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	*Заочна*
Рік підготовки, семестр	*3 курс, осінній або весняний семестр*
Обсяг дисципліни	*2 кредити (60 годин). Лекційні заняття - 6 годин, практичні (семінарські) заняття - 2 години, СРС - 52 години*
Семестровий контроль/	*Залік / ДКР*
Розклад занять	*http://rozklad.kpi.ua/*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: *старший викладач, к.ю.н., старший дослідник Радзієвська Оксана Григорівна, e- mail: radeoksa@gmail.com.; 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; викладач Самчинська Оксана Андріївна, e-mail: samchynska.kpi@gmail.com; старший викладач, к.ю.н., старший дослідник Радзієвська Оксана Григорівна, e-mail: radeoksa@gmail.com; старший викладач, к.ю.н., Дорогих Сергій*

Програма навчальної дисципліни

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

Розвиток та впровадження сучасних інформаційно-комунікаційних технологій призвели до суттєвих змін в усіх сферах життя сучасного суспільства. Активна цифровізація суспільних відносин супроводжується виникненням новітніх викликів та загроз для людини, суспільства і держави в інформаційному та кібернетичному просторі. Питання забезпечення інформаційної безпеки, як на індивідуальному, так і державному й світовому рівнях, стає дедалі актуальним. Відповідно до положень статті 17 Конституції України, забезпечення інформаційної безпеки України є справою усього Українського народу.

Розуміння природи і сутності процесів та явищ, які відбуваються в інформаційному просторі у нинішній час, механізму їх впливу на процеси забезпечення інформаційної безпеки людини, суспільства і держави є одним з головних превентивних шляхів запобігання інформаційній небезпеці та її наслідкам.

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

- надання основоположних знань щодо сутності інформаційної безпеки, особливостей правовідносин, що виникають в інформаційній сфері;

- опанування знаннями щодо 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 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.

Відповідно до інтегрованих вимог ОПП різних спеціальностей **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**:**

- **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.

- **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 невирішені 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 та 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/спеціалізацією.

3. Зміст навчальної дисципліни

Тема 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.

Тема 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 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 4. Інформаційна діяльність як об'єкт небезпеки (частина 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.

Тема 4. Інформаційна діяльність як об'єкт небезпеки (частина 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.

Тема 5. Основні чинники, які впливають на рівень забезпеченості інформаційної та кібернетичної безпеки

Зовнішні чинники

Внутрішньодержавні чинники

Тема 6. 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 7. Юридична відповідальність за правопорушення в сфері забезпечення інформаційної безпеки

Поняття кіберзлочинності. Конвенція Ради Європи «Про кіберзлочинність» 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.

Тема 8. Стратегічні підходи правового вирішення питань забезпечення інформаційної та кібернетичної безпеки

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;
- Стратегії зовнішньополітичної діяльності України;

Характеристика основних положень Закону України «Про основні засади забезпечення кібербезпеки України».

4. Навчальні матеріали та ресурси

Для успішного вивчення дисципліни достатньо опрацьовувати навчальний матеріал, який поряд з базовими положеннями, враховує обрану студентами спеціальність, викладається на лекціях та конспекти яких після завершення заняття надсилаються на електронну адресу навчальної групи та старості цієї групи.

Також доцільно ознайомитися з тематичними розділами наступних джерел інформації.

Базова література:

1. Правове забезпечення інформаційної безпеки : курс лекцій / В. Фурашев, О. Радзієвська ; ДНУ «Ін-т інформ., безпеки і права Нац. акад. прав. наук України». – Київ; Одеса : Фенікс, 2022. 158 с. URL: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-bezpeki

2. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації: навчальний посібник / О. Довгань , Н. Ткачук , Т. Ткачук , В. Петров. – К., Артек. 2022. 171 с. URL: https://ippi.org.ua/pravovi-zasadi-zabezpechennya-kiberbezpeki-v-umovakh-tsifrovoi-transformatsii

3. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. – Київ-Одеса : Фенікс, 2020. 260 с. URL: https://ippi.org.ua/zakhist-prav-privatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu

4. 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 права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. URL: https://ippi.org.ua/kiberbezpeka-v-informatsiinomu-suspilstvi

Допоміжна література:

1. Права людини: інформаційний вимір: монографія / О.О. Тихомиров. – Одеса: Видавництво «Юридика», 2023. 304 с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf

2. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О. П. Дзьобаня. – Харків: Право, 2021. – 776 с. URL: http://ippi.org.ua/natsionalna- bezpeka-svitoglyadni-ta-teoretiko-metodologichni-zasadi

