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

Кафедра інформаційного, господарського та адміністративного права

ПРАВОВІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*08 Право*
Спеціальність	*081 Право*
Освітня програма	*Право*
Статус дисципліни	*Вибіркова*
Форма навчання	*Очна (денна), заочна*
Рік підготовки, семестр	*4 курс, осінній семестр*
Обсяг дисципліни	*4 кредити ЄКТС / 120 годин* *Денна форма навчання: лекції – 18 год., практичні – 36 год., самостійна робота – 66 год.* *Заочна форма навчання: лекції – 12 год., практичні – 8 год., самостійна робота – 100 год.*
Семестровий контроль/ контрольні заходи	*Очна (денна) форма навчання - залік, МКР* *Заочна форма навчання – залік, ДКР*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	**Лектор**: *старший викладач* *Солончук Ірина Вікторівна* *e-mail: ivsolonchuk@gmail.com*
Розміщення курсу	*Платформа дистанційного навчання «Сікорський»*

Програма навчальної дисципліни

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

Освітній компонент “Правові основи інформаційної безпеки” є вибірковою дисципліною для здобувачів першого (бакалаврського) рівня вищої освіти, за освітньою програмою 081 “Право” та є складовою сертифікатної програми “Право в інформаційній сфері”.

Розвиток сучасних інформаційно-комунікаційних технологій загострює проблеми, 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 наразі відбуваються 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.

Тому **метою** вивчення навчальної дисципліни «Правові основи інформаційної безпеки» є:

- надання основоположних знань щодо сутності, проявів, наслідків та механізмів інформаційної безпеки та щодо особливостей виникнення інформаційних правовідносин в сфері забезпечення інформаційної безпеки;
- формування у здобувачів вищої освіти (далі – здобувачів) розуміння механізмів правового забезпечення запобігання та усунення загроз в інформаційній сфері, спрямованих 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 щодо класифікації та правової оцінки дій суб'єктів суспільних відносин в сфері забезпечення інформаційної безпеки.

Предметом навчальної дисципліни є природа інформації та її властивості; розуміння прийомів та методів маніпулювання свідомістю людини; сутність інформаційного насильства та його запобігання; місце інформації та інформаційної безпеки у забезпеченні національної та міжнародної безпеки.

Результатом вивчення дисципліни є досягнення здобувачами:
- здатності до абстрактного мислення, аналізу та синтезу;
- здатності вчитися і оволодівати сучасними знаннями;
- здатності бути критичним і самокритичним;
- здатності 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;
- поваги до честі і гідності людини як найвищої соціальної цінності, розуміння їх правової природи;
- розуміння сутності основних понять, їх тотожностей та відмінностей у сфері інформаційної безпеки;
- розуміння взаємозв'язку інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;
- знання основ державної політики у сфері забезпечення інформаційної безпеки та змісту основних положень нормативно-правових актів у сфері інформаційної безпеки;
- розуміння реальних та потенційних загроз у сфері інформаційної безпеки та нормативно-правових шляхів їх запобігання;
- розуміння основних методів маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;
- знання основних положень юридичної відповідальності за правопорушення в інформаційній сфері;
- знання змісту основних міжнародних договорів з питань інформаційної безпеки;
- уявлення про основні проблеми нормативно-правового забезпечення інформаційної безпеки.

Для досягнення даних результатів необхідним є формування таких програмних компетентностей та програмних результатів навчання:

загальні компетентності (ЗК):

- (ЗК6) Здатність використовувати інформаційні та комунікаційні технології;

фахові компетентності (ФК):

- (ФК14) Здатність до консультування з правових питань, зокрема, можливих способів захисту прав та інтересів клієнтів, відповідно до вимог професійної етики, належного дотримання норм щодо нерозголошення персональних даних та конфіденційної інформації;
- (ФК18) Здатність застосовувати теоретичні знання в сфері права, бізнесу, інформаційних технологій, інтелектуальної власності та інновацій у практичній діяльності правника;
- (ФК19) Знання і розуміння ролі права в розбудові цифрових економіки, суспільства та держави;
- (ФК22) Здатність до інноваційного мислення та оперування знаннями про суспільство, інформаційні технології та правничу професію.

