.П. Горбулін, О.Г. Додонов, Д.В. Ланде. – К.: Інтертехнологія, 2009. 164 с. URL: http://dwl.kiev.ua/art/gdl/gdl.pdf
3. 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
4. О.Д. Довгань, І.М. Доронін. Ескалація кіберзагроз національним інтересам України та правові аспекти кібербезпеки: монографія / О.Д. Довгань, І.М. Доронін; НАПрН України, НДІІП К.: Видавничий дім «АртЕк». 2017. 107 с. URL: http://ippi.org.ua/sites/default/files/eskalaciya_kiberzagroz.pdf
5. Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони/ збірник документів і матеріалів / Упорядники: Беланюк М.В., Доронін І.М., Лебединська О.В., Радзієвська О.Г., Пилипчук В.Г., Шамара О.В., Фурашев В.М. – К.: Видавничий дім «АртЕк». 2020. 756 с. URL: http://ippi.org.ua/sites/default/files/verstka_zbirnuk_zakoniv.pdf
6. Юридична відповідальність за правопорушення в інформаційній сфері : теорія і практика / Монографія / Кол. авторів; За загальною. ред. проф. К. І. Бєлякова. К.: 2016. 293 с. CD / Монографі_2016.pdf - URL: http://www.ippi.org.ua/yuridichna-vidpovidalnist-za-pravoporushennya-v-informatsiinii-sferi-teoriya-i-praktika

Інформаційні ресурси

Для пошуку іншої необхідної літератури та нормативно-правових актів 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)

Лекційні заняття

№ з/п	Назва теми лекції та перелік основних питань (завдання на СРС)
1	**Тема 1.1. Інформаційна безпека як навчальна дисципліна. 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. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Конституція України; - Про інформацію (*в редакції 2011 року)*; - Про друковані засоби масової інформації (пресу) в Україні; - Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Про Концепцію Національної програми інформатизації.
2	**Тема 1.2. 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. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Про засади внутрішньої і зовнішньої політики; - Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Про національну безпеку України; - Про основи національної безпеки України; - Про телекомунікації.
3	**Тема 1.3. Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки.** Кібернетика як джерело небезпеки. Процеси створення та впровадження інформаційно-комунікаційних технологій (ІКТ) як об'єкт і предмет нормативно-правового регулювання. Безпека глобальних інформаційних систем та мереж. Визначення поняття «кібернетична безпека» (кібербезпека). Сутність поняття «кіберсоціалізація». Соціальні мережі. Мережева мобілізація: питання демократії та безпеки. Наслідки кіберсоціалізації. Сутність поняття «кіберцивілізація». Потенційні загрози кіберцивілізації для людства. Об'єкти інформаційних загроз. Об'єкти кіберзагроз. Сутність зв`язку інформаційної безпеки та кібербезпеки. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Про основні засади забезпечення кібербезпеки України; - Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Про національну безпеку України.
4	**Тема 1.4. Інформаційна діяльність як об'єкт небезпеки.** *Лекція 1.* Сутність, поняття та правове визначення поняття «інформаційна діяльність». Складові інформаційної діяльності. Засоби та їх структура здійснення інформаційної діяльності. Інформаційні ресурси: поняття, основні функції, ієрархічні рівні. Інформаційний ресурс як об'єкт інформаційної небезпеки. Взаємозв'язок інформаційної діяльності та інформаційної безпеки. Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства. Перспективи та напрями розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Про інформацію; - Про друковані засоби масової інформації (пресу) в Україні; - Про електронні документи та електронний документообіг; - Про авторське право і суміжні права.
5	**Тема 1.4. Інформаційна діяльність як об'єкт небезпеки.** *Лекція 2.* Сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя» 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. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Про інформацію (*в редакції 1992 року)*; - Про інформацію (*в редакції 2011 року)*; - Про основні засади забезпечення кібербезпеки України; - Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки.
6	**Тема 1.5. Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки, кібербезпеки.** Зовнішні чинники Внутрішньодержавні чинники *Завдання на СРС:* Розглянути основні тематичні положення: - Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Закону України «Про основні засади забезпечення кібербезпеки України»; - Стратегії інформаційної безпеки України; - Стратегії кібербезпеки України; - Стратегії національної безпеки України; - Стратегія Воєнної безпеки України; - Стратегії зовнішньополітичної діяльності України; - Закону України «Про запобігання корупції»
7	**Тема 2.1. Поняття «нормативно-правове забезпечення» Законодавче забезпечення безпечного обігу інформації.** Загальний огляд нормативно-правового забезпечення в сфері інформаційної безпеки. Складові нормативно-правового забезпечення та їх коротка характеристика. Роль та значення категорійно-понятійного апарату в системі правового забезпечення інформаційної безпеки. Правові гарантії безпечного обігу інформації. Правові обмеження щодо створення, поширення, збереження, обробки та знищення інформації. Інформаційний ресурс як об'єкт інформаційної небезпеки. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Конституція України; - Про інформацію (в редакції 2011 року); - Про друковані засоби масової інформації (пресу) в Україні; - Про захист інформації в інформаційно-телекомунікаційних системах; - Про основні засади забезпечення кібербезпеки України; - Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Про запобігання корупції; - - Про доступ до публічної інформації.
8	**Тема 2.2. Доктринальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.** 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. Трансформація кіберзагроз в сучасних умовах. Характеристика основних тематичних положень - Стратегії національної безпеки України; - Стратегії інформаційної безпеки України - Стратегії кібербезпеки України; - Характеристика основних положень Закону України «Про основні засади забезпечення кібербезпеки України». *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Конституція України;

