

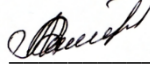
ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ

Навчально-науковий інститут денної освіти

Кафедра комп'ютерних наук та інформаційних технологій

ЗАТВЕРДЖУЮ

Завідувач (начальник) кафедри



доц. Олена ОЛЬХОВСЬКА

« 28 » _____ 06 _____ 2024 р.

РОБОЧА ПРОГРАМА

навчальної дисципліни:	«Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки»
освітньо-професійна програма:	Комп'ютерні науки
спеціальність:	122 Комп'ютерні науки
галузь знань:	12 Інформаційні технології
ступінь вищої освіти:	бакалавр


Робоча програма навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки» схвалена та рекомендована до використання в освітньому процесі на засіданні кафедри комп'ютерних наук та інформаційних технологій
Протокол від «28» червня 2024 року № 13

ПОЛТАВА – 2024

Укладач: Кульчій Олег Олександрович, доцент закладу вищої освіти кафедри комп'ютерних наук та інформаційних технологій Полтавського університету економіки і торгівлі, к. ю. н., доцент.

ПОГОДЖЕНО:

Гарант освітньо-професійної програми «Комп'ютерні науки» спеціальності 122 Комп'ютерні науки ступеня бакалавр


_____ Оксана ЧЕРНЕНКО
« 28 » _____ 06 _____ 2024 року

ЗМІСТ

Розділ 1. Опис навчальної дисципліни	4
Розділ 2. Перелік компетентностей та програмні результати навчання з навчальної дисципліни.....	5
Розділ 3. Програма навчальної дисципліни	7
Розділ 4. Тематичний план навчальної дисципліни	15
Розділ 5. Система поточного та підсумкового контролю знань студентів.....	38
Розділ 6. Інформаційні джерела	40
Розділ 7. Програмне забезпечення навчальної дисципліни.....	48

Розділ 1. Опис навчальної дисципліни

Таблиця 1. Опис навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки»

Місце в структурно-логічній схемі підготовки	<i>Пререквізити:</i> висхідна <i>Постреквізити:</i> Програмування II, Виробнича практика 3 курс.
Мова викладання	Українська мова
Статус дисципліни – обов’язкова	
Курс/семестр вивчення	1 курс, 1 семестр
Кількість кредитів ЄКТС/ кількість модулів	Кількість кредитів за ЄКТС – 3 / 2 модулі
Денна форма навчання:	
Кількість годин:	
– загальна кількість: 2 семестр – 90	
– лекції: 1 семестр – 16	
– семінарські заняття: 2 семестр – 20	
– самостійна робота: 2 семестр – 54	
– вид підсумкового контролю: 2 семестр – екзамен	
Заочна форма навчання:	
Кількість годин:	
– загальна кількість: 2 семестр – 90	
– лекції: 1 семестр – 4	
– семінарські заняття: 2 семестр – 2	
– самостійна робота: 2 семестр – 84	
– вид підсумкового контролю: 2 семестр – екзамен	

Розділ 2. Перелік компетентностей, які забезпечує дана навчальна дисципліна, програмні результати навчання

Метою вивчення навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки» є засвоєння здобувачами вищої освіти системних знань із правового регулювання у сфері професійної діяльності за фахом, що передбачає ознайомлення із ключовими темами та питаннями різних галузей права, об'єднаними довкола спільного предмета регулювання – відносин, що складаються у ході здійснення професійної діяльності в сфері інформаційних технологій (як самостійної підприємницької, так і у якості найманого працівника) та інформаційної безпеки.

Основними завданнями навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки» є ознайомлення зі змістом нормативно-правових актів, що регламентують різні аспекти професійної діяльності у сфері інформаційних технологій та інформаційної безпеки, формування готовності самостійно орієнтуватися у приписах таких нормативно-правових актів з метою пошуку відповідей на питання юридичного характеру, що можуть виникати у ході професійної діяльності та розуміння ситуації, коли буде необхідним використання професійної правничої допомоги.

Таблиця 2. Перелік компетентностей, які забезпечує дана навчальна дисципліна, програмні результати навчання

Компетентності, якими повинен оволодіти здобувач	Програмні результати навчання
<p>Загальні компетентності</p> <p>Здатність до абстрактного мислення, аналізу та синтезу (ЗК 1)</p> <p>Здатність застосовувати знання у практичних ситуаціях (ЗК 2)</p> <p>Здатність вчитися й оволодівати сучасними знаннями (ЗК 6).</p> <p>Здатність до пошуку, оброблення та аналізу інформації з різних джерел (ЗК 7).</p> <p>Здатність бути критичним і самокритичним (ЗК 10).</p> <p>Здатність приймати обґрунтовані рішення (ЗК 11).</p> <p>Здатність оцінювати та забезпечувати якість виконуваних робіт (ЗК 12).</p> <p>Здатність діяти на основі етичних міркувань (ЗК 13).</p> <p>Здатність реалізувати свої права і</p>	<p>Володіти навичками управління життєвим циклом програмного забезпечення, продуктів і сервісів інформаційних технологій відповідно до вимог і обмежень замовника, вміти розробляти проектну документацію (техніко-економічне обґрунтування, технічне завдання, бізнес-план, угоду, договір, контракт) (ПР 11).</p> <p>Володіти та застосовувати поглиблені правові знання, розвиток практичних умінь і навичок щодо питань нормативно-правового регулювання цифрової та інформаційної безпеки особи, суспільства, держави (ПР 18).</p>

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 (ЗК 14). Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя (ЗК 15). Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь-яких інших проявів не доброчесності (ЗК16)

Спеціальні компетентності

Здатність до логічного мислення, побудови логічних висновків, використання формальних мов і моделей алгоритмічних обчислень, проектування, розроблення й аналізу алгоритмів, оцінювання їх ефективності та складності, розв'язності та нерозв'язності алгоритмічних проблем для адекватного моделювання предметних областей і створення програмних та інформаційних систем (СК 3).

Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури (СК 14).

Здатність застосовувати поглиблені правові знання, розвиток практичних умінь і навичок щодо питань нормативно-правового регулювання цифрової та інформаційної безпеки особи, суспільства, держави (СК 18).

Розділ 3. Програма навчальної дисципліни

Програма навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки» укладена відповідно до освітньо-професійної програми Комп'ютерні науки підготовки здобувачів першого (бакалаврського) рівня вищої освіти спеціальності 122 «Комп'ютерні науки», розробленої на підставі стандарту вищої освіти зі спеціальності 122 «Комп'ютерні науки» галузі знань 12 Інформаційні технології для першого (бакалаврського) рівня вищої освіти, затвердженого та введеного в дію наказом Міністерства освіти і науки України від 10 липня 2019 року № 962, затвердженої Вченою радою ВНЗ Укоопспілки «Полтавський університет економіки і торгівлі» 25 травня 2022 р. (протокол № 5, наказ № 87-н).

Програму навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки» обговорено і схвалено на засіданні кафедри комп'ютерних наук та інформаційних технологій. Протокол засідання кафедри від 28 червня 2024 р., № 13.

Програмний зміст навчальної дисципліни

Модуль 1.

Правове регулювання інформаційних відносин та професійної діяльності в сфері інформаційних технологій

Тема 1. Загальна характеристика правового регулювання інформаційних відносин.

Поняття права. Значення права як регулятора суспільних відносин. Правовідносини та їх структура.

Аналіз правових відносин, що можуть виникати у ході здійснення професійної діяльності у сфері інформаційних технологій. Загальний огляд основних галузей права, з допомогою яких врегульовуються визначені відносини: Інформаційне, цивільне, господарське, трудове, міжнародне приватне, адміністративне, кримінальне право тощо.

Поняття, зміст та сутність інформаційного права, його предмет, метод та система, підходи до розуміння. Суспільні відносини, які регулюються інформаційним правом. Принципи інформаційного права. Суб'єкти інформаційних правовідносин та їх види. Зміст інформаційних правовідносин.

Інформаційні права і свободи у контексті прав людини. Право на пошук, отримання, поширення інформації та інші права, закріплені за фізичними та юридичними особами чинним законодавством. Межі інформаційних прав людини в Україні. Право на приватність.

Поняття інформаційного суспільства та державна політика у сфері розвитку інформаційного суспільства в Україні.

Класифікація та загальний огляд джерел інформаційного права та інших галузей права, дотичних до регулювання професійної діяльності у сфері інформаційних технологій.