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

Пререквізити: Критичне мислення (ЗО 03), Теорія держави і права (ПО 04), Інформація та інформаційно-комунікаційні технології у правничій діяльності, цивільне право (ПО 06), Права людини: міжнародні стандарти та захист (ПО 07), Адміністративне право: Загальна частина (ПО 17), Філософія, Соціологія. Ці дисципліни створюють основу для розуміння Правових основ інформаційної безпеки.

Постреквізити: Кримінальне право: Особлива частина» (ПО 16), Адміністративне право: Особлива частина (ПО 18), Інформаційне право (ПО 21), «Практика в судах, системі прокуратури та адвокатури» (ПО 41).

3. Зміст навчальної дисципліни

Розділ 1. Природні та суспільні витоки інформаційної небезпеки

Тема 1.1. Правові основи інформаційної безпеки 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.

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.

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.

Тема 1.4. Інформаційна діяльність як об'єкт небезпеки.

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.

Тема 1.5. Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки, кібербезпеки.

Зовнішні чинники. Внутрішньодержавні чинники.

Розділ 2. Нормативно-правове забезпечення інформаційної безпеки

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.

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, Закону України «Про основні засади забезпечення кібербезпеки України».

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.

4. Навчальні матеріали та ресурси

Для успішного вивчення дисципліни достатньо опрацьовувати навчальний матеріал, який викладається на лекціях та конспекти лекцій, які 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
(підручники, навчальні посібники)

1. Фурашев В., Радзієвська О. «Правове забезпечення інформаційної безпеки : курс лекцій». ДНУ «Ін-т інформ., безпеки і права Нац. акад. прав. наук України». Київ; Одеса : Фенікс, 2022. -158 с.
2. Вишня Б.В. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с. URL: //er.dduvs.in.ua/bitstream/123456789/4206/1/Основи%20інформаційної%20безпеки%20навчальний%20посібник%2006.2019%20%283%29.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. – № 6 (червень). – 261с - URL: http://ippi.org.ua/sites/default/files/2021-6.pdf
4. 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/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC.%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B4%D0%B5%D1%80%D0%B6.%20New%20booklet%201.pdf?sequence=1&isAllowed=y
5. 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

Допоміжна література
(факультативно / ознайомлення)

1. 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
2. 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

3. 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. (Розділ4. Характеристика галузевих видів юридичної відповідальності за інформаційні делікти.) - URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf

4. 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

5. 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

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 / Монографія_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/
- https://ippi.org.ua/golovne-menyu/vidannya

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Опанування дисципліни здійснюється на засадах проблемного методу навчання, тобто шляхом виявлення проблемних питань і вирішення їх на основі інтерактивної дискусії. Для підвищення рівня з'ясування змісту дисципліни, інформація надається також через зоровий канал сприйняття за допомогою презентацій.

Під час опанування дисципліни застосовуються різноманітні форми оцінювання результатів навчання, зокрема: виступи з усними доповідями, виступи з презентаціями, виступи з доповідями, написання ессе, презентація порівняльно-правового дослідження, дискусія, моделювання проблемних та практичних ситуацій і пошук вірних рішень, аналіз юридичних документів, усне опитування, тестування, модульна контрольна робота.

Всі ці форми потребують від здобувачів розвитку умінь щодо дослідницької діяльності, яка притаманна будь-якій юридичній професії. Тому в процесі викладання приділяється увага подальшому розвитку когнітивних навичок в частині пошуку інформації, зокрема нормативно-правової, її аналізу, виявлення правових проблем, визначення можливих шляхів їх вирішення.

Пошук та вирішення правових проблем в процесі колективної роботи здійснюється на основі особистісно-орієнтованих (розвиваючих) технологій, які засновані на активних формах і методах навчання («мозковий штурм», «аналіз ситуацій» дискусія кейс-технологія і ін.).

Здобувачам буде забезпечуватись допомога в опануванні відповідних інформаційно-комунікаційних технологій для забезпечення проблемно-дослідницького характеру процесу навчання та активізації самостійної роботи студентів (електронні презентації власних есе та доповідей тощо).

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.

