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	*12 Інформаційні технології*
Спеціальність	*122 Комп'ютерні науки*
Освітня програма	*Цифрові технології в енергетиці*
Статус дисципліни	*Нормативна*
Форма навчання	*Очна (денна, заочна)*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*2 кредити (60 годин). Лекційні заняття - 18 годин, практичні заняття - 18 годин, СРС - 24 години — денна форма навчання* *2 кредити (60 годин). Лекційні заняття - 6 годин, практичні заняття - 4 години, СРС - 50 годин — заочна форма навчання*
Семестровий контроль/ контрольні заходи	*Залік, МКР*
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, старший викладач, к.ю.н., старший дослідник Радзієвська Оксана Григорівна, e-mail: radeoksa@gmail.com.* Практичні**:** *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 Олександрович, e-mail: dorohykh@gmail.com*
Розміщення курсу	*Сайт кафедри, Google Class, https://ecampus.kpi.ua/home.*

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.

Метою дисципліни є формування у студентів наступних *компетентностей:*

- здатність до абстрактного мислення, аналізу та синтезу (ЗК1);

- здатність вчитися і оволодівати сучасними знаннями(ЗК6);
- здатність бути критичним і самокритичним (ЗК10);
- 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 (ЗК14).

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.

Завданням дисципліни є вдосконалення 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:

- розуміти і реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності вільного демократичного суспільства, верховенства права, прав і свобод людини і громадянина в Україні, дотримуватися академічної доброчесності (ПР 24);
- 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)

Зазначена дисципліна викладається на 3 курсі, тобто тоді, коли студенти вже прослухали дисципліни «Україна в контексті історичного розвитку Європи», «Безпека інформаційних систем», «Об'єктно-орієнтоване програмування», «Технології розробки програмного забезпечення».

З іншого боку, викладений матеріал може бути використаний при вивченні дисциплін, наприклад, «Проектування інформаційних систем» та при виконанні дипломної роботи.

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 безпеки, кібербезпеки

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. 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».

Тема 8. 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.

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 одразу 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. 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
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:

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. 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

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 моделюваннння: 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. 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

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, практичних заняттях та під час підготовки самостійної роботи студента. Під час лекційних та практичних 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 практичних занять застосовується методи дискусії (доповідач-опонент/опоненти), аналізу та прогнозування з наведенням конкретних прикладів зі сфери обраної спеціальності. Крім того, під час проведення практичного заняття може здійснюватися бліц-опитування не лише в межах теми поточного заняття, а й тем, що розглядалися раніше.

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.

6. Самостійна робота студента

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

Особливу увагу студентам заочної форми навчання слід звернути на підготовку практичних 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 занятту та тих, що віднесені до завдань на СРС, використовуючи конспект лекцій відповідної теми 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 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.

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)

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 одразу після проведення лекційного заняття з метою підготовки до практичного заняття. Бали за відвідування лекційних занять не нараховуються. Факт присутності на практичному занятті також не оцінюється, проте основна частина рейтингу студента формується через активну участь у практичних заняттях та належний рівень підготовки до них.

Правила поведінки на заняттях: здобувач вищої освіти має можливість отримувати бали за відповідні види навчальної активності на практичних заняттях, передбачені РСО дисципліни. Використання засобів зв'язку для пошуку інформації в мережі Інтернет здійснюється за умови вказівки викладача.

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. Проте, у випадку порушення строку відпрацювання пропущеного практичного заняття передбачене зниження максимального балу на один рівень.

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 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	≥ 15 балів	≥ 35 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 практичного заняття;

2) модульна контрольна робота (МКР).

Оцінювання якості та глибини розкриття поставленого питання під час проведення практичних занять 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	8
активна участь у проведенні заняття; надання правильних відповідей або правильне вирішення задач з незначними неточностями	7
надання відповідей або вирішення задач з похибками	6
надання відповідей з чисельними значними похибками	5
суттєве доповнення відповідей студентів	5

Модульна контрольна робота

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 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 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:

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)	28 балів
письмове тестування ступеня засвоєння навчального матеріалу з наданням відповіді на поставлене питання з незначними неточностями або порушеннями логіки	20 балів
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання	20 бали
письмове тестування ступеня засвоєння навчального матеріалу з наданням неповної відповіді на поставлене питання з незначними похибками	17 балів
письмове тестування ступеня засвоєння навчального матеріалу з наданням не повної відповіді на поставлене питання з чисельними значними похибками	15 балів

Заохочувальні бали

Критерій оцінювання	Ваговий бал
підготовка тез доповіді на науковій (науково-практичній) конференції або круглому столі за тематикою навчальної дисципліни	3
проходження тематичних курсів на онлайн-платформах	3

участь у вебінарах, лекціях, майстер-класах та інших заходах за тематикою навчальної дисципліни	2
активна участь у засіданні студентського гуртка наукового спрямування «Право в епоху цифровізації»	2

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.

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

Семестровий контроль: залік.

Студенти, які на момент проведення заліку мають рейтинг ≥ 60 балів, за бажанням, отримують залік «автоматом».

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 практичного заняття	72	8	9	72
2.	Оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу під час проведення МКР	28	28	1	28
				Всього	100

У разі складання заліку студент дає відповідь на 2 теоретичних питання та вирішує ситуаційне завдання.

Теоретичне питання *(під час проведення заліку)*

Критерій оцінювання	Вагови й бал
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.	25-35
Студент розкрив тему на задовільному рівні. Здобувач вказав основні поняття та нормативно-правові акти. У відповіді висновки обґрунтовано неповністю.	20-24

Вирішення ситуаційного завдання *(під час проведення заліку)*

Критерій оцінювання	Вагов ий бал
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.	30
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.	25-29
Студент не розкрив задачу (кейс) на достатньому рівні, відповідь не містить посилань на нормативно-правові акти. Робота не містить обґрунтованих висновків.	20-24

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. 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.
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 здійсненню 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 забезпеченнямправ і свободлюдини, громадянина в інформаційної сфері та забезпечення інформаційної безпеки.
60. Основні положення Стратегії кібербезпеки України.
61. Основні положення Воєнної доктрина України в частин 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 ЗаконуУкраїни «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
старший викладач, к.ю.н., старший дослідник Радзієвська Оксана Григорівна
викладач Самчинська Оксана Андріївна

Ухвалено кафедрою інформаційного, господарського і адміністративного права (протокол № 16 від 20.05.2023р.)

Погоджено Методичною комісією ННІАТЕ КПІ ім. Ігоря Сікорського (протокол № 9 від _26.05.2023 р.)