Тема 2. Поняття інформації та інших об'єктів інформаційних відносин. Правові режими інформаційних ресурсів. Публічна інформація.

Поняття та сутність об'єктів інформаційних правовідносин, їх види. Інформація як основний об'єкт інформаційних правовідносин. Юридичні особливості інформації. Інформація як вид власності. Підстави виникнення права власності на інформацію.

Співвідношення категорій «інформація», «відомості», «дані», «знання», «таємниця» та інших у суспільних правовідносинах. Особливості їх застосування у нормативних актах. Види інформації за галузями застосування, її зміст. Поняття категорії «документ» в інформаційних відносинах.

Інформаційні системи. Поняття та сутність інформаційних ресурсів. Державна інформаційна політика як об'єкт правовідносин. Інформаційна культура як об'єкт правовідносин. Інформаційна безпека як об'єкт правовідносин.

Класифікація об'єктів інформаційних правовідносин за сферами законодавчого регулювання. Честь, гідність та ділова репутація як об'єкти інформаційного права. Засоби масової інформації як об'єкт інформаційних правовідносин. Архівна, бібліотечна та видавнича діяльність як об'єкти інформаційних правовідносин. Реклама, піар, недобросовісна конкуренція, інформаційна боротьба як об'єкти інформаційних правовідносин.

Технічні засоби та технології як об'єкти в інформаційних відносинах. Бази даних як об'єкти інформаційних відносин. Інформатизація як об'єкт інформаційних правовідносин.

Класифікація інформації за правовим режимом доступу. Відкрита інформація. Державна таємниця та правове регулювання відносин щодо секретної інформації. Службова інформація. Професійна таємниця та її види. Комерційна таємниця. Конфіденційна інформація.

Поняття публічної інформації. Відкриті дані. Розпорядники публічної інформації. Міжнародно-правові гарантії реалізації права на доступ до інформації. Національне законодавство, що регулює порядок доступу до інформації. Інформаційний запит та звернення громадян. Порядок надання інформації за запитом, усними та письмовими зверненнями громадян. Плата за послуги з надання інформації. Правові підстави відмови громадянам у доступі до інформації. Оскарження рішень, дій чи бездіяльності щодо порушення права громадян на доступ до інформації.

Тема 3. Право інтелектуальної власності на об'єкти інформаційних відносин.

Поняття права інтелектуальної власності як підгалузі цивільного права України. Основні джерела права інтелектуальної власності.

Право інтелектуальної власності (суб'єктивне). Об'єкти, суб'єкти та зміст права інтелектуальної власності.

Регулювання інформаційних відносин інститутом авторського права. Правове регулювання інформаційних відносин щодо виробництва і поширення комп'ютерних програм і баз даних. Код комп'ютерної програми як об'єкт авторського права.

Комп'ютерні програми та інші результати професійної діяльності у сфері інформаційних технологій як об'єкти права інтелектуальної власності. Ліцензії на використання програмного забезпечення та їх види.

Право промислової власності. Особливості регулювання інформаційних відносин інститутом патентного права (винаходи, корисні моделі, промислові зразки). Перспективи правової охорони комп'ютерних програм засобами патентного права.

Засоби індивідуалізації: знаки для товарів і послуг, комерційні (фірмові) найменування, географічні зазначення. Доменні імена.

Інформація як об'єкт майнового права. Особливості інформаційних правовідносин, які виникають при виробництві, передачі та споживанні інформації, що становить комерційну таємницю. Правовий режим комерційної таємниці. Охорона комерційної таємниці у трудових відносинах. Поняття угоди про нерозголошення комерційної таємниці (NDA).

Поняття та ознаки науково-технічної інформації. Право на науково-технічну інформацію. Проблеми захисту науково-технічної інформації. Особливості регулювання інформаційних відносин інститутом ноу-хау.

Об'єкти права інтелектуальної власності у віртуальному просторі (мета-всесвіті).

Тема 4. Організаційно-правові засади здійснення професійної діяльності у сфері інформаційних технологій.

Правові форми здійснення професійної діяльності у сфері інформаційних технологій: трудовий договір, цивільно-правовий договір, самостійна підприємницька діяльність та інші. Особливості трудових договорів зі спеціалістами з інформаційних технологій, порядок їх укладення та припинення, права та обов'язки їх сторін. Відмінності трудових договорів, цивільно-правових договорів та господарських договорів із фізичною особою-підприємцем.

Поняття та правовий режим резидентів Дія Сіті. Особливості гіг-контрактів з гіг-спеціалістами: сфера використання, правове регулювання, переваги та недоліки.

Організаційно-правові форми здійснення самостійної підприємницької діяльності у сфері інформаційних технологій: загальна характе-

ристика. Фізична особа-підприємець (ФО-П) та товариство з обмеженою відповідальністю (ТОВ) як найбільш зручні та популярні організаційно-правові форми здійснення малої підприємницької діяльності в Україні. Акціонерне товариство. Вибір організаційно-правових форм для стартапів.

Започаткування підприємницької діяльності у сфері інформаційних технологій. Законодавство, що врегульовує підприємницьку діяльність у сфері інформаційних технологій.

Порядок державної реєстрації підприємницької діяльності. Установчі документи. Особливості реєстрації ТОВ на підставі модельного статуту. Порядок внесення майнових інтелектуальної власності до статутного капіталу суб'єктів господарювання.

Зупинення та припинення підприємницької діяльності. Державна реєстрація припинення підприємницької діяльності.

Тема 5. Договірні відносини у сфері інформаційних відносин.

Застосування зобов'язального та договірної права в регулюванні інформаційних відносин та професійної діяльності у сфері інформаційних технологій.

Поняття та загальна характеристика цивільних зобов'язань. Особливості господарських зобов'язань та їх види. Суб'єкти, об'єкти та зміст зобов'язання. Заміна сторін у зобов'язанні. Припинення зобов'язання.

Підстави виникнення зобов'язання. Поняття договору. Зміст та форма договору, його істотні умови. Порядок укладення, зміни та припинення договору.

Види договорів. Договори, що можуть застосовуватися для врегулювання інформаційних відносин та професійної діяльності у сфері інформаційних технологій.

Договір купівлі-продажу та його види. Особливості договору купівлі-продажу майнових прав (корпоративних, майнових прав інтелектуальної власності тощо). Договори про відчуження виключних майнових прав інтелектуальної власності.

Договори про передачу майна в користування. Договір лізингу.

Договори про виконання робіт та характеристика їх видів. Договори про створення за замовленням і використання об'єктів права інтелектуальної власності. Договори на виконання науково-дослідних, дослідно-конструкторських і технологічних робіт.

Договори про надання послуг. Юридичні та фактичні послуги. Фінансові послуги. Страхування.

Договори, спрямовані на створення продуктів у сфері ІТ, їх правова природа та зміст, супровідна документація (технічне завдання та ін.). SAAS договори. Угоди про нерозголошення комерційної таємниці (NDA) та проблеми їх застосування в Україні. Угоди про неконкуренцію (NCA), та оцінка їх законності відповідно до права України.

Договори у сфері інтелектуальної власності. Передача прав на використання об'єктів інтелектуальної власності. Ліцензія на викорис-

тання об'єкта інтелектуальної власності. Види ліцензій. Ліцензійні договори. Договір комерційної концесії.

Поняття смарт-контрактів та їх можлива сфера використання.

Модуль 2.

Правове регулювання відносин інформаційної безпеки

Тема 6. Поняття та об'єкти інформаційної безпеки. Законодавство України щодо забезпечення інформаційної безпеки.

Поняття національних інтересів та національної безпеки. Поняття та правові засади інформаційної безпеки України.

Конституційне визначення способів захисту в інформаційних правовідносинах. Визначення компетенції державних органів влади щодо регулювання та захисту інформаційних відносин в Україні. Інституційний механізм інформаційної безпеки. Органи державної влади, до функціональних повноважень яких входять питання забезпечення інформаційної безпеки (у т.ч. кібербезпеки, захисту інформації).

Правові засади захисту об'єктів інформаційних правовідносин від загроз в інформаційній сфері. Інформаційна безпека людини й суспільства. Правові засади охорони комерційної, банківської таємниці та персональних даних в Україні. Правовий захист інформації, інформаційних ресурсів та інформаційних систем від загроз несанкціонованого та неправомірного впливу сторонніх осіб. Забезпечення інформаційної безпеки в мережі Інтернет.

