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

Кафедра інформаційного, господарського та адміністративного права

ІНФОРМАЦІЙНА БЕЗПЕКА ЗО 09

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	***Перший (бакалаврський)***
Галузь знань	*11 Математика та статистика*
Спеціальність	***113 Прикладна математика***
Освітня програма	***Наука про дані та математичне моделювання***
Статус дисципліни	*Нормативна*
Форма навчання	*очна(денна)*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*2 кредити ЕКТС / 60 год.:* *(18 год. – лекції, 18 год. – семінарські заняття, 24 год. – СРС)*
Семестровий контроль/ контрольні заходи	*залік*
Розклад занять	*http://rozklad.kpi.ua*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	Лектор: кандидат юридичних наук Рудник Людмила Іванівна, Rudnyklyudmyla@gmail.com Практичні: кандидат юридичних наук Рудник Людмила Іванівна, Rudnyklyudmyla@gmail.com
Розміщення курсу	Посилання на дистанційний ресурс Google classroom https://classroom.google.com/c/NzU5OTk0Mjg0ODc4

1. Програма навчальної дисципліни

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

У сучасному інформаційному суспільстві безпека даних є не лише технічним, а й правовим питанням. Порушення конфіденційності, цілісності та доступності інформації несе юридичні наслідки як для фахівців, так і для компаній. Законодавство України (зокрема Закон «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», ККУ, КУпАП) встановлює чіткі правила обробки та захисту даних. Фахівець з прикладної математики, що працює з персональними, критично важливими або комерційними даними, повинен володіти юридичними основами інформаційної безпеки, розуміти відповідальність за порушення, а також вміти проектувати рішення з урахуванням норм права.

Мета дисципліни. Сформувати в студентів базові правові знання у сфері інформаційної безпеки, надати уявлення про національні та міжнародні нормативно-правові акти, що регулюють діяльність з обробки, зберігання та захисту інформації, а також сформувати відповідальні та етичні підходи до професійної діяльності.

Предмет дисципліни. Сукупність теоретичних та практичних знань про нормативно-правове регулювання інформаційної безпеки, включаючи принципи кібергігієни, юридичну відповідальність за порушення режиму захисту інформації, правові механізми захисту персональних даних, цифрових прав, авторського права та конфіденційної інформації.

Загальні компетентності

ЗК06 (Здатність до абстрактного мислення, аналізу та синтезу.),

ЗК08 (Знання та розуміння предметної області та розуміння професійної діяльності.),

ЗК14 (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.),

ЗК16 (Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів недоброчесності).

Фахові компетентності

ФК06 (Здатність розв'язувати професійні задачі за допомогою комп'ютерної техніки, комп'ютерних мереж та Інтернету, в середовищі сучасних операційних систем, з використанням стандартних офісних додатків),

ФК10 (Здатність створення документів встановленої звітності, використання нормативно-правових документів),

ФК12 (Здатність до пошуку, систематичного вивчення та аналізу науково-технічної інформації, вітчизняного й закордонного досвіду, пов'язаного із застосуванням математичних методів для дослідження різноманітних процесів, явищ та систем),

ФК16 (Здатність до ефективної професійної письмової й усної комунікації українською мовою та однією з офіційних мов ЄС),

ФК18 (Здатність оцінювати коректність застосування математичних моделей та методів до проблемних ситуацій).

Програмні результати навчання (ПРН)

ПРН 14 В являти здатність до самонавчання та продовження професійного розвитку.

ПРН 15 Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу.

ПРН 16 Демонструвати навички взаємодії з іншими людьми, уміння працювати в команді.

ПРН 17 Уміти здійснювати збір, опрацювання, аналіз, систематизацію науково-технічної інформації, уникаючи при цьому

академічної недоброчесності.

ПРН 18 Ефективно спілкуватися з питань інформації, ідей, проблем та рішень зі спеціалістами та суспільством загалом.

ПРН 19 Збирати та інтерпретувати відповідні дані й аналізувати складності в межах своєї спеціалізації для донесення суджень, які відбивають відповідні соціальні та етичні проблеми.

ПРН 20 Демонструвати навички професійного спілкування, включаючи усну та письмову комунікацію українською мовою та принаймні однією з офіційних мов ЄС.