	- Про інформацію (в редакції 2011 року); - Про друковані засоби масової інформації (пресу) в Україні; - Про основні засади забезпечення кібербезпеки України; - Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Стратегія національної безпеки України.
9	**Тема 2.3. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки.** Поняття кіберзлочинності. Про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. № 994-575. 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. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. - Про ратифікацію Конвенції про кіберзлочинність; - Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи від 28.01.03 р.; - Господарський кодекс України; - Кодекс України про адміністративні правопорушення; - Кримінальний Кодекс України; - Цивільний Кодекс України.

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. Інформаційна безпека як навчальна дисципліна. Інформація як джерело небезпеки.** *Питання для розгляду:* 1. Власне бачення основних світових тенденцій розвитку суспільств. 2. Власне бачення та оцінка трансформаційних процесів сучасності з точки зору безпеки людини. 3. Основні трансформаційні процеси сучасності з точки зору безпеки держави. 4. Природа та сутність інформації. Законодавче визначення поняття «інформація». 5. Сутність поняття «носій інформації» та його значення. 6. Сутність понять «безпека інформації», «безпечність інформації» та «захист інформації». 7. Законодавче визначення поняття «інформаційна безпека». 8. Основні властивості інформації з позиції інформаційної безпеки. 9. Що є основними об'єктами інформаційної безпеки та чому? 10. Основні завдання інформаційної безпеки. 11. Основні критерії визначення об'єктів інформаційної небезпеки та їх обґрунтування. 12. Ієрархія об'єктів інформаційної небезпеки. *Завдання на СРС:* 1. Що таке війна? Чим війна відрізняється від збройного конфлікту? 2. Основні види війн. 3. Основні цілі та завдання сучасних війн. 4. У зв'язку з чим відбуваються трансформаційні процеси організації та проведення локальних і регіональних конфліктів та війн. 5. Основна спрямованість трансформаційних процесів організації та проведення локальних та регіональних конфліктів і війн. 6. Характерні ознаки гібридних війн.
2	**Тема 1.2. Інтернет та інформаційна безпека.** *Питання для розгляду:* - Розкриття поняття «Інтернет». - Юридичні особливості мережі Інтернет.