Напрями державної політики у сфері інформаційної безпеки. Поняття та напрями державної інформаційної безпеки. Види загроз національній безпеці в інформаційній сфері. Принципи правового регулювання напрямів інформаційної безпеки. Державно-правовий механізм інформаційної безпеки в Україні.

Тема 7. Зарубіжний досвід правового регулювання інформаційної безпеки. Міжнародні акти в сфері інформаційної безпеки.

Досвід державного регулювання забезпечення різних аспектів інформаційної безпеки у розвинених зарубіжних державах.

Правові аспекти захисту інформації та принципи інформаційної безпеки у Європейському Союзі та окремих країнах ЄС (Німеччина, Франція, Італія, держави Східної Європи). Правові аспекти захисту інформації та принципи інформаційної безпеки у Сполучених Штатах Америки, Канаді, Великобританії. Кращі практики США і держав Європейського Союзу.

Директива 95/46 ЄС Європейського парламенту та Ради Європейського Союзу «Про захист прав приватних осіб стосовно обробки персональних даних». GDPR.

Міжнародно-правові основи інформаційної безпеки. Міжнародні конвенції та угоди в сфері інформаційної безпеки та кібербезпеки. Глобальна коаліція з цифрової безпеки. Види загроз безпеці суб'єктів

інформаційних правовідносин. Питання попередження інформаційної війни та інформаційного тероризму в документах ООН.

Тема 8. Забезпечення інформаційної безпеки особи, держави та суспільства.

Види інформаційної безпеки за критерієм об'єкта. Загрози інформаційній безпеці. Види загроз безпеці суб'єктів інформаційних правовідносин в інформаційній сфері та їх класифікація.

Інформаційна безпека особи. Задоволення інформаційних потреб учасників інформаційних правовідносин як спосіб забезпечення інформаційної безпеки. Забезпечення інформаційної безпеки суб'єктів підприємницької діяльності.

Інформаційна безпека держави. Забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів і підтримуючої інфраструктури в органах державної влади та місцевого самоврядування.

Інформаційна безпека суспільства. Особливості поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України.

Зовнішні деструктивні інформаційні впливи на суспільну свідомість (мережа Інтернет, засоби масової інформації). Поняття та форми інформаційного протиборства. Деструктивні інформаційні впливи. Інформаційний тероризм, інформаційна війна.

Тема 9. Організаційно-правові засади захисту інформації. Захист персональних даних.

Інформація як об'єкт інформаційної безпеки. Диференціація завдань щодо захисту інформації залежно від правового режиму інформації.

Особливості організації захисту інформації в автоматизованих (комп'ютерних) системах. Правові аспекти захисту інформації в автоматизованих системах. Технічний захист інформації. Криптографічний захист інформації. Національна система конфіденційного зв'язку. Державна служба спеціального зв'язку та захисту інформації України.

Організація системи запобігання інформаційним загрозам за допомогою організаційно-правових заходів: основні документи.

Законодавство України у сфері захисту персональних даних, його порівняння із GDPR.

Поняття персональних даних та їх ознаки. Критерії належності даних до персональних за законодавством України та GDPR. Класифікації персональних даних. Співвідношення персональних даних та конфіденційної інформації. Особливості правового режиму публічних персональних даних.

Приватність, захист даних та інформаційна безпека – співвідношення понять. Відмінність кібербезпеки від інформаційної безпеки. Вплив розвитку ІТ на захист персональних даних.

Поняття обробки (опрацювання) персональних даних. Характеристика операцій з персональними даними, що вважаються обробкою персональних даних. Загальні вимоги до обробки персональних даних відповідно до законодавства України. Принципи обробки персональних даних відповідно до GDPR. Підстави для обробки персональних даних. Збирання персональних даних: поняття, підстави, порядок здійснення та принципи. Накопичення та зберігання персональних даних. Зміни і доповнення до персональних даних, їх видалення та знищення. Поширення персональних даних. Доступ до власних персональних даних та персональних даних третіх осіб.

Загальна характеристика учасників відносин у сфері обробки персональних даних відповідно до законодавства України та відповідно до GDPR. Поняття суб'єкта персональних даних. Права та обов'язки суб'єктів персональних даних. Поняття володільця персональних даних (контролера). Спільні контролери персональних даних відповідно до ст. 26 GDPR. Поняття розпорядника персональних даних (оператор).

Правове становище Уповноваженого Верховної Ради України з прав людини. DPO.

Вимоги до обробки персональних даних, яких слід дотримуватись під час здійснення професійної діяльності у сфері ІТ. Проектування приватності (Privacy by design). Кодекс поведінки щодо обробки персональних даних: його зміст, порядок розробки та затвердження. Privacy policy. Згода суб'єкта на обробку персональних даних відповідно до законодавства України та GDPR. Інформування суб'єкта про обробку його персональних даних (Privacy Notice).

Міжнародна та національна сертифікація з захисту даних.

Тема 10. Правове регулювання електронних комунікацій та забезпечення кібербезпеки.

Законодавство, спрямоване на регулювання суспільних відносин у сфері електронних комунікацій, щодо надання та отримання електронних комунікаційних послуг, постачання та доступу до електронних комунікаційних мереж.

Правові заходи та методи захисту систем електронних комунікацій. Технічні засоби кіберзахисту.

Національна система кібербезпеки в Україні. Кібербезпека в сучасному глобалізаційному світі. Кіберінциденти та їх категорії. Кібератаки та кіберзлочини на національні електронні інформаційні ресурси, об'єкти критичної інформаційної інфраструктури. Ідентифікації та реагування на кібератаки, захист від негативних інформаційних впливів: матеріали судової практики.

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA.

Державні стандарти та нормативні документи, що стосуються технічного захисту інформації. Стандарти кібербезпеки.

Тема 11. Захист прав учасників інформаційних відносин, юридична відповідальність у сфері інформаційної безпеки та запобігання корупції в ІТ-галузі.

Відповідальність за порушення законодавства у сфері інформаційної безпеки: об'єкти та суб'єкти, підстави (юридичні та фактичні) та умови застосування, склад правопорушень.

Порушення законодавства у сфері інформаційної безпеки, кібербезпеки.

Data incident, data breach – належне реагування та принципи застосування відповідальності відповідно до GDPR та законодавства України.

Цивільно-правова відповідальність та господарсько-правова відповідальність за правопорушення в інформаційній сфері. Відшкодування шкоди, завданої порушенням інформаційної безпеки.

Дисциплінарна та матеріальна відповідальність за правопорушення в інформаційній сфері.

Адміністративно-правова відповідальність за правопорушення в інформаційній сфері.

Кримінальна відповідальність за правопорушення в сфері інформаційної безпеки.

Особливості інформаційних правопорушень у кіберпросторі. Загальна характеристика кіберзлочинів та відповідальність за них.

Нагляд і контроль за дотриманням законодавства під час здійснення професійної діяльності у сфері інформаційних технологій та з приводу дотримання вимог щодо забезпечення інформаційної безпеки.

Порядок притягнення до відповідальності за порушення законодавства у сфері інформаційної безпеки.

Форми та способи захисту прав та законних інтересів учасників інформаційних правовідносин.

Міжнародні конвенції, законодавство України та інші документи, які врегульовують відносини щодо запобігання та протидії корупції.

Види корупційних правопорушень та їх можливі прояви у сфері ІТ (корупційні ризики).

Внутрішні політики компаній щодо запобігання корупційним проявам. Етичні принципи діяльності ІТ-фахівців (етичні кодекси ІТ-компаній) та їх зв'язок з протидією корупції. Етичні дилеми, пов'язані з корупцією в ІТ-сфері. Антикорупційний комплаєнс та його роль у запобіганні корупційним проявам.

Заходи, спрямовані на запобігання та протидію корупції. Механізм анонімного повідомлення про корупцію (whistleblowing). Етичні дилеми, пов'язані з корупцією в ІТ-сфері (аналіз змодельованих ситуацій).

Відповідальність за порушення законодавства у сфері протидії корупції та інших актів, спрямованих на запобігання корупційним проявам та недоброчесності.