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

Вивченню дисципліни «Інформаційне право» повинне передувати вивчення дисциплін: «Програмне забезпечення обчислювальних систем», «Бази даних та інформаційні системи», «Математична логіка та теорія алгоритмів».

Отримані практичні навички та засвоєні знання можна використовувати в таких дисциплінах як: «Системний аналіз», «Курсова робота з системного аналізу», «Переддипломна практика», «Дипломне проєктування»

Результати навчання, які формуються освітнім компонентом	***Як, яким чином, за допомогою яких методів формуються результати навчання***	***Як перевіряється формування результатів навчання***
Студенти матимуть розуміння, як діяти на	*Методика опанування навчальної дисципліни:*	*Поточний контроль здійснюється через:*

основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки	*лекційні заняття, практичні заняття, самостійна робота студентів*	- *Опрацювання лекційного матеріалу (ведення конспекту, робота з підручниками та додатковими джерелами);* - *Участь у практичних заняттях (усні відповіді, підготовка доповідей з проблемних правових питань, вирішення кейсів);* - *Виконання тематичних контрольних завдань;* - *Проходження модульної контрольної роботи.*
Студенти вмітимуть готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки	*Формування результатів навчання здійснюється з використанням таких методів:* • *Пояснювально-ілюстративний* • *Метод проблемного викладу* • *Дослідницький метод*	*Календарний контроль: проводиться двічі на семестр як моніторинг поточного стану виконання вимог Силабусу.* *Семестровий контроль: залік*
Студенти вмітимуть впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки		
Вмітимуть виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем		
Вмітимуть виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах		

3. Зміст навчальної дисципліни

Тема 1. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИ

1. Концепція інформаційної безпеки України.
2. Інформаційна безпека: понятійний апарат
3. Інтереси особи, суспільства та держави в інформаційній сфері
4. Об’єкти, суб’єкти інформаційної безпеки
5. Види інформаційної безпеки

Тема 2. ІНТЕРНЕТ ТА ІНФОРМАЦІЙНА БЕЗПЕКА

1. Правова природа Інтернет-правовідносин
2. Суб’єктний склад відносин у мережі Інтернет
3. Об’єкти Інтернет-правовідносин
4. Загрози при роботі в Інтернеті і способи їх уникнення

Тема 3. КІБЕРНЕТИЧНА БЕЗПЕКА. ЗВ’ЯЗОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ

1. Кібербезпека як складова міжнародної, регіональної та національної безпеки
2. Кіберсоціалізація особистості
3. Мережна мобілізація: питання демократії та безпеки
4. Сутність та характерні ознаки кіберцивілізації
5. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект

Тема 4. ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ЯК ОБ’ЄКТ НЕБЕЗПЕКИ (ЧАСТИНА ПЕРША)

1. Інформаційна діяльність: сутність, складові та засоби здійснення.
2. Інформаційне виробництво.
3. Інформаційне забруднення.
4. Інформаційне середовище.
5. Інформаційні ресурси: поняття, функції, ієрархічні рівні.

Тема 4. ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ЯК ОБ’ЄКТ НЕБЕЗПЕКИ (ЧАСТИНА 2)

1. Сутність поняття «інформаційний вплив»
2. Співвідношення понять «Інформаційна операція» та «інформаційна війна»
3. «Інформаційна зброя» як засіб ведення інформаційних війн
4. Маніпулювання свідомістю, сутність та види маніпуляції.
5. Сутність та прояви інформаційного насильства.
6. Проблемні питання правового запобігання здійсненню інформаційного насильства.

Тема 5. Основні напрями реалізації прав і свобод людини в сфері інформації

1. Право громадян на звернення щодо надання інформації.
2. Доступ до правової інформації.
3. Доступ до екологічної інформації.
4. Право на доступ до інформації для споживачів щодо харчових продуктів
5. Інформаційні права громадян як суб’єктів виборчого процесу.
6. Захист персональних даних.
7. Особливості реалізації права на доступ до інформації про стан довкілля, якість харчових продуктів та предметів побуту в умовах воєнного стану

Тема 6. ПОНЯТТЯ «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ». ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ОБІГУ ІНФОРМАЦІЇ