Денна форма навчання

№ з\п	Теми	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.	Правові основи інформаційної безпеки як навчальна дисципліна. Інформація як джерело небезпеки. □	8	2	4	-	2
1.2.	Інтернет та інформаційна безпека.□	12	2	4	-	6
1.3.	Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки. □	12	2	4	-	6
1.4.	Інформаційна діяльність як об'єкт небезпеки. □	28	2	6	-	20
1.5.	Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки, кібербезпеки. □	16	2	6	-	8
Всього за розділом:		**76**	**10**	**24**	-	**42**
Розділ 2. Нормативно-правове забезпечення інформаційної безпеки						
2.1.	Поняття «нормативно-правове забезпечення» Законодавче забезпечення безпечного обігу інформації. □	16	2	4	-	10
2.2.	Доктринальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.□	14	4	4	-	6
2.3.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки. □	12	2	4	-	6
МКР					(1)	
Всього за розділом:		**42**	**8**	**12**	**(1)**	**22**
Залік:		2	-	-	(2)	2
Разом:		**120**	**18**	**36**	**(3)**	**66**

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

Заочна форма навчання

п\п	Теми	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.	Правові основи інформаційної безпеки як навчальна дисципліна. Інформація як джерело небезпеки.	14	2	2	-	10
1.2.	Інтернет та інформаційна безпека.	14	2	-	-	12
1.3.	Кібернетична безпека. Зв'язок інформаційної безпеки та кібербезпеки.	14	-	-	-	14
1.4.	Інформаційна діяльність як об'єкт небезпеки.	18	2	2	-	14
1.5.	Основні чинники, які впливають на рівень забезпеченості інформаційної безпеки, кібербезпеки.	14	-	-	-	14
	Всього за розділом:	**74**	**6**	**4**	-	**64**
	Розділ 2. Нормативно-правове забезпечення інформаційної безпеки					
2.1.	Поняття «нормативно-правове забезпечення». Законодавче забезпечення безпечного обігу інформації.	14	2	2	-	10
2.2.	Доктринальні, концептуальні та стратегічні підходи правового вирішення питань забезпечення інформаційної безпеки, кібербезпеки.	16	2	-	-	14
2.3.	Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки.	14	2	2	-	10
ДКР					(1)	
Всього за розділом:		**44**	**6**	**4**	**-**	**34**
Залік:		2	-	-	(**2**)	2
Разом:		**120**	**12**	**8**	**(3)**	**100**

 Лекція та семінарське заняття проводяться із застосуванням мультимедійних засобів навчання.

6. Самостійна робота здобувача

Основним видом самостійної роботи здобувача в рамках навчальної дисципліни є опанування лекційного матеріалу, дослідження положень нормативних актів та підготовка до практичних занять.

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.

Проходження дистанційних курсів/тренінгів: у разі самостійного проходження дистанційних курсів/тренінгів можливе зарахування результатів навчання до поточного рейтингу, за умови надання викладачу курсу підтверджуючих документів.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила відвідування занять

Відповідно до РСО навчальної дисципліни бали нараховують за відповідні види навчальної активності на лекційних та практичних заняттях.

На момент проведення кожного заняття, як лекційного, так і практичного, у здобувача на пристрої, з якого він працює, має бути встановлено додаток Zoom (у випадку дистанційного навчання), а також відкрито курс «Інформаційна безпека» на платформі «Сікорський» (код доступу до курсу надається на першому занятті згідно з розкладом).

Всі навчальні матеріали з дисципліни (силабус; лекційний матеріал; завдання до кожного практичного заняття; варіанти модульної контрольної роботи; тести, які потрібно виконати за лекціями; перелік питань до залікової контрольної роботи) розміщено на платформі дистанційного навчання «Сікорський» та у системі «Електронний Кампус КПІ».

Відвідування семінарських занять, незалежно від форми їх проведення, є обов'язковим. 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.

Форми роботи

Семінарське заняття складається з двох частин — відповіді на теоретичні питання і захисти практичних завдань. Орієнтовний обсяг доповіді здобувача на одне теоретичне питання — до 3 хв. Орієнтовний обсяг доповіді під час захисту практичних завдань — від 5 до 7 хв. Під час захисту практичних завдань застосовуються такі форми: виступи з усними

доповідями, виступи з презентаціями, усна доповідь за результатом аналізу чи узагальнення аналітичних матеріалів, написання есе, презентація порівняльно-правового дослідження, дискусія, моделювання проблемних та практичних ситуацій і пошук вірних рішень, аналіз юридичних документів, усне опитування, тестування, модульна контрольна робота.