Розділ 4. Тематичний план навчальної дисципліни

Таблиця 4.1. Тематичний план навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки» для студентів спеціальності 122 «Комп'ютерні науки» ОПП «Комп'ютерні науки» денної форми навчання

Назва теми (лекції) та питання теми (лекції)	Кількість годин	Назва теми та питання практичного заняття	Кількість годин	Завдання самостійної роботи у розрізі теми	Кількість годин
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>
Модуль 1.					
Правове регулювання інформаційних відносин та професійної діяльності в сфері інформаційних технологій					
Тема 1. Загальна характеристика правового регулювання інформаційних відносин					
<i>Лекція 1:</i> 1) Право, правове регулювання суспільних відносин. Правовідносини та їх структура; 2) Правовідносини, що можуть виникати у ході здійснення професійної діяльності у сфері інформаційних технологій та галузі права, що їх врегульовують; 3) Загальна характеристика інформаційного права; 4) Джерела інфор-	2	–	–	<i>Питання для самостійного опрацювання:</i> 1) Поняття інформаційного суспільства та державна політика у сфері розвитку інформаційного суспільства в Україні; 2) Інформаційні права і свободи у контексті прав людини та їх обмеження; 3) Суб'єкти інформаційних правовідносин та їх види. Зміст інформаційних правовідносин; 4) Класифікація та загальний огляд джерел інформаційного права та інших галузей права,	4

1	2	3	4	5	6
маційного права та суміжних галузей права.				<p>дотичних до регулювання професійної діяльності у сфері інформаційних технологій.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми.</p> <p>2) Скласти таблицю нормативних актів, що врегульовують відносини у сфері ІТ із колонками: назва н.-п.а., .</p> <p>3) Скласти</p>	
Тема 2. Поняття інформації. Правові режими інформаційних ресурсів. Публічна інформація.					
<p><i>Лекція 2:</i> 1) Поняття об'єктів інформаційних правовідносин, їх види; 2) Інформація як об'єкт правовідносин та її властивості; 3) Класифікація інформації за правовим режимом доступу.</p>	2	<p><i>Семінарське заняття 1:</i></p> <p>1) Поняття об'єктів інформаційних правовідносин, їх види; 2) Інформаційні системи. Поняття та сутність інформаційних ресурсів; 3) Правове регулювання доступу до публічної інформації. Відкриті дані; 4) Правовий режим інформації з обмеженим доступом: державна таємниця, службова інформація, конфіденційна інформація; 5) Професійна таємниця; 6) Технічні засоби та технології як об'єкти в інформаційних відносинах.</p>	2	<p><i>Литання для самостійного опрацювання:</i></p> <p>1) Інформація як вид власності. Підстави виникнення права власності на інформацію; 2) Співвідношення категорій «інформація», «відомості», «дані», «знання», «таємниця» та інших у суспільних правовідносинах; 3) Державна інформаційна політика; 4) Інформаційна культура; 5) Засоби масової інформації як об'єкти інформаційних правовідносин; 6) Реклама, піар, недобросовісна конкуренція, інформаційна боротьба як об'єкти інформаційних правовідносин; 7) Честь, гідність та ділова репутація як об'єкти інформаційного права.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник</p>	6

1	2	3	4	5	6
				<p>до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Скласти схему або таблицю видів об'єктів інформаційних правовідносин за всіма відомими Вам критеріями їх класифікації.</p>	
Тема 3. Право інтелектуальної власності на об'єкти інформаційних відносин					
<p><i>Лекція 3:</i> 1) Поняття та загальна характеристика права інтелектуальної власності; 2) Регулювання інформаційних відносин інститутом авторського права; 3) Право промислової власності, об'єкти патентних прав; 4) Засоби індивідуалізації. Доменні імена; 5) Комп'ютерна програма як комплексний об'єкт права інтелектуальної власності.</p>	2	<p><i>Семінарське заняття 2:</i> 1) Суб'єктивне право інтелектуальної власності. Об'єкти, суб'єкти та зміст права інтелектуальної власності; 2) Правове регулювання інформаційних відносин щодо виробництва і поширення комп'ютерних програм і баз даних; 3) Ліцензії на використання програмного забезпечення та їх види; 4) Об'єкти патентних прав. Перспективи правової охорони комп'ютерних програм засобами патентного права; 5) Правові засади використання доменних імен в Україні; 6) Комерційна таємниця та ноу-хау.</p>	2	<p><i>Литання для самостійного опрацювання:</i> 1) Основні джерела права інтелектуальної власності; 2) Комп'ютерні програми та інші результати професійної діяльності у сфері інформаційних технологій як об'єкти права інтелектуальної власності; 3) Засоби індивідуалізації: знаки для товарів і послуг, комерційні (фірмові) найменування, географічні зазначення; 4) Поняття та правовий режим науково-технічної інформації. Ноу-хау; 5) Об'єкти права інтелектуальної власності у віртуальному просторі (мета-всесвіті). <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Скласти схему класифікації об'єктів</p>	6

1	2	3	4	5	6
				права інтелектуальної власності (особливу увагу приділити тим із них, що можуть створюватися у сфері ІТ).	
Тема 4. Організаційно-правові засади здійснення професійної діяльності у сфері інформаційних технологій					
<p><i>Лекція 4:</i> 1) Правові форми здійснення професійної діяльності у сфері інформаційних технологій: загальна характеристика; 2) Особливості трудових договорів зі спеціалістами з інформаційних технологій, порядок їх укладення та припинення, права та обов'язки їх сторін; 3) Організаційно-правові форми здійснення самостійної підприємницької діяльності у сфері інформаційних технологій.</p>	2	<p><i>Семинарське заняття 3:</i></p> <p>1) Здійснення підприємницької діяльності у сфері ІТ у формі ФО-П; 2) Товариство з обмеженою відповідальністю (ТОВ); 3) Загальна характеристика акціонерного товариства; 4) Порядок державної реєстрації підприємницької діяльності. Зупинення та припинення підприємницької діяльності; 5) Поняття та правовий режим резидентів Дія Сіті. Особливості гіг-контрактів з гіг-спеціалістами; 6) Особливості трудових договорів зі спеціалістами з інформаційних технологій. Цивільно-правові договори.</p>	2	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Особливості трудових договорів зі спеціалістами з інформаційних технологій, права та обов'язки їх сторін; 2) Відмінності трудових договорів, цивільно-правових договорів та господарських договорів із фізичною особою-підприємцем; 3) Вибір організаційно-правових форм для стартапів; 4) Відмінності трудових договорів, цивільно-правових договорів та господарських договорів із фізичною особою-підприємцем; 5) Порядок внесення майнових інтелектуальної власності до статутного капіталу суб'єктів господарювання.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми.</p> <p>2) Virшення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p> <p>3) Підготувати пакет документів для реєстрації ФОП або ТОВ для діяльності у сфері ІТ.</p>	6
Тема 5. Договірні відносини у сфері інформаційних відносин					

1	2	3	4	5	6
<p><i>Лекція 5:</i> 1) Поняття та загальна характеристика цивільних та господарських зобов'язань, їх види; 2) Поняття договору. Зміст та форма договору, його істотні умови; 3) Порядок укладення, зміни та припинення договору; 4) Види договорів. Договори, що можуть застосовуватися для врегулювання інформаційних відносин та професійної діяльності у сфері інформаційних технологій.</p>	2	<p><i>Семінарське заняття 4:</i> 1) Договори, спрямовані на створення продуктів у сфері ІТ, їх правова природа та зміст; 2) Договори про виконання робіт та їх види; 3) Договори про надання послуг; 4) Договори у сфері інтелектуальної власності; 5) Поняття смарт-контрактів та їх можлива сфера використання; 6) Угоди про нерозголошення комерційної таємниці (NDA). Угоди про неконкуренцію (NCA); 7) Договір купівлі-продажу та його види. Особливості договору купівлі-продажу майнових прав; 8) Договори про передачу майна в користування. Договір лізингу;</p>	2	<p><i>Питання для самостійного опрацювання:</i> 1) Договір купівлі-продажу та його види. Особливості договору купівлі-продажу майнових прав; 2) Договори про передачу майна в користування. Договір лізингу; 3) Договори про відчуження виключних майнових прав інтелектуальної власності; 4) Договори про створення за замовленням і використання об'єктів права інтелектуальної власності. Договори на виконання науково-дослідних, дослідно-конструкторських і технологічних робіт; 5) Юридичні та фактичні послуги. Фінансові послуги. Страхування.</p> <p><i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Знайти та проаналізувати договір про виконання робіт чи надання послуг у сфері ІТ або інший договір із суміжної сфери діяльності (з наданням пояснень, коментарів, потенційних ризиків)</p>	5
Модуль 2. Правове регулювання відносин інформаційної безпеки					
Тема 6. Поняття та об'єкти інформаційної безпеки.					