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. (Розділ 4. Характеристика галузевих видів юридичної відповідальності за інформаційні делікти.) URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf

4. 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

5. Інформаційне та соціально-правове моделювання: посібник / Д. В. Ланде, В. М. Фурашев; за заг. ред. Д. В. Ланде. – Київ-Одеса : Фенікс, 2021. – 276 с. - URL: http://ippi.org.ua/sites/default/files/posibnik.pdf

6. Кібербезпека «суспільства знань»: монографія/ Довгань О., Тарасюк А., Ткачук Т. : монографія. – Київ-Одеса : Фенікс, 2021. – 176 с. URL: http://ippi.org.ua/kiberbezpeka-%C2%ABsuspilstva-znan%C2%BB

7. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія / Н. Уханова; за заг. ред. В. Пилипчука. – Київ- Одеса: Фенікс, 2022. 140 с. URL: http://ippi.org.ua/problemi-protidii-negativnim- informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus

8. Соціальні та цифрові трансформації: нова парадигма кібербезпеки. Монографія. / О. А. Баранов. – Київ: 2021. 86 с. URL: https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsii-nova-paradigma-kiberbezpeki

9. Трансформація: соціальна & цифрова & правова: монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату / О. А. Баранов. – Одеса: Видавничий дім «Гельветика», 2022. 272 с. URL: https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova

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)

Опанування навчальної дисципліни «Інформаційна безпека» відбувається на лекційних, семінарському (практичному) занятті та під час самостійної роботи студента. Під час лекційних та семінарського (практичного) занять за конкретною темою акцент робиться не лише на доведенні фундаментальних положень, а й на об'єктивній необхідності цих знань за обраною студентом спеціальністю, а також у повсякденному житті. Під час проведення семінарського (практичного) заняття застосовується методи дискусії (доповідач-опонент/опоненти), аналізу та прогнозування з наведенням конкретних прикладів зі сфери обраної спеціальності. Крім того, під час проведення семінарського (практичного) заняття може здійснюватися бліц-опитування.

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 необхідності, у взаємно погоджений час.

6. Самостійна робота студента

Самостійна робота студента (СРС) передбачає самостійне опрацювання матеріалу, віднесеного до самостійного розгляду на семінарському (практичному) занятті, з використанням лекційного матеріалу і рекомендованої літератури. Перевірка рівня засвоєння матеріалу для самостійного опрацювання проводиться в процесі обговорення питань на аудиторних заняттях та під час виконання індивідуального завдання.

Для підготовки до семінарського (практичного) заняття студенти самостійно готуються, використовуючи конспект лекцій та рекомендовану літературу з даної тематики, а також будь-які інші джерела інформації.

У разі виникнення складнощів під час підготовки до проведення семінарського (практичного) 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, залежно від встановленої форми проведення навчального процесу.

Невід'ємною складовою самостійної роботи студента є виконання індивідуального завдання – *домашньої контрольної роботи (далі – ДКР)*. Написання *домашньої контрольної роботи (ДКР)* має на меті перевірку рівня засвоєння студентами матеріалів, отриманих на момент її проведення.

Головною метою ДКР 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 ДКР передбачає письмове викладення у довільної формі трьох питань за матеріалами навчальної дисципліни, визначених викладачем. Тематика ДКР надається викладачем індивідуально кожному студенту. Перелік питань, які пропонуються студентам у якості тематики ДКР, формується на основі переліку тематичних питань до лекційних занять та питань для самоперевірки. Виконані роботи надсилаються для перевірки на електронну пошту викладача не пізніше як за тиждень до початку заліково-екзаменаційної сесії. **Роботи, які здаються із порушенням вимог академічної доброчесності, не оцінюються.**

Під час семінарського (практичного) заняття навчальної дисципліни відбувається розгляд та обговорення виконаних ДКР. 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.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Відвідування занять

У зв'язку зі специфікою тематики навчальної дисципліни, стрімким науково-технічним прогресом у сфері інформаційно-комунікативних та комунікаційних засобів, контентна складова кожної теми, за виключенням базових положень, постійно змінюється. Саме тому конспект лекції надсилається студентам після проведення лекційного заняття з метою підготовки до семінарського (практичного) заняття. Відвідування семінарського (практичного) заняття, незалежно від форми його проведення, є обов'язковим. Бали за відвідування лекційних занять не нараховуються.

Правила поведінки на заняттях: здобувач вищої освіти має можливість отримати бали за відповідні види навчальної активності на семінарському (практичному) занятті. Використання засобів зв'язку для пошуку інформації в мережі Інтернет здійснюється за умови вказівки викладача.