	- Розкриття понять «інформаційні правовідносини» та «інформаційно-інфраструктурні відносини». - Особливості встановлення та проблеми реалізації інформаційних правовідносин в мережі Інтернет. - Розкриття взаємозв'язку глобалізації мережі Інтернет з поширенням та поглибленням трансформаційних процесів забезпечення національної та міжнародної безпеки. *Завдання на СРС:* 1. Розкриття поняття «трансформаційний процес». 2. Розкриття поняття «правове реагування» та його складові. 3. Що розуміється під поняттям «інформаційні правовідносини». 4. Розкриття поняття «міжнародна інформаційна безпека».
3	**Тема 1.3. Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки**. *Питання для розгляду:* - Кібернетика як джерело небезпеки. - Визначення поняття «кібернетична безпека» (кібербезпека). - Сутність поняття «кіберсоціалізація». - Сутність поняття «кіберцивілізація». Витоки загроз для особистості в умовах кіберцивілізації. - Об'єкти інформаційних загроз. Об'єкти кіберзагроз. Сутність зв'язку інформаційної безпеки та кібербезпеки. - Сутність та визначення поняття «інформаційно-комунікаційна система». - Сутність та визначення поняття «інформаційна технологія». Наведіть приклади. - Чинники, які вказують на об'єктність та предметність правового регулювання ІКТ. - Сутність процесів забезпечення безпеки глобальних інформаційних систем та мереж. - У чому полягають основні тотожності та відмінності процесів забезпечення інформаційної безпеки та кібербезпеки. <u>*Завдання на СРС:*</u> 1. Розкриття дефініцій «система», «інформаційна система», «технологія», «комунікація», «комунікаційна система». 2. Розкриття дефініцій «загроза», «загроза в інформаційної сфері», «інформаційний вплив», «інформаційна війна», «інформаційна зброя». 3. Сутність та визначення поняття «кіберпростір». 4. Чинники, які вказують на особливості сучасних інформаційних відносин.
4	**Тема 1.4. Інформаційна діяльність як об'єкт небезпеки**. <u>*Перше семінарське заняття*</u> *Питання для розгляду:* - Розкриття сутності інформаційної діяльності. Законодавче визначення поняття «інформаційна діяльність». - Основні види та напрями інформаційної діяльності. - Складові інформаційної діяльності. Суб'єкти та засоби здійснення інформаційної діяльності. - Розуміння поняття «інформаційна інфраструктура». - Чинники, які визначають ступінь ефективності здійснення інформаційної діяльності. - Сутність інформаційного виробництва. Поняття інформаційного продукту. - Основні елементи інформаційного виробництва. - Поняття інформаційного забруднення. - Сутність та визначення поняття «інформаційний ресурс». - Властивості та основні функції інформресурсів. - Взаємозв'язок інформаційної діяльності та інформаційної безпеки. - Власне бачення перспектив та напрямів розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки. *Завдання на СРС:* 1. Характерні риси постіндустріального суспільства з точки зору здійснення інформаційної діяльності. 2. Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства. 3. Сутність понять «насильство», «жорстокість», «порнографія». 4. Перспективи та напрями розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки. 5. Сутність та поняття «цензура».
5	**Тема 1.4. Інформаційна діяльність як об'єкт небезпеки.** <u>*Друге семінарське заняття*</u> *Питання для розгляду:*