1	2	3	4	5	6
Законодавство України щодо забезпечення інформаційної безпеки					
<p><i>Лекція 6:</i> 1) Поняття та правові засади інформаційної безпеки України; 2) Об'єкти та види інформаційної безпеки; 3) Напрями державної політики у сфері інформаційної безпеки; 4) Інституційний механізм інформаційної безпеки.</p>	2	<p><i>Семінарське заняття 5:</i> 1) Інституційний механізм інформаційної безпеки; 2) Види загроз національній безпеці в інформаційній сфері; 3) Правовий захист інформації, інформаційних ресурсів та інформаційних систем; 4) Поняття та правові засади інформаційної безпеки України; 5) Напрями державної політики у сфері інформаційної безпеки. Об'єкти інформаційної безпеки;</p>	2	<p><i>Питання для самостійного опрацювання:</i> 1) Поняття національних інтересів та національної безпеки; 2) Органи державної влади, до функціональних повноважень яких входять питання забезпечення інформаційної безпеки (у т.ч. кібербезпеки, захисту інформації); 3) Правові засади захисту об'єктів інформаційних правовідносин від загроз в інформаційній сфері; 4) Інформаційна безпека людини й суспільства. <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми. 2) Ви рішення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p>	2
Тема 7. Зарубіжний досвід правового регулювання інформаційної безпеки. Міжнародні акти в сфері інформаційної безпеки					
	–	<p><i>Семінарське заняття 6:</i> 1) Досвід державного регулювання забезпечення різних аспектів інформаційної безпеки у розвинених зарубіжних державах; 2) Правові аспекти захисту інформації та принципи інформаційної безпеки у Європейському Союзі та окремих країнах</p>	2	<p><i>Питання для самостійного опрацювання:</i> 1) Досвід державного регулювання забезпечення різних аспектів інформаційної безпеки у розвинених зарубіжних державах; 2) Правові аспекти захисту інформації та принципи інформаційної безпеки у Європейському Союзі та окремих країнах ЄС (Німеч-</p>	4

1	2	3	4	5	6
		<p>ЄС (Німеччина, Франція, Італія, держави Східної Європи). GDPR; 3) Правові аспекти захисту інформації та принципи інформаційної безпеки у Сполучених Штатах Америки, Канаді, Великобританії;</p> <p>4) Міжнародно-правові основи інформаційної безпеки. Міжнародні конвенції та угоди в сфері інформаційної безпеки.</p>		<p>чина, Франція, Італія, держави Східної Європи). GDPR; 3) Правові аспекти захисту інформації та принципи інформаційної безпеки у Сполучених Штатах Америки, Канаді, Великобританії;</p> <p>4) Міжнародно-правові основи інформаційної безпеки. Міжнародні конвенції та угоди в сфері інформаційної безпеки.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми.</p> <p>2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p> <p>3) Скласти в ел. формі документ з активними посиланнями на основні міжнародні конвенції та угоди у сфері інформаційної безпеки.</p>	
Тема 8. Забезпечення інформаційної безпеки особи, держави та суспільства					
	–	<p><i>Семинарське заняття 7:</i></p> <p>1) Види загроз безпеці суб'єктів інформаційних правовідносин в інформаційній сфері;</p> <p>2) Інформаційна безпека особи. Задоволення інформаційних потреб учасників інформаційних правовідносин як спосіб забезпечення інформаційної безпеки; 3) Забезпечення інформаційної безпеки суб'єктів</p>	2	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Види загроз безпеці суб'єктів інформаційних правовідносин в інформаційній сфері; 2) Інформаційна безпека особи. Задоволення інформаційних потреб учасників інформаційних правовідносин як спосіб забезпечення інформаційної безпеки;</p> <p>3) Забезпечення інформаційної безпеки суб'єктів підприємницької діяльно-</p>	4

1	2	3	4	5	6
		<p>підприємницької діяльності; 4) Інформаційна безпека суспільства. Зовнішні деструктивні інформаційні впливи на суспільну свідомість; 5) Інформаційна безпека держави.</p>		<p>сті; 4) Інформаційна безпека суспільства. Зовнішні деструктивні інформаційні впливи на суспільну свідомість; 5) Інформаційна безпека держави. <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Скласти таблицю об'єктів інформаційної безпеки із зазначенням основних загроз таким об'єктам.</p>	
Тема 9. Організаційно-правові засади захисту інформації. Захист персональних даних					
<p><i>Лекція 7:</i> 1) Інформація як об'єкт інформаційної безпеки та завдання щодо її захисту; 2) Поняття персональних даних, їх ознаки та види; 3) Поняття обробки (опрацювання) персональних даних; 4) Принципи обробки персональних даних відповідно до законодавства України та GDPR.</p>	2	<p><i>Семінарське заняття 8:</i> 1) Правові аспекти захисту інформації в автоматизованих системах; 2) Підстави для обробки персональних даних; 3) Характеристика операцій з персональними даними; 4) Права та обов'язки суб'єктів персональних даних; 5) Правове становище володільця персональних даних (контролера) та розпорядника персональних даних (оператора); 6) Організаційно-правові заходи запобігання інформаційним загрозам: основні документи. Положення про захист комер-</p>	2	<p><i>Питання для самостійного опрацювання:</i> 1) Диференціація завдань щодо захисту інформації залежно від правового режиму інформації; 2) Технічний захист інформації. Національна система конфіденційного зв'язку; 3) Правове становище Уповноваженого Верховної Ради України з прав людини. ДРО; 4) Вимоги до обробки персональних даних, яких слід дотримуватись під час здійснення професійної діяльності у сфері ІТ; 5) Проектування приватності (Privacy by design); 6) Міжнародна та національна сертифікація з захисту даних. <i>Практичні завдання:</i></p>	6

1	2	3	4	5	6
		ційної таємниці та конфіденційної інформації та супутні документи, privacy policy, privacy notice, DPIО тощо.		1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Знайти і проаналізувати (або самостійно скласти за зразками) один із організаційно-правових документів, спрямованих на запобігання інформаційним загрозам	
Тема 10. Правове регулювання електронних комунікацій та забезпечення кібербезпеки					
	–	<i>Семінарське заняття 9:</i> 1) Законодавство у сфері електронних комунікацій: загальна характеристика та основні поняття; 2) Правові заходи та методи захисту систем електронних комунікацій; 3) Національна система кібербезпеки в Україні; 4) Кіберінциденти та їх категорії. Кібератаки та кіберзлочини; 5) Державні стандарти та нормативні документи, що стосуються технічного захисту інформації. Стандарти кібербезпеки.	2	<i>Питання для самостійного опрацювання:</i> 1) Законодавство у сфері електронних комунікацій: загальна характеристика та основні поняття; 2) Правові заходи та методи захисту систем електронних комунікацій; 3) Національна система кібербезпеки в Україні; 4) Кіберінциденти та їх категорії. Кібератаки та кіберзлочини; 5) Державні стандарти та нормативні документи, що стосуються технічного захисту інформації. Стандарти кібербезпеки. <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми.	6
Тема 11. Захист прав учасників інформаційних відносин, юридична відповідальність у сфері інформаційної безпеки та запобігання корупції в ІТ-галузі					
<i>Лекція 8:</i>	2	<i>Семінарське заняття 10:</i>	2	<i>Питання для самостійного опрацювання:</i>	5