Якщо заняття відбувається в дистанційному режимі (з використанням платформ Zoom, Google Meet тощо), під час відповіді студенти **обов'язково** повинні вмикати відеозв'язок.

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.

Порушення термінів виконання завдань та заохочувальні бали

Ключовими заходами при викладанні дисципліни є ті, які формують семестровий рейтинг студента.

Штрафних балів не передбачено.

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.

Визнання результатів здобутих у неформальній освіті

У разі проходження дистанційних курсів та/або вебінарів та участі у інших заходах, пов'язаних з тематикою дисципліни, можливе зарахування результатів навчання до поточного рейтингу, за умови надання студентом підтверджуючих документів.

Умови зарахування:

- тематика курсу/вебінару дотична до тем, які розглядаються під час вивчення дисципліни;
- студент надає сертифікат, або інший документ, який підтверджує проходження курсу/вебінару (за можливості із активним посиланням для перевірки автентичності);
- у сертифікаті (іншому підтверджувальному документі) одночасно зазначені прізвище та ім'я студента;
- дата проходження курсу припадає на поточний навчальний рік.

Викладач залишає за собою право провести усну співбесіду або отримати від здобувача вищої освіти короткий звіт про результати проходження курсу для того, щоб пересвідчитися, що студент особисто та добросовісно проходив курс.

Виконання вказаних робіт може бути зараховано студенту як відпрацювання одного із занять за темою, попередньо узгодженою із викладачем.

Залежно від кількості прослуханих тем, складності виконуваних завдань та тривалості вебінару (іншого заходу), до поточного рейтингу студента може бути зараховано від 5 до 10 балів.

Пропущені контрольні заходи оцінювання

Кожен студент зобов'язаний дотримуватися термінів виконання завдань у межах розкладу проведення аудиторних занять з дисципліни. Пропущені заходи оцінювання знань студентом(ами) по темі навчальної дисципліни вирішується шляхом усунення заборгованості за взаємною домовленістю з викладачем щодо дати та часу відпрацювання.

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 семінарського (практичного) заняття;

2) домашня контрольна робота (ДКР).

Оцінювання якості та глибини розкриття поставленого питання під час проведення семінарського (практичного) заняття здійснюється відповідно до наступних положень:

Критерій оцінювання	Ваговий бал
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	20
активна участь у проведенні заняття; надання правильних відповідей або правильне вирішення задач з незначними неточностями	18
надання відповідей або вирішення задач з похибками	15
надання відповідей з чисельними значними похибками	12
суттєве доповнення відповідей студентів	12

Оцінювання якості та глибини розкриття, під час проведення ДКР, кожного з 3-х поставлених питань здійснюється відповідно до наступних положень:

Критерій оцінювання	Ваговий бал
письмове тестування ступеня засвоєння навчального матеріалу по розділу навчальної дисципліни з наданням повної і аргументованої, логічно викладеної відповіддю на поставлене питання з наведенням власних прикладів (за необхідності)	10 балів
письмове тестування ступеня засвоєння навчального матеріалу з наданням відповіді на поставлене питання з незначними неточностями або порушеннями логіки	9 балів
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання	8 бали
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання з незначними похибками	7 балів
письмове тестування ступеня засвоєння навчального матеріалу з наданням не повної відповіді на поставлене питання з чисельними значними похибками	6 балів

Заохочувальні бали

Критерій оцінювання	Ваговий бал
підготовка тез доповіді на науковій (науково-практичній) конференції або круглому столі за тематикою навчальної дисципліни	10
проходження тематичних курсів на онлайн-платформах	5-10
участь у вебінарах, лекціях, майстер-класах та інших заходах за тематикою навчальної дисципліни	5-10

Відповідно до Положення про систему оцінювання результатів навчання сума всіх заохочувальних балів не може перевищувати 10% стартової складової рейтингової шкали оцінювання – балів, отриманих протягом поточного контролю, тобто 10 балів.

Семестровий контроль: залік (проводиться на окремому занятті).

Умови допуску до семестрового контролю: є виконання домашньої контрольної роботи (ДКР).

Залікова робота складається з п'ятдесяти тестових запитань, кожне з яких містить одну, або декілька правильних відповідей та оцінюється в один бал. Максимальна кількість балів – 50. Час для виконання тестових завдань – 50 хвилин. Орієнтовний перелік питань до заліку наведений у п. 9 цього Силабусу.