1. Нормативно-правове забезпечення в сфері інформаційної безпеки.
2. Роль категорійно-понятійного апарату в системі нормативно-правового забезпечення.
3. Правові гарантії безпечного обороту інформації.
4. Законодавче обмеження доступу до інформаційних ресурсів

Тема 7. КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРТЕРОРИЗМ

1. Кіберзлочинність: поняття та сутність. Конвенція Ради Європи «Про кіберзлочинність» від 23.11.01 р. № 994-575
2. Поняття комп'ютерної злочинності. Загальна характеристика комп'ютерних злочинів.
3. Кібертероризм: поняття та сутність.
4. Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
5. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
6. Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
7. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX

Тема 8. СТРАТЕГІЧНІ ПІДХОДИ ПРАВОВОГО ВИРІШЕННЯ ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

1. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері.
2. Поняття та сутність інформаційного суверенітету.
3. Трансформація кіберзагроз в сучасних умовах.
4. Характеристика основних положень:

- Стратегії національної безпеки України;
- Стратегії інформаційної безпеки України
- Стратегії кібербезпеки України;
- Стратегії зовнішньополітичної діяльності України; 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. 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-vinformatsiinomu-suspilstvi (дата звернення 20.05.2025 р.)
2. Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія. Київ-Одеса : Фенікс, 2020. 260 с. URL: https://ippi.org.ua/zakhist-pravprivatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu(дата звернення 20.05.2025 р.)
3. 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-tsifrovoitransformatsii (дата звернення 20.05.2025 р.)
4. Фурашев В., Радзієвська О. Правове забезпечення інформаційної безпеки: курс лекцій. Київ-Одеса : Фенікс, 2022. 158 с. URL: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi- bezpeki (дата звернення 20.05.2025 р.)

Допоміжна література:

1. Арістова І.В., Баранов О.А., Дзьобань О.П. та ін. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія. Київ: КВІЦ, 2019. 344 с. URL: http://ippi.org.ua/sites/default/files/monografiya_ok_0.pdf (дата звернення 20.05.2025 р.)
2. Баранов О. А. Соціальні та цифрові трансформації: нова парадигма кібербезпеки. Монографія. Київ: 2021. 86 с. URL: https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsiinova-paradigma-kiberbezpeki (дата звернення 20.05.2025 р.)
3. Баранов О. А.Трансформація: соціальна & цифрова & правова: монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату. Одеса: Видавничий дім «Гельветика», 2022. 272 с. URL: https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova (дата звернення 20.05.2025 р.)
4. Довгань О., Тарасюк А., Ткачук Т. Кібербезпека «суспільства знань»: монографія/ Київ-Одеса: Фенікс, 2021. 176 с. URL: http://ippi.org.ua/kiberbezpeka-%C2%ABsuspilstva-znan%C2%BB (дата звернення 20.05.2025 р.)
5. Ланде Д. В., Фурашев В. М. Інформаційне та соціально-правове моделювання: посібник. Київ-Одеса : Фенікс, 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf (дата звернення 20.05.2025 р.)
6. 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 (дата звернення 20.05.2025 р.)
7. 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 (дата звернення 20.05.2025 р.)
8. 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-protidiinegativnim-informatsiinim-vplivam-ta-zakhistu-informatsiinoi-bezpeki-lyudini-i-sus (дата звернення 20.05.2025 р.)
9. Тихомиров О.О. Права людини: інформаційний вимір: монографія. Одеса: Видавництво «Юридика», 2023. 304 с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf (дата звернення 20.05.2025 р.)

Для пошуку іншої необхідної літератури та нормативно-правових актів необхідно використовувати офіційні інтернет-портали:

- Офіційний веб-сайт Верховної Ради України: http://portal.rada.gov.ua
- Офіційний веб-сайт Європейського Суду з прав людини: http://www.echr.coe.int/Pages/home.aspx?p=home
- Офіційний веб-сайт Уповноваженого Верховної Ради з прав людини: http://www.ombudsman.gov.ua/
- Єдиний веб-портал органів виконавчої влади України: Урядовий портал. URL: https://www.kmu.gov.ua/
- Офіційний веб-сайт Міністерства юстиції України: http://old.minjust.gov.ua/
- Офіційний веб-сайт Конституційного Суду України: http://www.ccu.gov.ua/
- Єдиний реєстр судових рішень: http://reyestr.court.gov.ua/
- Судова влада України: http://court.gov.ua

Інформаційні ресурси КПІ ім. Ігоря Сікорського:

1. Науково-технічна бібліотека ім. Г.І. Денисенка КПІ ім. Ігоря Сікорського https://www.library.kpi.ua/

2. Електронний архів наукових та освітніх матеріалів КПІ ім. Ігоря Сікорського https://www.ela.kpi.ua/

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Опанування навчальної дисципліни «Інформаційна безпека» відбувається на лекційних, практичних заняттях та під час 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 прикладної математики. 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 консультацій з викладачем, які проводяться взаємно погоджений час.