1	2	3	4	5	6
<p>1) Відповідальність за порушення законодавства у сфері інформаційної безпеки: загальна характеристика; 2) Цивільно-правова відповідальність та господарсько-правова відповідальність за правопорушення в інформаційній сфері; 3) Кримінальна відповідальність за правопорушення в сфері інформаційної безпеки; 4) Форми та способи захисту прав та законних інтересів учасників інформаційних правовідносин. 5) Поняття корупції та її прояви. Правове регулювання запобігання корупції.</p>		<p>1) Порушення законодавства у сфері інформаційної безпеки, кібербезпеки; 2) Дисциплінарна та матеріальна відповідальність за правопорушення в інформаційній сфері; 3) Адміністративно-правова відповідальність за правопорушення в інформаційній сфері; 4) Особливості інформаційних правопорушень у кіберпросторі. Загальна характеристика кіберзлочинів та відповідальність за них; 5) Нагляд і контроль за дотриманням законодавства під час здійснення професійної діяльності у сфері інформаційних технологій та з приводу дотримання вимог щодо забезпечення інформаційної безпеки; 6) Заходи, спрямовані на запобігання та протидію корупції. Відповідальність за порушення законодавства у сфері протидії корупції та інших актів, спрямованих на запобігання корупційним проявам та недоброочесності.</p>		<p><i>вання:</i> 1) Порядок притягнення до відповідальності за порушення законодавства у сфері інформаційної безпеки; 2) Цивільно-правова відповідальність та господарсько-правова відповідальність за правопорушення в інформаційній сфері; 3) Data incident, data breach – належне реагування та принципи застосування відповідальності відповідно до GDPR та законодавства України; 4) Види корупційних правопорушень та їх можливі прояви у сфері ІТ (корупційні ризики); 5) Етичні принципи діяльності ІТ-фахівців (етичні кодекси ІТ-компаній). Антикорупційний комплаєнс. Етичні дилеми, пов'язані з корупцією в ІТ-сфері. <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Змоделювати ситуації, у яких можуть виникнути корупційні ризики та/або етичні дилеми щодо них у сфері ІТ.</p>	
Разом	16		20		54

Таблиця 4.2. Тематичний план навчальної дисципліни
 «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки»
 для студентів спеціальності 122 «Комп'ютерні науки» ОПП «Комп'ютерні науки» заочної форми навчання

Назва теми (лекції) та питання теми (лекції)	Кількість годин	Назва теми та питання практи- чного заняття	Кількість годин	Завдання самостійної роботи у розрізі теми	Кількість годин
1	2	3	4	5	6
Модуль 1.					
Правове регулювання інформаційних відносин та професійної діяльності в сфері інформаційних технологій					
Тема 1. Загальна характеристика правового регулювання інформаційних відносин					
<i>Лекція 1:</i> 1) Право, правове регулювання суспільних відносин. Правовідносини та їх структура; 2) Правовідносини, що можуть виникати у ході здійснення професійної діяльності у сфері інформаційних технологій та галузі права, що їх врегульовують; 3) Загальна характеристика інформаційного права; 4) Джерела інформаційного права та суміжних галузей права.	2	–	–	<i>Питання для самостійного опрацювання:</i> 1) Поняття інформаційного суспільства та державна політика у сфері розвитку інформаційного суспільства в Україні; 2) Інформаційні права і свободи у контексті прав людини та їх обмеження; 3) Суб'єкти інформаційних правовідносин та їх види. Зміст інформаційних правовідносин; 4) Класифікація та загальний огляд джерел інформаційного права та інших галузей права, дотичних до регулювання професійної діяльності у сфері інформаційних технологій. <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми.	4

1	2	3	4	5	6
				2) Скласти таблицю нормативних актів, що врегульовують відносини у сфері ІТ із колонками: назва н.-п.а., . 3) Скласти	
Тема 2. Поняття інформації. Правові режими інформаційних ресурсів. Публічна інформація.					
–	–	–	–	<i>Питання для самостійного опрацювання:</i> 1) Поняття об'єктів інформаційних правовідносин, їх види; 2) Інформація як об'єкт правовідносин та її властивості; 3) Класифікація інформації за правовим режимом доступу; 4) Інформаційні системи. Поняття та сутність інформаційних ресурсів; 4) Правове регулювання доступу до публічної інформації. Відкриті дані; 5) Правовий режим інформації з обмеженим доступом: державна таємниця, службова інформація, конфіденційна інформація; 6) Професійна таємниця; 7) Технічні засоби та технології як об'єкти в інформаційних відносинах; 8) Інформація як вид власності. Підстави виникнення права власності на інформацію; 9) Співвідношення категорій «інформація», «відомості», «дані», «знання», «таємниця» та інших у суспільних правовідносинах; 10) Державна інформаційна політика; 11) Інформаційна культура; 12) Засоби масової інформації як об'єкт інформаційних правовідносин; 13) Реклама, піар, недобросовісна конкуренція, інформаційна боротьба як об'єкти інформаційних правовідносин; 14) Честь, гідність та ділова репутація як об'єкти інформаційного права.	10

1	2	3	4	5	6
				<p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Скласти схему або таблицю видів об'єктів інформаційних правовідносин за всіма відомими Вам критеріями їх класифікації.</p>	
Тема 3. Право інтелектуальної власності на об'єкти інформаційних відносин					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Поняття та загальна характеристика права інтелектуальної власності; 2) Регулювання інформаційних відносин інститутом авторського права; 3) Право промислової власності, об'єкти патентних прав; 4) Засоби індивідуалізації. Доменні імена; 5) Комп'ютерна програма як комплексний об'єкт права інтелектуальної власності; 6) Суб'єктивне право інтелектуальної власності. Об'єкти, суб'єкти та зміст права інтелектуальної власності; 7) Правове регулювання інформаційних відносин щодо виробництва і поширення комп'ютерних програм і баз даних; 8) Ліцензії на використання програмного забезпечення та їх види; 9) Об'єкти патентних прав. Перспективи правової охорони комп'ютерних програм засобами патентного права; 10) Комерційна таємниця та ноу-хау; 11) Основні джерела права інтелектуальної власності; 12) Засоби індивідуалізації: знаки для товарів і послуг, комерційні (фірмові) найменування, географічні зазначення; 13) Поняття та правовий режим науково-</p>	6

1	2	3	4	5	6
				<p>технічної інформації. Ноу-хау; 14) Об'єкти права інтелектуальної власності у віртуальному просторі (мета-всесвіті).</p> <p><i>Практичні завдання:</i></p> <ol style="list-style-type: none"> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Скласти схему класифікації об'єктів права інтелектуальної власності (особливу увагу приділити тим із них, що можуть створюватися у сфері ІТ). 	
Тема 4. Організаційно-правові засади здійснення професійної діяльності у сфері інформаційних технологій					
–	–	<p><i>Семінарське заняття 1:</i></p> <ol style="list-style-type: none"> 1) Правові форми здійснення професійної діяльності у сфері інформаційних технологій: загальна характеристика; 2) Особливості трудових договорів зі спеціалістами з інформаційних технологій, порядок їх укладення та припинення, права та обов'язки їх сторін; 	2	<p><i>Питання для самостійного опрацювання:</i></p> <ol style="list-style-type: none"> 1) Особливості трудових договорів зі спеціалістами з інформаційних технологій, права та обов'язки їх сторін; 2) Відмінності трудових договорів, цивільно-правових договорів та господарських договорів із фізичною особою-підприємцем; 3) Вибір організаційно-правових форм для стартапів; 4) Відмінності трудових договорів, цивільно-правових договорів та господарських договорів із фізичною особою-підприємцем; 5) Порядок внесення майнових інтелектуальної власності до статутного капіталу суб'єктів господарювання; 6) Загальна характеристика акціонерного товариства; 7) Особливості трудових договорів зі спеціалістами з інформаційних технологій. Цивільно-правові договори. <p><i>Практичні завдання:</i></p> <ol style="list-style-type: none"> 1) Скласти термінологічний словник до теми. 	8

1	2	3	4	5	6
		<p>3) Організаційно-правові форми здійснення самостійної підприємницької діяльності у сфері інформаційних технологій;</p> <p>4) Здійснення підприємницької діяльності у сфері ІТ у формі ФО-П;</p> <p>5) Товариство з обмеженою відповідальністю (ТОВ);</p> <p>6) Порядок державної реєстрації підприємницької діяльності. Зупинення та припинення підприємницької діяльності;</p> <p>7) Поняття та правовий режим резидентів Дія Сіті. Особливості гіг-контрактів з гіг-спеціалістами.</p>		<p>2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p> <p>3) Підготувати пакет документів для реєстрації ФОП або ТОВ для діяльності у сфері ІТ.</p>	
Тема 5. Договірні відносини у сфері інформаційних відносин					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Поняття та загальна характеристика цивільних та господарських зобов'язань, їх види;</p>	9