Рейтинг студента з дисципліни складається з балів, отриманих за:

- роботу на семінарському (практичному) занятті;
- виконання домашньої контрольної роботи (ДКР);
- виконання залікової роботи.

Для отримання найвищого рейтингу студенту потрібно брати активну участь у семінарському (практичному) занятті, виконати ДКР та залікову роботу.

Студент може оскаржити оцінку викладача, подавши відповідну скаргу не пізніше наступного дня після ознайомлення студента з виставленою оцінкою. Скарга розглядатиметься за процедурами, встановленими університетом.

Система оцінювання

№ з/п	Контрольний захід оцінювання	%	Ваговий бал	Кіл-сть	Всього
1.	Оцінювання знань студентів під час проведення семінарського (практичного) заняття	20	20	1	20
2.	Оцінювання знань студентів під час проведення ДКР	30	30	1	30
3.	Оцінювання результатів залікової роботи	50	50	1	50
	Всього				**100**

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

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

9. Додаткова інформація з дисципліни (освітнього компонента)

Орієнтовні питання до заліку

1. Основні трансформаційні процеси сучасності з точки зору інформаційної безпеки.
2. Тотожності та відмінності сутностей війни та збройного конфлікту. Основні види війн. Основні цілі та завдання сучасних війн.
3. Витоки трансформаційних процесів організації та проведення локальних та регіональних конфліктів та війн. Характерні ознаки гібридних війн.
4. Предмет та основні завдання інформаційної безпеки.
5. Природа та сутність інформації. Визначення поняття «інформація» з точки зору інформаційної безпеки. Законодавче визначення поняття «інформація».
6. Основні властивості інформації з позиції інформаційної безпеки. Сутність та визначення понять «безпека інформації», «безпечність інформації» та «захист інформації».
7. Сутність та визначення поняття «інформаційна безпека». Об'єкти інформаційної небезпеки та їх ієрархія.
8. Спрямованість законодавчо визначених обмежень прав людини та громадянина в інформаційної сфері.
9. Сутність прав та свобод людини і громадянина в інформаційної сфері.
10. Сутність та поняття цензури.
11. Взаємозв'язок між забезпеченням прав та свобод людини і громадянина в інформаційної сфері та забезпеченням інформаційної безпеки.
12. Відображення терміну «інформаційна безпека» у законодавстві України.
13. Зв'язок сутності понять «кібернетика» та «небезпеки».
14. Сутність та визначення поняття «кібербезпека».
15. Взаємозв'язок інформаційної безпеки та кібербезпеки. Ознаки коректності застосування термінів «інформаційна безпека» та «кібербезпека».
16. Сутність та законодавче визначення поняття «інформаційна діяльність». Основні види та напрями інформаційної діяльності.
17. Чинники які визначають ступінь ефективності проведення інформаційної діяльності.
18. Складові інформаційної діяльності. Сутність інформаційного виробництва. Основні елементи інформаційного виробництва.
19. Взаємозв'язок інформаційної діяльності та інформаційної безпеки.
20. Характерні риси постіндустріального суспільства з точки зору здійснення інформаційної діяльності.
21. Перспективи та напрями розвитку інформаційної діяльності в умовах науково- технічного прогресу в інформаційної сфері та її вплив на процеси забезпечення інформаційної безпеки.
22. Сутність поняття «маніпуляція». Види маніпуляції та їх характерні прийоми.
23. Роль та місце маніпулювання в системі державного управління та політичних системах (з наведенням конкретних прикладів).
24. Роль та місце маніпулювання у здійсненні міжнародних стосунків (з наведенням конкретних прикладів).
25. Сутність інформаційного насильства. Прояви інформаційного насильства (з наведенням конкретних прикладів).
26. Тотожності та відмінності процесів маніпулювання свідомістю людини та інформаційного насильства. Чинники, які створюють проблемні питання правового запобігання здійснення інформаційного насильства.
27. Сутність поняття «національна безпека». Законодавчі акти в системі забезпечення національної безпеки.
28. Сутність поняття «міжнародна безпека». Міжнародні системи колективної безпеки та їх сутності. Наведіть приклади.

29. Спрямованість трансформаційних процесів в системах міжнародної безпеки.

30. Роль та місце інформаційної безпеки у системі національної безпеки.

31. Роль та місце інформаційної безпеки в системах міжнародної безпеки.

32. Сутність понять «загроза» в інформаційної сфері та «інформаційна операція».

33. Сутність поняття «спеціальна інформаційна операція». Наведіть приклади.

34. Сутність поняття «інформаційна експансія». Наведіть приклади.