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

Правила призначення заохочувальних та штрафних балів

Заохочувальні бали не входять до основної шкали РСО, а їх сума не перевищує 10% від максимальної кількості балів. Загальна сума заохочувальних балів не може перевищувати 10 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.

Штрафних балів з дисципліни не передбачається.

Політика дедлайнів та перескладань

Кожен здобувач 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. Здобувач, 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 .

Визнання результатів, здобутих у неформальній освіті

У разі проходження дистанційних курсів/тренінгів можливе зарахування результатів навчання до поточного рейтингу, за умови надання викладачу курсу підтверджуючих документів.

Умови зарахування: у документі (чи на сайті курсу/тренінгу) є перелік тем, які дотичні до тематики курсу із зазначенням обсягу годин.

Дата сертифікату проходження курсу — календарний рік, у якому здійснюється викладання навчальної дисципліни.

Результат проходження дистанційного курсу складає до 75% від можливого результату методики оцінювання курсу. Залежно від кількості прослуханих тем, складності виконуваних завдань до поточного рейтингу здобувача може бути зараховано від 5 до 8 балів.

Здобувач має надати результати практичних робіт (або зробити коротку доповідь про хід виконання цих робіт, та цікавих аспектів прослуханого курсу).

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 здобувачі, що вивчають дану дисципліну, зобов'язані дотримуватися положень прийнятого в університеті Кодексу честі ;

Норми етичної поведінки.

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.

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

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 здобувачем(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 здобувачів 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 балів

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

Система оцінювання/Денна форма навчання

№ з/п	Контрольний захід оцінювання	%	Ваговий бал	Кіл-ть	Всього
1.	Оцінювання знань здобувачів під час проведення семінарського заняття	75	5	15	75
2.	Оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу під час проведення МКР	25	25	1	25
Всього					100

Поточний контроль: оцінка знань за кожною темою заняття, оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу (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 обґрунтуванням, у поєднанні зі слушними доповненнями відповідей інших студентів у процесі дискусії	*5 балів*
активна участь у проведенні заняття; надання правильних відповідей або правильне вирішення задач з незначними неточностями	*4 бали*
суттєве доповнення відповідей здобувачів	*3 бали*
надання відповідей з чисельними значними похибками	*2 бали*

У навчальній дисципліні передбачено проведення *модульної контрольної роботи (МКР)*. Написання МКР має на меті перевірку рівня засвоєння студентами матеріалів, отриманих на момент її проведення. Головним завданням МКР є визначення ступеня розуміння здобувачем 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 здобувачу під час проведення контрольної перевірки рівня засвоєння пройденого матеріалу.

Перелік питань, які пропонуються здобувачам 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. Здобувачі мають можливість звернути увагу на ті питання, розв’язання яких викликало у них певні складності. Викладач має можливість дати здобувачу 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	*25 балів*
письмове тестування ступеня засвоєння навчального матеріалу з наданням відповіді на поставлене питання з незначними неточностями або порушеннями логіки	*20-24 бали*
письмове тестування ступеня засвоєння навчального матеріалу з наданням	*10-19 балів*

неповної відповіді на поставлене питання	
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання з н езначними похибками	*6-9 балів*
письмове тестування ступеня засвоєння навчального матеріалу з наданням не повної відповіді на поставлене питання з чисельними значними похибками	*1-5 балів*

Календарний контроль: провадиться двічі на семестр як моніторинг поточного стану виконання вимог силабусу.