1	2	3	4	5	6
				<p>2) Поняття договору. Зміст та форма договору, його істотні умови; 3) Порядок укладення, зміни та припинення договору; 4) Види договорів. Договори, що можуть застосовуватися для врегулювання інформаційних відносин та професійної діяльності у сфері інформаційних технологій; 4) Договори, спрямовані на створення продуктів у сфері ІТ, їх правова природа та зміст; 5) Договори про виконання робіт та їх види; 6) Договори про надання послуг; 7) Договори у сфері інтелектуальної власності; 8) Поняття смарт-контрактів та їх можлива сфера використання; 9) Угоди про нерозголошення комерційної таємниці (NDA). Угоди про неконкуренцію (NCA); 10) Договір купівлі-продажу та його види. Особливості договору купівлі-продажу майнових прав; 11) Договори про передачу майна в користування. Договір лізингу; 12) Особливості договору купівлі-продажу майнових прав; 13) Договори про відчуження виключних майнових прав інтелектуальної власності; 14) Договори про створення за замовленням і використання об'єктів права інтелектуальної власності. Договори на виконання науково-дослідних, дослідно-конструкторських і технологічних робіт; 15) Юридичні та фактичні послуги. Фінансові послуги. Страхування.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p>	

1	2	3	4	5	6
				3) Знайти та проаналізувати договір про виконання робіт чи надання послуг у сфері ІТ або ін. договір із суміж. сфери діяльності (з наданням пояснень, коментарів, потенційних ризиків)	
Модуль 2. Правове регулювання відносин інформаційної безпеки					
Тема 6. Поняття та об'єкти інформаційної безпеки. Законодавство України щодо забезпечення інформаційної безпеки					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Поняття та правові засади інформаційної безпеки України; 2) Об'єкти та види інформаційної безпеки; 3) Напрями державної політики у сфері інформаційної безпеки; 4) Інституційний механізм інформаційної безпеки; 5) Види загроз національній безпеці в інформаційній сфері; 6) Правовий захист інформації, інформаційних ресурсів та інформаційних систем; 7) Об'єкти інформаційної безпеки; 8) Поняття національних інтересів та національної безпеки; 9) Органи державної влади, до функціональних повноважень яких входять питання забезпечення інформаційної безпеки (у т.ч. кібербезпеки, захисту інформації); 10) Правові засади захисту об'єктів інформаційних правовідносин від загроз в інформаційній сфері; 11) Інформаційна безпека людини й суспільства.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p>	6

1	2	3	4	5	6
Тема 7. Зарубіжний досвід правового регулювання інформаційної безпеки. Міжнародні акти в сфері інформаційної безпеки					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Досвід державного регулювання забезпечення різних аспектів інформаційної безпеки у розвинених зарубіжних державах; 2) Правові аспекти захисту інформації та принципи інформаційної безпеки у Європейському Союзі та окремих країнах ЄС (Німеччина, Франція, Італія, держави Східної Європи). GDPR;</p> <p>3) Правові аспекти захисту інформації та принципи інформаційної безпеки у Сполучених Штатах Америки, Канаді, Великобританії;</p> <p>4) Міжнародно-правові основи інформаційної безпеки. Міжнародні конвенції та угоди в сфері інформаційної безпеки.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми.</p> <p>2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО.</p> <p>3) Скласти в ел. формі документ з активними посиланнями на основні міжнародні конвенції та угоди у сфері інформаційної безпеки.</p>	6
Тема 8. Забезпечення інформаційної безпеки особи, держави та суспільства					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Види загроз безпеці суб'єктів інформаційних правовідносин в інформаційній сфері;</p> <p>2) Інформаційна безпека особи. Задоволення інформаційних потреб учасників інформаційних правовідносин як спосіб забезпечення інформаційної безпеки; 3) Забезпечення інфо-</p>	6

1	2	3	4	5	6
				<p>раційної безпеки суб'єктів підприємницької діяльності; 4) Інформаційна безпека суспільства. Зовнішні деструктивні інформаційні впливи на суспільну свідомість; 5) Інформаційна безпека держави.</p> <p><i>Практичні завдання:</i></p> <p>1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Скласти таблицю об'єктів інформаційної безпеки із зазначенням основних загроз таким об'єктам.</p>	
Тема 9. Організаційно-правові засади захисту інформації. Захист персональних даних					
<p><i>Лекція 2:</i> 1) Інформація як об'єкт інформаційної безпеки та завдання щодо її захисту; 2) Поняття персональних даних, їх ознаки та види; 3) Поняття обробки (опрацювання) персональних даних; 4) Принципи обробки персональних даних відповідно до законодавства України та GDPR.</p>	2	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Правові аспекти захисту інформації в автоматизованих системах; 2) Диференціація завдань щодо захисту інформації залежно від правового режиму інформації; 3) Технічний захист інформації. Національна система конфіденційного зв'язку; 4) Підстави для обробки персональних даних; 5) Характеристика операцій з персональними даними; 6) Права та обов'язки суб'єктів персональних даних; 7) Правове становище володільця персональних даних (контролера) та розпорядника персональних даних (оператора); 8) Організаційно-правові заходи запобігання інформаційним загрозам: основні документи. Положення про захист комерційної таємниці та конфіденційної інформації та супутні докумен-</p>	8

1	2	3	4	5	6
				<p>ти, privacy policy, privacy notice, DPIO тощо; 9) Правове становище Уповноваженого Верховної Ради України з прав людини. DPO; 10) Вимоги до обробки персональних даних, яких слід дотримуватись під час здійснення професійної діяльності у сфері ІТ; 11) Проектування приватності (Privacy by design); 12) Міжнародна та національна сертифікація з захисту даних.</p> <p><i>Практичні завдання:</i></p> <ol style="list-style-type: none"> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Знайти і проаналізувати (або самостійно скласти за зразками) один із організаційно-правових документів, спрямованих на запобігання інформаційним загрозам 	
Тема 10. Правове регулювання електронних комунікацій та забезпечення кібербезпеки					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <ol style="list-style-type: none"> 1) Законодавство у сфері електронних комунікацій: загальна характеристика та основні поняття; 2) Правові заходи та методи захисту систем електронних комунікацій; 3) Національна система кібербезпеки в Україні; 4) Кіберінциденти та їх категорії. Кібератаки та кіберзлочини; 5) Державні стандарти та нормативні документи, що стосуються технічного захисту інформації. Стандарти кібербезпеки. <p><i>Практичні завдання:</i></p> <ol style="list-style-type: none"> 1) Скласти термінологічний словник до теми. 	8

1	2	3	4	5	6
Тема 11. Захист прав учасників інформаційних відносин, юридична відповідальність у сфері інформаційної безпеки та запобігання корупції в IT-галузі					
–	–	–	–	<p><i>Питання для самостійного опрацювання:</i></p> <p>1) Відповідальність за порушення законодавства у сфері інформаційної безпеки: загальна характеристика; 2) Цивільно-правова відповідальність та господарсько-правова відповідальність за правопорушення в інформаційній сфері; 3) Кримінальна відповідальність за правопорушення в сфері інформаційної безпеки; 4) Форми та способи захисту прав та законних інтересів учасників інформаційних правовідносин; 5) Порушення законодавства у сфері інформаційної безпеки, кібербезпеки; 6) Дисциплінарна та матеріальна відповідальність за правопорушення в інформаційній сфері; 7) Адміністративно-правова відповідальність за правопорушення в інформаційній сфері; 8) Особливості інформаційних правопорушень у кіберпросторі. Загальна характеристика кіберзлочинів та відповідальність за них; 9) Нагляд і контроль за дотриманням законодавства під час здійснення професійної діяльності у сфері інформаційних технологій та з приводу дотримання вимог щодо забезпечення інформаційної безпеки; 10) Порядок притягнення до відповідальності за порушення законодавства у сфері інформаційної безпеки; 11) Data incident, data breach – належне реагування та принципи застосування відповідальності відповідно до GDPR та законодавства України; 12) Поняття корупції та її прояви. Пра-</p>	10

1	2	3	4	5	6
				<p>воє регулювання запобігання корупції; 13) Заходи, спрямовані на запобігання та протидію корупції. Відповідальність за порушення законодавства у сфері протидії корупції та інших актів, спрямованих на запобігання корупційним проявам та недоброчесності.; 14) Види корупційних правопорушень та їх можливі прояви у сфері ІТ (корупційні ризики); 15) Етичні принципи діяльності ІТ-фахівців (етичні кодекси ІТ-компаній). Антикорупційний комплаєнс. Етичні дилеми, пов'язані з корупцією в ІТ-сфері. <i>Практичні завдання:</i> 1) Скласти термінологічний словник до теми. 2) Вирішення практичного завдання (кейс), запропонованого за НМП чи у СДО. 3) Змоделювати ситуації, у яких можуть виникнути корупційні ризики та/або етичні дилеми щодо них у сфері ІТ.</p>	
Разом	4		2		84

Розділ 5. Система оцінювання знань студентів

Система поточного і підсумкового контролю має за мету оцінювання рівня сформованості тих чи інших компетентностей та досягнення програмних результатів навчання за навчальною дисципліною «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки».