Навчання здійснюється на основі студентоцентрованого підходу та стратегії взаємодії викладача та студента для засвоєння студентами матеріалу та розвитку у них практичних навичок. Для проведення занять застосовується практичний метод. Для лекційних занять використовуються пояснювально-ілюстративний метод та метод проблемного виконання, для проведення практичних занять використовується частково-пошуковий та дослідницький методи навчання, при яких викладач ставить перед студентами проблему, і ті вирішують її самостійно або під керівництвом викладача, висуваючи ідеї, перевіряючи їх, підбираючи для цього необхідні джерела інформації, методи, підходи тощо.

Дистанційна форма навчання: Платформа дистанційного навчання на основі системи Google Classroom та платформа для проведення онлайн-зустрічей Zoom (присутність студента підтверджується увімкненою камерою, у випадку виникнення форс-мажорних обставин і неможливості працювати з нею, то повідомити про це викладача), електронна пошта, канали Telegram (в робочий час).

Модульна контрольна робота виконується онлайн, студентам надається посилання на гугл-форму. МКР передбачає виконання 56 тестових завдань.

Лекційні та практичні заняття

Тема кожного лекційного заняття розглядається на відповідному практичному занятті.

№ з/п	Назва теми лекції та перелік основних питань	Зміст заняття	Рекомендовані завдання	Рекомендації щодо засвоєння
1.	**Тема 1. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИ** 1. Концепція інформаційної безпеки України. 2. Інформаційна безпека: понятійний апарат	Підготувати конспект, проаналізувати Концепцію інформаційної безпеки України	Рекомендується опрацювати нормативні документи (Конституція, ЗУ "Про інформацію"),	Проаналізувати Концепцію інформаційної безпеки України, а також проєкт/презентацію на одне із питань

	3. Інтереси особи, суспільства та держави в інформаційній сфері 4. Об'єкти, суб'єкти інформаційної безпеки 5. Види інформаційної безпеки		переглянути аналітичні матеріали СБУ/РНБО	плану лекції. Підготувати структурну схему: «Суб'єкти та об'єкти інформаційної безпеки»
2.	**Тема 2. ІНТЕРНЕТ ТА ІНФОРМАЦІЙНА БЕЗПЕКА** 1. Правова природа Інтернет-правовідносин 2. Суб'єктний склад відносин у мережі Інтернет 3. Об'єкти Інтернет-правовідносин 4. Загрози при роботі в Інтернеті і способи їх уникнення	Підготувати повідомлення про практичні приклади кіберзагроз	Рекомендується самостійно дослідити кейси порушень безпеки в українському Інтернет-просторі	Підготувати повідомлення про практичні приклади кіберзагроз, а також проєкт/презентацію на одне із питань плану лекції. Скласти таблицю порівняння: «Ризики в Інтернеті – Засоби протидії»
3.	**Тема 3. КІБЕРНЕТИЧНА БЕЗПЕКА. ЗВ'ЯЗОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКИ** 1. Кібербезпека як складова міжнародної, регіональної та національної безпеки 2. Кіберсоціалізація особистості 3. Мережна мобілізація: питання демократії та безпеки 4. Сутність та характерні ознаки кіберцивілізації 5. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект	Порівняльна таблиця: кібербезпека vs інформаційна безпека	Рекомендується опрацювати Стратегію кібербезпеки України	Порівняльна таблиця: кібербезпека vs інформаційна безпека, а також проєкт/презентацію на одне із питань плану лекції. Підготувати міні-реферат на тему: «Кіберсоціалізація в умовах воєнного часу»
4.	**Тема 4. ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ЯК ОБ'ЄКТ НЕБЕЗПЕКИ (ЧАСТИНА ПЕРША)** 1. Інформаційна діяльність: сутність, складові та засоби здійснення. 2. Інформаційне виробництво. 3. Інформаційне забруднення. 4. Інформаційне середовище. 5. Інформаційні ресурси: поняття, функції, ієрархічні рівні.	Дослідити приклади впливу інформаційного забруднення	Використати приклади з медіа, порівняти ефективність комунікацій	Дослідити приклади впливу інформаційного забруднення, а також проєкт/презентацію на одне із питань плану лекції. Підготувати розбір фейку.
5.	**Тема 4. ІНФОРМАЦІЙНА ДІЯЛЬНІСТЬ ЯК ОБ'ЄКТ НЕБЕЗПЕКИ (ЧАСТИНА 2)** 1. Сутність поняття «інформаційний вплив» 2. Співвідношення понять «Інформаційна операція» та «інформаційна війна» 3. «Інформаційна зброя» як засіб ведення інформаційних війн 4. Маніпулювання свідомістю, сутність та види маніпуляції.	Аналіз маніпулятивних технологій у ЗМІ	Рекомендується обрати 1 приклад фейку та розібрати, як він створювався	Аналіз маніпулятивних технологій у ЗМІ, а також підготувати проєкт/презентацію на одне із питань плану лекції. Пошукове завдання: знайти приклади інформаційних маніпуляцій у ЗМІ (2–3