	- Сутність поняття «маніпуляція». - Види маніпуляції та розкриття їх сутність. - Роль та місце маніпулювання в системі державного управління (з наведенням конкретних прикладів). - Роль та місце маніпулювання в політичних системах (з наведенням конкретних прикладів). - Роль та місце маніпулювання у здійсненні міжнародних стосунків (з наведенням конкретних прикладів). - Сутність інформаційного насильства. - Прояви інформаційного насильства (з наведенням конкретних прикладів). - Тотожності та відмінності процесів маніпулювання свідомістю людини та інформаційного насильства. - Чинники, які створюють проблемні питання правового запобігання здійсненню інформаційного насильства. - Сутність поняття «інформаційна війна» та «інформаційна операція» *Завдання на СРС:* 1. Розкриття сутності поняття «інформаційна операція» з наведенням конкретних прикладів. 2. Розкриття сутності поняття «спеціальна інформаційна операція» з наведенням конкретних прикладів. 3. Сутність понять «експансія» та «інформаційна експансія» з наведенням конкретних прикладів.
6	**Тема 1.5. Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки.** *Питання до розгляду:* Зовнішні чинники Внутрішньодержавні чинники *Завдання на СРС:* Розглянути основні тематичні положення: - Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки; - Закону України «Про основні засади забезпечення кібербезпеки України»; - Стратегії інформаційної безпеки України; - Стратегії кібербезпеки України; - Стратегії національної безпеки України; - Стратегія Воєнної безпеки України; - Стратегії зовнішньополітичної діяльності України; - Закону України «Про запобігання корупції»
7	**Тема 2.1. Поняття «нормативно-правове забезпечення». Законодавче забезпечення безпечного обігу інформації**. *Питання до розгляду:* - Сутність поняття «нормативно-правове забезпечення» та його складові. - Розкриття сутності понять «безпечний оборот інформації» та «правові гарантії обігу інформації». - Що розуміємо під поняттям «життєвий цикл інформації»? - Характерна риса сучасності, яка суттєво ускладнює забезпечення безпечного обігу інформації як на національному рівні, так і міжнародному. - У зв'язку з чим існують правові обмеження збору, зберігання та поширення певної інформації? Інформація якої спрямованості обмежується у поширенні, збиранні та зберігання на законодавчому рівні? - Об'єкти захисту в інформаційно-телекомунікаційних системах. *Завдання на СРС:* Розглянути основні тематичні положення законів України: - Конституція України; - Про інформацію; - Про захист інформації в інформаційно-телекомунікаційних системах; - Про доступ до публічної інформації.
8	**Тема 2.2. Доктринальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.** *Питання до розгляду:* - Сутність понять «національна безпека» та «міжнародна безпека». - Міжнародні системи колективної безпеки та механізми здійснення. - Дефініція поняття «доктрина». Актуальні воєнні загрози для України з використанням властивостей інформації, які можуть перерости в загрозу застосування воєнної сили проти України та які знайшли своє відображення у Воєнної доктрині України. - Дефініція поняття «стратегія». Механізми реалізації Стратегії. Основна функція Стратегії, відповідно до