Критерій	Перший	Другий
Термін	8-й тиждень	14-й тиждень
Умови отримання позитивного результату	10 балів	30 балів

Система оцінювання/Заочна форма навчання

№ з/п	Контрольний захід оцінювання	%	Ваговий бал	Кіл-ть	Всього
1.	Оцінювання знань здобувачів під час проведення семінарського заняття (виступи з усними доповідями, виступи з презентаціями, написання есе, презентація порівняльно-правового дослідження, дискусія)	50	5	10	50
2.	Оцінювання результатів домашньої контрольної роботи (ДКР)	50	50	1	50
Всього					100

Теоретична частина включає в себе опрацювання студентами лекційного матеріалу та виступів з доповідями, есе, дискусії, мозковий штурм, моделювання проблемних ситуацій. Критерії оцінювання:

Ваговий бал	Критерій оцінювання
4-5 балів	Здобувач опрацював матеріали лекцій, матеріалом додаткову літературу, вільно володіє, вірно відповідає на питання, підтримує дискусію.
1-3 бали	Здобувач опрацював матеріали лекцій, додаткову літературу, частково володіє матеріалом, частково вірно відповідає на питання, дискусію майже не підтримує.

Домашня контрольна робота

Ваговий бал	Критерій оцінювання
50 балів	Виконується у формі письмового оформлення вирішення ситуаційного кейсу.

Критерії оцінювання домашньої контрольної роботи

письмова робота ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням повної і аргументованої, логічно	*50 балів*

викладеної відповіддю на поставлене питання	
письмова робота ступеня засвоєння навчального матеріалу з наданням відповіді на поставлене питання з незначними неточностями або порушеннями логіки	*30-49 балів*
письмова робота ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання	*20-29 балів*
письмова робота, оцінена менше, ніж 20 балів, підлягає обов'язковому доопрацюванню	*примітка*

Семестровий контроль: залік.

Умови допуску до семестрового контролю: необхідною умовою допуску до заліку є підсумковий рейтинг за семестр не менше 30 балів.

Порядок допуску, критерії оцінювання спільні для денної та заочної форми навчання.

Можливість отримання оцінки "автоматом": так, для здобувачів, які виконали умови допуску до заліку і мають рейтинг ≥ 60 балів. Здобувачі, які набрали протягом семестру 60 і більше балів, мають можливість (при бажанні) отримати залік відповідно до набраного рейтингу без підсумкової співбесіди з викладачем як заохочення за активну та продуктивну роботу протягом семестру.

Зі здобувачами, які набрали протягом семестру від 30 до 59 балів за умови позитивного виконання МКР (ДКР), проводиться *залікова співбесіда*, яка передбачає відповіді на чотири теоретичні питання навчального матеріалу і вирішення одного ситуаційного завдання.

Також залікова співбесіда застосовується щодо здобувачів, які не бажають отримати залік "автоматом".

Залік проходить за умовами жорсткого РСО (попередні бали не додаються).

Залік проходить в режимі співбесіди за теоретичними питаннями та з виконанням практичних завдань.

Здобувач має дати відповідь на чотири залікові питання зі списку, та виконати одне практичне завдання в межах цих питань.

№ з/п	Контрольний захід залікової співбесіди	%	Ваговий бал	Кіл-ть	Всього
1	Залікове питання	80	20	4	80
2	Вирішення ситуаційного завдання	20	20	1	20
Всього					100

Критерії оцінювання заліку

Теоретичне питання (під час проведення заліку)

Викладач задає 4 залікових питання.

Ваговий бал	Критерій оцінювання
18 - 20	Здобувач 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.

14 - 17	Не зовсім повна або не достатньо чітка відповідь на поставлене питання, що свідчить про правильне розуміння суті питання, ознайомлення здобувача з матеріалом лекцій та підручника
10 - 13	Здобувач 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
18 - 20	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 та робити самостійні, обґрунтовані висновки. Здобувач вірно визначив правовідносини, сформулював предмет, поняття та окреслив права та обов'язки сторін в межах фабули.
14 - 17	Здобувач розкрив тему на достатньому та задовільному рівні. Матеріал викладено логічно, висновки у відповідях обґрунтовано неповністю. Здобувач вірно визначив правовідносини, частково сформулював предмет, поняття та окреслив права та обов'язки сторін в межах фабули.
10 - 13	Здобувач 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: старший дослідник, кандидат юридичних наук, старший викладач Оксана РАДЗІЄВСЬКА, старший викладач Ірина СОЛОНЧУК

Ухвалено кафедрою інформаційного, господарського і адміністративного права (протокол № 13 від 24 червня 2024 р.)

Погоджено Методичною радою факультету соціології і права (протокол № 9 від 26 червня 2024 р.)