	5. Сутність та прояви інформаційного насильства. 6. Проблемні питання правового запобігання здійсненню інформаційного насильства.			приклади, аналіз)
6.	**Тема 5. Основні напрями реалізації прав і свобод людини в сфері інформації** 1. Право громадян на звернення щодо надання інформації. 2. Доступ до правової інформації. 3. Доступ до екологічної інформації. 4. Право на доступ до інформації для споживачів щодо харчових продуктів 5. Інформаційні права громадян як суб'єктів виборчого процесу. 6. Захист персональних даних. 7. Особливості реалізації права на доступ до інформації про стан довкілля, якість харчових продуктів та предметів побуту в умовах воєнного стану	Написати інформаційний запит до державного органу	Ознайомитись з кейсами щодо захисту персональних даних у судах	Написати інформаційний запит до державного органу, а також проєкт/презентацію на одне із питань плану лекції. Написати зразок інформаційного запиту до державного органу (за Законом «Про доступ до публічної інформації»)
7.	**Тема 6. ПОНЯТТЯ «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ». ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ОБІГУ ІНФОРМАЦІЇ** 1. Нормативно-правове забезпечення в сфері інформаційної безпеки. 2. Роль категорійно-понятійного апарату в системі нормативно-правового забезпечення. 3. Правові гарантії безпечного обороту інформації. 4. Законодавче обмеження доступу до інформаційних ресурсів	Таблиця нормативно-правових актів за темою	Рекомендується опрацювати ЗУ "Про інформацію", "Про доступ до публічної інформації"	Таблиця нормативно-правових актів за темою, а також проєкт/презентацію на одне із питань плану лекції. Створити короткий огляд (таблиця): основні нормативні акти у сфері ІБ
8.	**Тема 7. КІБЕРЗЛОЧИННІСТЬ ТА КІБЕРТЕРОРИЗМ** 1. Кіберзлочинність: поняття та сутність. Конвенція Ради Європи «Про кіберзлочинність» від 23.11.01 р. № 994-575 2. Поняття комп'ютерної злочинності. Загальна характеристика комп'ютерних злочинів. 3. Кібертероризм: поняття та сутність. 4. Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. 5. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки. 6. Цивільна відповідальність за	Підготувати презентацію про види кіберзлочинів	Рекомендується вивчити положення ККУ щодо комп'ютерних злочинів	Підготувати презентацію/презентацію про види кіберзлочинів Ознайомитись з Конвенцією про кіберзлочинність, скласти карту понять (майндмеп)