	Закону України «Про національну безпеку». - Основні цілі Стратегії національної безпеки України. - Які основні загрози у сфері забезпечення інформаційної безпеки та кібербезпеки, визначає Стратегія національної безпеки? - Які пріоритети визначені у Стратегії національної безпеки України у сфері забезпечення кібербезпеки і безпеки інформаційних ресурсів? - Що має на меті Стратегія кібербезпеки України. На дію яких чинників, що актуалізують загрози кібербезпеці, вказує дана Стратегія? - Особливості сучасних обставин, які впливають на стратегічні рішення забезпечення інформаційної безпеки. - Що розуміється під поняттям «Життєво важливі інтереси людини та суспільства в інформаційної сфері». - Значення корупції у вирішенні питань правового забезпечення інформаційної безпеки, кібербезпеки. - Сутність поняття «суверенітет». Види суверенітету. - Сутність (принципи) інформаційного суверенітету. - Проблемні питання забезпечення інформаційного суверенітету України *Завдання на СРС:* 1. Основні показники національної безпеки. 2. Складові сфери національної безпеки. 3. Чинники, від яких залежить ефективність тієї чи іншої системи міжнародної безпеки. 5. Основні загрози національної та міжнародної безпеці в інформаційній сфері. 6. Спрямованість трансформаційних процесів в системах міжнародної безпеки. 7. Роль та місце інформаційної безпеки у системі національної безпеки. 8. Сутність понять «експансія» та «інформаційна експансія». Наведіть приклади. 9. В чому полягають проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення.
9	**Тема 2.3. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки.** *Питання до розгляду:* 1. Випадки коли особа, яка здійснила правопорушення в інформаційної сфері, не підлягає юридичній відповідальності. 2. Класифікація комп'ютерної злочинності, прийнята у Європейському Союзі. 3. Основні спрямованості/види правопорушень у сфері забезпечення інформаційної безпеки та кібербезпеки відповідно до положень Господарського кодексу України. 4. Види адміністративних стягнень. 5. Основні спрямованості/види правопорушень у сфері забезпечення інформаційної безпеки та кібербезпеки відповідно до положень Цивільного кодексу України. 6. Основні спрямованості/види правопорушень у сфері забезпечення інформаційної безпеки та кібербезпеки відповідно до положень Кодексу України про адміністративні правопорушення. 7. Основні спрямованості/види правопорушень у сфері забезпечення інформаційної безпеки та кібербезпеки відповідно до положень Кримінального кодексу України. 8. Власна оцінка ступеня повноти охоплення кола правопорушень в сфері забезпечення інформаційної безпеки та кібербезпеки. 9. Власна оцінка адекватності юридичної відповідальності за правопорушення в сфері забезпечення інформаційної безпеки та кібербезпеки наслідкам від здійснення цих правопорушень. *Завдання на СРС:* 1. Сутність та визначення поняття «злочин». 2. Сутність та визначення поняття «злочинність». 3. Основні ознаки злочинності. 4. Сутність та визначення поняття «кіберзлочин». 5. Сутність та визначення поняття «кіберзлочинність». 6. Сутність та визначення поняття «комп'ютерна злочинність». 7. Тотожності та відмінності понять «кіберзлочинність» та «комп'ютерна злочинність». Дефініція поняття «тероризм». 8. Природа тероризму. 9. Дефініція поняття «терористичний акт». 10. Чим приваблює кіберпростір терористів? 11. Відображення кібертероризму в законодавстві України

6. Самостійна робота студента

Самостійна робота студента (СРС) передбачає самостійне, на основі зазначених питань віднесених до розгляду на практичному (семінарському) 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)

Система вимог, які викладач ставить перед студентом:

- *правила відвідування занять:* відповідно до Наказу 1-273 від 14.09.2020 р. заборонено оцінювати присутність або відсутність здобувача на аудиторному занятті, в тому числі нараховувати заохочувальні або штрафні бали за це. Відповідно до РСО даної дисципліни бали нараховують за відповідні види навчальної активності на семінарських (практичних) заняттях.

На момент проведення кожного заняття, як лекційного, так і практичного, у студента на пристрої, з якого він працює, має бути встановлено додаток Zoom (у випадку дистанційного навчання). Силабус; лекційний матеріал; практикум; завдання до кожного практичного заняття; варіанти модульної контрольної роботи; тести, які потрібно виконати за лекціями; методичні рекомендації до виконання розрахункової роботи; перелік питань до залікової контрольної роботи розміщено на платформі «Сікорський» та у системі «Електронний Кампус КПІ».

Відвідування семінарських (практичних) занять, незалежно від форми їх проведення, є обов'язковим. Бали за присутність на лекціях не додаються. За відвідування семінарських (практичних) занять студенти також не отримують бали, але головна частина рейтингу студента формується через активну участь у семінарських заняттях й підготовленість до них;

- *правила поведінки на заняттях:* студент має можливість отримувати бали за відповідні види навчальної активності на семінарських (практичних) заняттях, передбачені РСО дисципліни. Використання засобів зв'язку для пошуку інформації в Інтернеті, в дистанційному курсі на платформі Сікорський здійснюється за умови вказівки викладача;

- *правила призначення заохочувальних та штрафних балів*. Заохочувальні бали нараховують за участь у наукових конференціях, студентських конкурсах та олімпіадах, за написання статті та її публікацію. За участь у Всеукраїнській олімпіаді (конкурсі наукових робіт) студенту нараховується 5 (І тур) або 10 (ІІ тур) балів. За написання статті та її публікацію студенту нараховується 10 балів (видання, що входить до Scopus або Web of Science) або 8 балів (фахове видання України). За публікацію тез доповіді на науковій конференції – 5 балів. За проходження тематичних курсів на онлайн-платформах – 10 балів. *При цьому, відповідно до Положення про систему оцінювання результатів навчання сума всіх заохочувальних балів не може перевищувати 10% рейтингової шкали оцінювання.* Штрафних балів з дисципліни не передбачається;