35. Сутність понять «насильство», «жорстокість», «порнографія».

36. Розуміння поняття «інформаційна інфраструктура».

37. Доктринальні та стратегічні нормативно-правові акти України в сфері забезпечення інформаційної безпеки, які визначають сучасні реальні та потенційні загрози в інформаційної сфері.

38. Основні загрози міжнародній безпеці в сфері інформаційної безпеки.

39. Сутність та визначення понять «інформаційна система», «комунікаційна система» та «інформаційно-комунікаційна система». Наведіть приклади.

40. Сутність та визначення поняття «технологія». Наведіть приклади.

41. Сутність процесів забезпечення безпеки глобальних інформаційних систем та мереж.

42. Сутність та визначення поняття «соціалізація» та «кіберсоціалізація».

43. Витоки загроз для особистості в умовах кіберсоціалізації.

44. Основні положення Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки», які стосуються питань забезпечення інформаційної безпеки.

45. Принципи та механізми глобалізації інформаційного простору.

46. Наслідки глобалізації інформаційного простору.

47. Сутність, цілі, завдання та можливості соціальних мереж .

48. Наслідки функціонування та розширення соціальних мереж.

49. Чинники які визначають особливості та проблеми реалізації інформаційних правовідносин в мережі Інтернет.

50. Сутність та визначення поняття «кіберзлочин» та «кіберзлочинність».

51. Сутність, мотивація та визначення поняття «кібертероризм».

52. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Україні.

53. Спрямованість юридичної відповідальності за правопорушення в кіберпросторі в Європейському Союзі.

54. Сутність, прояви та наслідки кібертероризму.

55. Відображення у законодавстві України юридичної відповідальності за спробу здійснення або здійснення кібертероризму.

56. Законодавче визначені обмеження прав людини та громадянина в інформаційній сфері.

57. Сутність та поняття цензури.

58. Взаємозв’язок між забезпеченням прав та свобод людини і громадянина в інформаційної сфері та забезпечення інформаційної безпеки.

59. Основні положення Стратегії кібербезпеки України.

60. Основні положення Воєнної доктрина України в частині забезпечення інформаційної та кібернетичної безпеки.

61. Основні положення Концепції розвитку сектору безпеки і оборони України в частині забезпечення інформаційної та кібернетичної безпеки.

62. Основні положення Конституції України в частині забезпечення інформаційної безпеки. Концепція розвитку сектору безпеки і оборони України.

63. Основні положення Закону України «Про інформацію» в частині забезпечення інформаційної безпеки.

64. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» в частині забезпечення інформаційної безпеки.

65. Основні положення Закону України «Про основні засади забезпечення кібербезпеки України» в частині забезпечення кібернетичної безпеки.

66. Сутність поняття «правове забезпечення». Складові процесу правового забезпечення та їх зміст. Об'єкти та суб'єкти складових системи правового забезпечення.

67. Відмінності та тотожності понять «правове забезпечення» та «законодавче забезпечення».

68. Тенденції розвитку постіндустріального суспільства. Спрямованість трансформаційних процесів правовідносин у постіндустріальному суспільстві.

69. Характер та спрямованість реальних та потенційних загроз в інформаційній сфері у постіндустріальному суспільстві.

70. Сутність та витоки глобалізації інформаційного простору.

71. Сутність поняття «суверенітет». Види суверенітету. Сутність (принципи) інформаційного суверенітету. Законодавче визначення поняття «інформаційний суверенітет держави».

72. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері.

73. Проблемні питання правового реагування на трансформаційні процеси забезпечення національної та міжнародної інформаційної безпеки та можливі шляхи їх вирішення.

74. Правові обмеження щодо створення, поширення, збереження, обробки та знищення інформації.

75. Сутність поняття «інформаційний ресурс». Інформаційний ресурс як об'єкт інформаційної небезпеки.

76. Основоположні положення Конституції України щодо поводження з інформацією.

77. Основні напрями дій, які віднесені до правопорушень в інформаційної сфері відповідно до положень Кримінального кодексу України сфері

78. Законодавчо визначені обмеження прав людини та громадянина в інформаційній сфері.

Робочу програму навчальної дисципліни (силабус):

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

старший викладач, к.ю.н., старший дослідник Радзієвська Оксана Григорівна;

викладач Самчинська Оксана Андріївна.

Ухвалено кафедрою інформаційного, господарського та адміністративного права (протокол № 12 від 27 травня 2024 р.)

Погоджено Методичною радою КПІ ім. Ігоря Сікорського (протокол № 8 від 20 червня 2024 р.)