	правопорушення в системі забезпечення інформаційної безпеки. 7. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX			
9.	**Тема 8. СТРАТЕГІЧНІ ПІДХОДИ ПРАВОВОГО ВИРІШЕННЯ ПИТАНЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ** 1. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері. 2. Поняття та сутність інформаційного суверенітету. 3. Трансформація кіберзагроз в сучасних умовах. 4. Характеристика основних положень: • Стратегії національної безпеки України; • Стратегії інформаційної безпеки України • Стратегії кібербезпеки України; • Стратегії зовнішньополітичної діяльності України; Закону України «Про основні засади забезпечення кібербезпеки України».	Порівняти основні стратегії України у сфері безпеки	Рекомендуєтьс я скласти SWOT-аналіз Стратегії інформаційної безпеки	Порівняти основні стратегії України у сфері безпеки, а також проєкт/презентацію на одне із питань плану лекції. Порівняльна таблиця: «Стратегія кібербезпеки vs Стратегія національної безпеки»

6. Самостійна робота здобувача вищої освіти

Студент повинен завчасно готуватись до лекцій та практичних занять. Перед лекціями необхідно повторити теоретичний матеріал, наданий у попередніх лекціях. Перед практичними заняттями необхідно повторити відповідний теоретичний матеріал.

Самостійна робота студента (СРС) передбачає самостійне опрацювання матеріалу, віднесеного до самостійного розгляду на практичному занятті, з використанням лекційного матеріалу і рекомендованої літератури.

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 дистанційно 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.

Форми контролю самостійної роботи: перевірка письмових робіт (рефератів, таблиць, аналітичних звітів, запитів, проєктів); оцінювання презентацій; усні або письмові опитування; проведення тестів на платформі Google Forms; залікове заняття.

Самостійна робота студента

№ з/п	Вид самостійної роботи	Кількість годин СРС
2.	Підготовка до практичних занять	16
3.	Підготовка до МКР	2
4.	Підготовка до заліку	6
	Загалом	**24**

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Політика навчальної дисципліни спрямована на створення умов для якісного засвоєння знань, формування навичок професійної етики, відповідальності та академічної доброчесності.

Відповідно до Наказу 1-273 від 14.09.2020 р. заборонено оцінювати присутність або відсутність здобувача на аудиторному занятті. Матеріал занять, які були з тих чи інших причин пропущені, необхідно опановувати самостійно. У будь-якому випадку студентам рекомендується відвідувати усі види занять, оскільки на них викладається теоретичний матеріал та розвиваються навички, необхідні для виконання домашніх завдань, контрольних та розрахункових робіт. Система оцінювання орієнтована на отримання балів за активність студента, а також виконання завдань, що розвивають практичні уміння та навички.

Невиконані або несвоєчасно здані без поважних причин роботи не приймаються. Кожне завдання буде мати чітко встановлений термін виконання (відповідно до графіку навчального процесу). Здобувач зобов'язаний: дотримуватись принципів самостійності виконання робіт; уникати плагіату (використання чужих текстів без посилання); не використовувати заборонені засоби під час тестування або захисту. Виявлений факт порушення академічної доброчесності призводить до анулювання оцінки за роботу. Участь у позааудиторних заходах (конференціях, вебінарах, семінарах, лекціях з теми ІБ) вітається і може бути врахована при підсумковій оцінці (в якості заохочувальних балів). Викладач залишає за собою право змінювати окремі положення політики з попереднім повідомленням групи.

Правила поведінки на заняттях: здобувач вищої освіти має можливість отримувати бали за відповідні види навчальної активності на семінарських 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.

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.

Процедура оскарження результатів контрольних заходів

Студенти мають можливість підняти будь-яке питання, яке стосується процедури проведення та/або оцінювання контрольних заходів, та очікувати, що воно буде розглянуто згідно із наперед визначеними процедурами. Студенти мають право оскаржити результати контрольних заходів, але обов'язково аргументовано, пояснивши, з яким критерієм не погоджуються відповідно до оціночного листа та/або зауважень.

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.