- *політика дедлайнів та перескладань*: кожен студент зобов'язаний дотримуватися термінів виконання завдань у межах розкладу проведення аудиторних занять з дисципліни. Обов'язковим контрольним заходом оцінювання для допуску до заліку є написання МКР. Студент, що з поважної

причини (лікарняний, академічна мобільність тощо) не написав МКР, має право зробити це під час регулярних консультацій викладача згідно розкладу. Порядок перескладання семестрового контролю визначається загальними правилами університету .

• *політика щодо академічної доброчесності*: Кодекс честі Національного технічного університету України «Київський політехнічний інститут» https://kpi.ua/files/honorcode.pdf встановлює загальні моральні принципи, правила етичної поведінки осіб та передбачає політику академічної доброчесності для осіб, що працюють і навчаються в університеті, якими вони мають керуватись у своїй діяльності, у тому числі при вивченні та складанні контрольних заходів з дисципліни «Інформаційна безпека». Викладачі та студенти, що вивчають дану дисципліну, зобов'язані дотримуватися положень прийнятого в університеті Кодексу честі ;

• при використанні цифрових засобів зв'язку з викладачем (мобільний зв'язок, електронна пошта, переписка на форумах та у соц. мережах тощо) необхідно дотримуватись загальноприйнятих етичних норм, зокрема бути ввічливим та обмежувати спілкування робочим часом викладача.

Інклюзивне навчання. Засвоєння знань та умінь в ході вивчення дисципліни може бути доступним для більшості осіб з особливими освітніми потребами, окрім здобувачів з серйозними вадами зору, які не дозволяють виконувати завдання за допомогою персональних комп'ютерів, ноутбуків та/або інших технічних засобів.

Навчання іноземною мовою. У ході викладання навчального матеріалу може бути застосовані англомовна термінологія.

Пропущені контрольні заходи оцінювання

Пропущені заходи оцінювання знань студентом(ами) по темі навчальної дисципліни вирішується шляхом усунення заборгованості не пізніше перших 2-ох днів календарного контролю за взаємною домовленістю з викладачем щодо дати та часу відпрацювання.

Календарний контроль

Метою проведення календарного контролю є підвищення якості навчання студентів та моніторинг виконання графіка освітнього процесу. Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Критерій	Перший календарний контроль	Другий календарний контроль
Термін календарного контролю	8-ий тиждень	14-ий тиждень
Умови позитивного отримання	≥ 20 балів	≥ 40 бал

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: 1) оцінювання якості та глибини розкриття поставленого питання під час проведення кожного семінарського (практичного) заняття; 2) модульна контрольна робота (МКР).

Оцінювання якості та глибини розкриття поставленого питання під час проведення кожного семінарського (практичного) заняття 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 обґрунтуванням, у поєднанні зі слушними доповненнями відповідей інших студентів у процесі дискусії	*8 балів*

активна участь у проведенні заняття; надання правильних відповідей або правильне вирішення задач з незначними неточностями	*7 балів*
суттєве доповнення відповідей студентів	*6 балів*
надання відповідей з чисельними значними похибками	5 *балів*
Всього за 9 занять	*72 бали*

Написання *модульної контрольної роботи (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 МКР передбачає письмове викладення у довільної формі одного з питань за тематикою розділу навчальної дисципліни визначеного викладачем. Тематика 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 даною навчальною дисципліною.

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, під час проведення МКР, 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	*28 балів*
письмове тестування ступеня засвоєння навчального матеріалу з наданням відповіді на поставлене питання з незначними неточностями або порушеннями логіки	25 *балів*
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання	23 *бали*
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання з незначними похибками	20 *балів*
письмове тестування ступеня засвоєння навчального матеріалу з наданням не повної відповіді на поставлене питання з чисельними значними похибками	*17 балів*

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.