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

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 поточного контролю (від дати проведення практичного заняття) 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-й тиждень	14-й тиждень
Умови позитивного отримання	≥ 15 балів	≥ 35 бал

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

Поточний контроль: експрес-опитування, опитування за темою заняття, МКР, захист проєктів, презентацій, виконання завдань (вирішення задач) на практичних заняттях; тести; активна участь в обговореннях тощо

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 практичного заняття; надання повної і аргументованої, логічно викладеної доповіді, відповіді, висловлення власної позиції з дискусійних питань або повністю правильне вирішення задачі з відповідним обґрунтуванням, коректне вирішення тестових та практичних завдань, у поєднанні зі значними доповненнями відповідей інших студентів у процесі дискусії	8

активна участь у проведенні заняття; надання правильних відповідей або правильне вирішення задач, коректне вирішення тестових та практичних завдань, з незначними неточностями	7
надання відповідей або вирішення задач, тестових та практичних завдань, з похибками	6
надання відповідей з чисельними значними похибками	5
суттєве доповнення відповідей студентів (активна участь в практичному занятті)	5
Підготовка проєкту/презентації	3

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

Написання МКР передбачає виконання 56 тестових завдань на платформі Google Forms, максимальна кількість балів – 28.

Перелік тестових завдань, 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 останнього лекційного 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.

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.

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

Семестровий контроль: залік

На заліку здобувач одержує білет з питаннями, відповіді на які оцінюються по 40-бальній шкалі за такими критеріями:

- *повна відповідь (не менше 90% потрібної інформації), 35 - 40 балів;*
- *достатньо повна відповідь (не менше 75% потрібної інформації), 30 -34 балів;*
- *неповна відповідь (не менше 60% потрібної інформації), 20 – 29 балів;*
- *незадовільна відповідь – до 20 балів.*

Умови допуску до семестрового контролю: мінімально позитивна оцінка із врахуванням всіх видів робіт – більше 30 балів.

Загальна рейтингова оцінка студента після завершення семестру складається з балів, отриманих за:

Система оцінювання

№	Контрольний захід оцінювання	%	Ваговий бал	Кількість	Всього
1	Оцінювання знань студентів під час проведення семінарського заняття	72	8	9	72
2	Оцінювання результатів письмового тестування ступеня засвоєння навчального матеріалу під час проведення МКР	28	28	1	28
	Всього				100

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

Зі здобувачами, які мають рейтингову оцінку менше 60 балів, а також з тими здобувачами, хто бажає підвищити свою рейтингову оцінку в семестрі, викладач проводить семестровий контроль у вигляді додаткової контрольної роботи або співбесіди. Попередній рейтинг здобувача скасовується, додаткова контрольна оцінюється в 100 балів.

9. Додаткова інформація з дисципліни (освітнього компонента)

Рекомендації студентам

Готуючись до семінарського (практичного) заняття студент має обов'язково опрацювати лекційний матеріал певної теми, бажано ознайомитись з додатковими ресурсами в мережі. При виникненні питань, виявленні незрозумілих положень, необхідно обов'язково обговорити їх з викладачем.

Якщо **лекційне заняття** припадає на святковий (неробочий) день, матеріал виноситься на самостійне опрацювання (викладач розміщує конспект лекції на платформі «Сікорський» чи Telegram групи).

Якщо **семінарське (практичне) заняття** припадає на святковий (неробочий) день, студентам необхідно виконати завдання відповідно до теми заняття до визначеної викладачем дати. Завдання розміщується на платформі «Сікорський» або в Telegram групи.

Увага! У разі, якщо навчальний процес відбувається дистанційно (online) у період дії воєнного стану і:

1) лекційне заняття за розкладом не відбулось або перервалось (повітряна тривога, раптова відсутність електрики у викладача, …) – конспект лекції з відповідної теми розміщується

викладачем в Telegram групи для самостійного опрацювання студентами;
2) практичне заняття за розкладом не відбулось або перервалось (повітряна тривога, раптова відсутність електрики у викладача, …) – **виконане завдання* до теми заняття** всі студенти групи завантажують в Classroom на перевірку;
3) студент був відсутнім на практичному занятті (хвороба, повітряна тривога, відсутність електрики, …) – виконане завдання до теми заняття завантажується в Classroom на перевірку.

***Під «виконаним завданням» мається на увазі** підготувати стислі відповіді на всі теоретичні питання + розв'язати всі ситуаційні вправи (задачі/кейси/тести) до теми заняття.

Позааудиторні заняття

Передбачається в межах вивчення навчальної дисципліни участь в конференціях.

Для отримання додаткових балів студенти можуть пройти дистанційні або онлайн курси на таких платформах (максимум – три курси, кожен курс оцінюється в 3 бали):

- Дезінформація: види, інструменти та способи захисту https://courses.prometheus.org.ua/courses/course-1:Prometheus+DISINFO101+2021_T2/about.
- Інформаційна гігієна. Як розпізнати брехню в соцмережах, в інтернеті та на телебаченні https://courses.prometheus.org.ua/courses/course-v1:Prometheus+IH101+2021_T3/about,
- Медіаграмотність: як не піддаватися маніпуляціям? https://courses.prometheus.org.ua/courses/course-v1:Prometheus+MEDIA_L101+2022_T3/about,
- Освітній серіал «Персональні дані» https://osvita.diia.gov.ua/courses/personaldata,
- Захист персональних даних https://study.ed-era.com/uk/courses/course/371,
- Захист персональних даних (спеціалізований курс) https://study.ed-era.com/uk/courses/course/372

Орієнтовні питання до заліку

1. Концепція інформаційної безпеки України.
2. Інформаційна безпека: понятійний апарат
3. Інтереси особи, суспільства та держави в інформаційній сфері
4. Об'єкти, суб'єкти інформаційної безпеки
5. Види інформаційної безпеки
6. Правова природа Інтернет-правовідносин
7. Суб'єктний склад відносин у мережі Інтернет
8. Об'єкти Інтернет-правовідносин
9. Загрози при роботі в Інтернеті і способи їх уникнення
10. Кібербезпека як складова міжнародної, регіональної та національної безпеки
11. Кіберсоціалізація особистості
12. Мережна мобілізація: питання демократії та безпеки
13. Сутність та характерні ознаки кіберцивілізації
14. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект
15. Інформаційна діяльність: сутність, складові та засоби здійснення.
16. Інформаційне виробництво.
17. Інформаційне забруднення.
18. Інформаційне середовище.
19. Інформаційні ресурси: поняття, функції, ієрархічні рівні.
20. Сутність поняття «інформаційний вплив»
21. Співвідношення понять «Інформаційна операція» та «інформаційна війна»

22. «Інформаційна зброя» як засіб ведення інформаційних війн
23. Маніпулювання свідомістю, сутність та види маніпуляції.
24. Сутність та прояви інформаційного насильства.
25. Проблемні питання правового запобігання здійсненню інформаційного насильства.
26. Право громадян на звернення щодо надання інформації.
27. Доступ до правової інформації.
28. Доступ до екологічної інформації.
29. Право на доступ до інформації для споживачів щодо харчових продуктів
30. Інформаційні права громадян як суб'єктів виборчого процесу.
31. Захист персональних даних.
32. Особливості реалізації права на доступ до інформації про стан довкілля, якість харчових продуктів та предметів побуту в умовах воєнного стану
33. Нормативно-правове забезпечення в сфері інформаційної безпеки.
34. Роль категорійно-понятійного апарату в системі нормативно-правового забезпечення.
35. Правові гарантії безпечного обороту інформації.
36. Законодавче обмеження доступу до інформаційних ресурсів
37. Кіберзлочинність: поняття та сутність. Конвенція Ради Європи «Про кіберзлочинність» від 23.11.01 р. № 994-575
38. Поняття комп'ютерної злочинності. Загальна характеристика комп'ютерних злочинів.
39. Кібертероризм: поняття та сутність.
40. Адміністративна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
41. Кримінальна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
42. Цивільна відповідальність за правопорушення в системі забезпечення інформаційної безпеки.
43. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX
44. Життєво важливі інтереси людини та суспільства в інформаційної сфері. Національні інтереси в інформаційної сфері.
45. Поняття та сутність інформаційного суверенітету.
46. Трансформація кіберзагроз в сучасних умовах.
47. Характеристика основних положень Стратегії національної безпеки України
48. Характеристика основних положень Стратегії інформаційної безпеки України
49. Характеристика основних положень Стратегії кібербезпеки України;
50. Характеристика основних положень Стратегії зовнішньополітичної діяльності України; Характеристика основних положень Закону України «Про основні засади забезпечення кібербезпеки України».

Робочу програму навчальної дисципліни (силабус):

Складено Доцент кафедри інформаційного, господарського та адміністративного права, к.ю.н. Рудник Людмила Іванівна

Ухвалено кафедрою інформаційного та господарського права (протокол № 13 від 29.05.2026)

Погоджено Методичною комісією факультету (протокол № ___ від _____)