Система оцінювання

№ з/п	Контрольний захід оцінювання	%	Ваговий бал	Кіл-ть	Всього
1.	Оцінювання знань студентів під час проведення семінарського заняття	72	8	9	72
2.	Оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу під час проведення МКР	28	28	1	28
	Всього				100

Теоретичне питання *(під час проведення заліку)*

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.
6-8	Студент розкрив тему на задовільному рівні. Здобувач вказав основні поняття та нормативно-правові акти. У відповіді висновки обґрунтовано неповністю.

Вирішення ситуаційного завдання *(під час проведення заліку)*

Ваговий бал	Критерій оцінювання
15	Студент 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 та робити самостійні, обґрунтовані висновки. Студент 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, висновки у відповідях обґрунтовано неповністю. Студент 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)

Орієнтовний перелік питань 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. Основні базові положення Доктрини інформаційної безпеки України, які відображають трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн.
5. Предмет та основні завдання інформаційної безпеки.
6. Природа та сутність інформації. Визначення поняття «інформація» з точки зору інформаційної безпеки. Законодавче визначення поняття «інформація».
7. Основні властивості інформації з позиції інформаційної безпеки. Сутність та визначення понять «безпека інформації», «безпечність інформації» та «захист інформації».
8. Сутність та визначення поняття «інформаційна безпека». Об'єкти інформаційної небезпеки та їх ієрархія.
9. Спрямованість законодавче визначених обмежень прав людини та громадянина в інформаційної сфері.
10. Сутність прав людини та прав суспільства в інформаційної сфері.

11. Сутність та поняття цензури.
12. Взаємозв'язок між забезпеченням прав і свобод людини, громадянина в інформаційної сфері та забезпеченням інформаційної безпеки.
13. Відображення терміну «інформаційна безпека» у законодавстві України. Законодавче визначення поняття «інформаційна безпека».
14. Зв'язок сутності понять «кібернетика» та «небезпеки».
15. Сутність та визначення поняття «кібербезпека».
16. Взаємозв'язок інформаційної безпеки та кібербезпеки. Ознаки коректності застосування термінів «інформаційна безпека» та «кібербезпека».
17. Сутність та законодавче визначення поняття «інформаційна діяльність». Основні види та напрями інформаційної діяльності.
18. Чинники які визначають ступінь ефективності проведення інформаційної діяльності.
19. Складові інформаційної діяльності. Сутність інформаційного виробництва. Основні елементи інформаційного виробництва.
20. Взаємозв'язок інформаційної діяльності та інформаційної безпеки.
21. Характерні риси постіндустріального суспільства з точки зору здійснення інформаційної діяльності.
22. Перспективи та напрями розвитку інформаційної діяльності в умовах науково-технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки.
23. Сутність поняття «маніпуляція». Види маніпуляції та їх характерні прийоми.
24. Роль та місце маніпулювання в системі державного управління та політичних системах (з наведенням конкретних прикладів).
25. Роль та місце маніпулювання у здійсненні міжнародних стосунків (з наведенням конкретних прикладів).
26. Сутність інформаційного насильства. Прояви інформаційного насильства (з наведенням конкретних прикладів).
27. Тотожності та відмінності процесів маніпулювання свідомістю людини та інформаційного насильства. Чинники, які створюють проблемні питання правового запобігання здійснення інформаційного насильства.
28. Сутність поняття «національна безпека». Законодавчі акти в системі забезпечення національної безпеки.
29. Сутність поняття «міжнародна безпека». Міжнародні системи колективної безпеки та їх сутності. Наведіть приклади.
30. Спрямованість трансформаційних процесів в системах міжнародної безпеки.
31. Роль та місце інформаційної безпеки у системі національної безпеки.
32. Роль та місце інформаційної безпеки в системах міжнародної безпеки.
33. Сутність понять «загроза» в інформаційної сфері та «інформаційна операція».
34. Сутність поняття «спеціальна інформаційна операція». Наведіть приклади.
35. Сутність поняття «інформаційна експансія». Наведіть приклади.
36. Сутність понять «насильство», «жорстокість», «порнографія».
37. Розуміння поняття «інформаційна інфраструктура».
38. Доктринальні та стратегічні нормативно-правові акти України в сфері забезпечення інформаційної безпеки, які визначають сучасні реальні та потенційні загрози в інформаційної сфері.
39. Основні загрози міжнародній безпеці в сфері інформаційної безпеки.
40. Сутність та визначення понять «інформаційна система», «комунікаційна система» та «інформаційно-комунікаційна система». Наведіть приклади.
41. Сутність та визначення поняття «технологія». Наведіть приклади.
42. Сутність процесів забезпечення безпеки глобальних інформаційних систем та мереж.
43. Сутність та визначення поняття «соціалізація» та «кіберсоціалізація».
44. Витоки загроз для особистості в умовах кіберсоціалізації.
45. Основні положення Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки», які стосуються питань забезпечення інформаційної безпеки.
46. Принципи та механізми глобалізації інформаційного простору.
47. Наслідки глобалізації інформаційного простору.
48. Сутність, цілі, завдання та можливості соціальних мереж .
49. Наслідки функціонування та розширення соціальних мереж.

50. Чинники які визначають особливості та проблеми реалізації інформаційних правовідносин в мережі Інтернет.
51. Сутність та визначення поняття «кіберзлочин» та «кіберзлочинність».
52. Сутність, мотивація та визначення поняття «кібертероризм».
53. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Україні.
54. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Європейському Союзі.
55. Сутність, прояви та наслідки кібертероризму.
56. Відображення у законодавстві України юридичної відповідальності за спробу здійснення або здійснення кібертероризму.
57. Законодавче визначені обмеження прав людини та громадянина в інформаційній сфері.
58. Сутність та поняття цензури.
59. Взаємозв'язок між забезпеченням прав і свобод людини, громадянина в інформаційної сфері та забезпечення інформаційної безпеки.
60. Основні положення Стратегії кібербезпеки України.
61. Основні положення Воєнної доктрина України в частині забезпечення інформаційної та кібернетичної безпеки.
62. Основні положення Концепції розвитку сектору безпеки і оборони України в частині забезпечення інформаційної та кібернетичної безпеки.
63. Основні положення Конституції України в частині забезпечення інформаційної безпеки. Концепція розвитку сектору безпеки і оборони України.
64. Основні положення Закону України «Про інформацію» в частині забезпечення інформаційної безпеки.
65. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» в частині забезпечення інформаційної безпеки.
66. Основні положення Закону України «Про основні засади забезпечення кібербезпеки України» в частині забезпечення кібернетичної безпеки.
67. Сутність поняття «правове забезпечення». Складові процесу правового забезпечення та їх зміст. Об'єкти та суб'єкти складових системи правового забезпечення.
68. Відмінності та тотожності понять «правове забезпечення» та «законодавче забезпечення».
69. Тенденції розвитку постіндустріального суспільства. Спрямованість трансформаційних процесів правовідносин у постіндустріальному суспільстві.
70. Характер та спрямованість реальних та потенційних загроз в інформаційній сфері у постіндустріальному суспільстві.
71. Сутність та витоки глобалізації інформаційного простору.
72. Сутність поняття «суверенітет». Види суверенітету. Сутність (принципи) інформаційного суверенітету. Законодавче визначення поняття «інформаційний суверенітет держави».
73. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері.
74. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення.
75. Правові обмеження щодо створення, поширення, збереження, обробки та знищення інформації.
76. Сутність поняття «інформаційний ресурс». Інформаційний ресурс як об'єкт інформаційної небезпеки.
77. Основоположні положення Конституції України щодо поводження з інформацією.
78. 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, господарського і адміністративного права (протокол № 7 від 14.01.2022)

Погоджено Методичною радою університету (протокол № 3 від 27.01.2022).