Компетентність як інтегрований результат індивідуальної навчальної діяльності студентів, формується на основі оволодіння ними змістовими (знання), процесуальними (уміння) і мотиваційними компонентами, його рівень виявляється в процесі оцінювання. Визначення рівня сформованості дисциплінарних компетентностей (результатів навчання) здійснюється за: певним розділом (темою) робочої програми навчальної дисципліни; практичними заняттями (контрольна робота, перевірка та захист індивідуального завдання, тестування тощо).

Об'єктами контролю є: робота студентів на лекціях, семінарських заняттях, якість та своєчасність виконання завдань самостійної роботи, поточних модульних робіт. Контрольні заходи здійснюються науково-педагогічними працівниками і включають поточний і підсумковий контроль.

Поточний контроль здійснюється при проведенні лекцій, семінарів, перевірки завдань самостійної роботи та має на меті перевірку рівня засвоєння студентом навчального матеріалу навчальної дисципліни та оцінювання набутих компетентностей.

Під час проведення лекцій застосовуються такі методи контролю, як усне опитування студентів з питань, визначених планом лекцій та пов'язаних з матеріалом попередніх лекцій, дискусійне обговорення проблемних питань з теми лекції та інше.

У ході проведення семінарських занять застосовуються такі методи контролю, як усне та письмове опитування студентів з питань, визначених планом семінарських занять, дискусійне обговорення проблемних питань з теми заняття, письмове складання студентами тестів, відповідь у письмовій формі на індивідуальне теоретичне завдання, письмове виконання індивідуального практичного завдання (приватно-правової ситуації з іноземним елементом), розв'язок термінологічних завдань тощо. Завдання можуть виконуватися як індивідуально, так і «малими групами» (у такому випадку бали виставляються відповідно до внеску кожного студента, а у разі, якщо його встановити неможливо – в однаковому для всіх розмірі за результатами виконання завдання).

Поточний контроль виконання студентами завдань самостійної роботи здійснюється за допомогою перевірки науково-педагогічним працівником результатів розв'язання ситуаційних завдань.

Поточний контроль, який застосовується під час проведення поточних модульних робіт, здійснюється при перевірці виконання відповідних тестів в письмовій формі або за допомогою відповідного програмного

забезпечення комп'ютерної підтримки освітнього процесу, при перевірці виконання практичних ситуацій в письмовій формі тощо.

Поточна успішність студентів за виконання навчальних видів робіт на навчальних заняттях і за виконання завдань самостійної роботи оцінюються **за допомогою національної шкали оцінок**.

Таблиця 5. Розподіл балів за результатами вивчення навчальної дисципліни для студентів спеціальності 122 «Комп'ютерні науки» ОПП «Комп'ютерні науки»

Види робіт	Максимальна кількість балів
Модуль 1 (теми 1-5): відвідування усіх занять (не більше 3,5 балів – за наявності конспектів занять та за умови присутності на них); участь у обговоренні матеріалу тем семінарських занять (12 балів); виконання навчальних та практичних завдань, завдань самостійної роботи, вибіркове тестування (загалом – 5 балів); поточна модульна робота (тестування) (12 балів)	26,5
Модуль 2 (теми 6-11): відвідування усіх занять (не більше 3,5 балів – за наявності конспектів занять та за умови присутності на них); участь у обговоренні матеріалу тем семінарських занять (12 балів); виконання навчальних та практичних завдань, завдань самостійної роботи, вибіркове тестування (загалом – 5 балів); поточна модульна робота (тестування) (12 балів)	33,5
Екзамен (тест – 15 балів; відповідь на питання екзаменаційного білета – 25 балів)	40
Разом	100

Таблиця 6. Розподіл балів за результатами вивчення навчальної дисципліни «Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки»

Сума балів за всі види навчальної діяльності	Оцінка за шкалою ECTS	Оцінка за національною шкалою
90-100	A	Відмінно
82-89	B	Дуже добре
74-81	C	Добре
64-73	D	Задовільно
60-63	E	Задовільно достатньо
35-59	FX	Незадовільно з можливістю повторного підсумкового контролю
0-34	F	Незадовільно з обов'язковим повторним вивченням навчальної дисципліни та підсумковим контролем

Розділ 6. Інформаційні джерела

Нормативно-правові акти

1. Конституція України Конституція України прийнята на п'ятій сесії Верховної Ради України від 28 червня 1996 року. URL: <https://www.president.gov.ua/documents/constitution>
2. Господарський кодекс України: Закон України від 16 січня 2003 р. № 436-IV. *Офіційний вісник України*. 2003. № 11. Ст. 462.
3. Кодекс України про адміністративні правопорушення від 18 грудня 1984 р. Відомості Верховної Ради УРСР. 1984. № 40. Ст. 1122.
4. Кримінальний кодекс України: прийнятий 05.04.2001 № 2341-III від 19.08.2022. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
5. Податковий кодекс України: Закон України від 2 грудня 2010 р. № 2755-VI. *Офіційний вісник України*. 2010. № 92. Т. 1. Ст. 3248.
6. Про державну реєстрацію юридичних осіб, фізичних осіб – підприємців та громадських формувань: Закон України від 15 травня 2003 р. № 755-IV (в редакції Закону № 835-VIII від 26 листопада 2015 р.). *Відомості Верховної Ради України*. 2016. № 2. Ст. 17.
7. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
8. Про електронні довірчі послуги: Закон України від 5 жовтня 2017 р. № 2155-VIII // *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.
9. Про захист від недобросовісної конкуренції: Закон України від 7 червня 1996 року № 236/96-ВР. *Відомості Верховної Ради України*. 1996. № 36. Ст. 164.
10. Про запобігання корупції : Закон України від 14 жовтня 2014 року № 1700-VII. URL: <https://zakon.rada.gov.ua/laws/show/1700-18>
11. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
12. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
13. Про засади державної антикорупційної політики на 2021-2025 роки: Закон України від 20 червня 2022 року № 2322-IX. URL: <https://zakon.rada.gov.ua/laws/show/2322-20#n93>
14. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
15. Про міжнародне приватне право: Закон України від 23 червня 2005 р. № 2709-IV. *Відомості Верховної Ради України*. 2005. № 32. Ст. 422.
16. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#n355>
17. Про основні засади державного нагляду (контролю) у сфері господарської діяльності: Закон України від 5 квітня 2007 року № 877-V. *Відомості Верховної Ради*. 2007. № 29. Ст. 389.

18. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>

19. Про публічні закупівлі: Закон України від 25 грудня 2015 року № 922-VIII. URL: <https://zakon.rada.gov.ua/laws/show/922-19#Text>

20. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України. URL: <https://zakon.rada.gov.ua/laws/show/47/2017> та інші.

21. Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23 грудня 1997 року № 776/97-ВР. URL: <https://zakon.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80#Text>

22. Про фінансовий лізинг: Закон України від 16 грудня 1997 р. № 723/97-ВР. *Відомості Верховної Ради України*. 1998. № 16. Ст. 68.

23. Цивільний кодекс України: прийнятий 16.01.2003 № 435-IV в редакції від 10.10.2022. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

24. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних : прийнятий 08 листопада 2001 року. URL: https://zakon.rada.gov.ua/laws/show/994_363/sp:max50:nav7:font2#Text

25. Додатковий протокол до Конвенції Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних». URL: https://zakon.rada.gov.ua/laws/show/994_363?test=7pVMfVelm06OmUnYZiIPzapnHI41gs80msh8Ie6#Text

26. Загальна декларація прав людини : прийнята 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text

27. Конвенція Організації Об'єднаних Націй проти корупції від 31 жовтня 2003 року. URL: https://zakon.rada.gov.ua/laws/show/995_c16#Text

28. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини). URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

29. Конвенція про кіберзлочинність. 23.11. 2001. Ратифікація від 07.09.2005, підстава – 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575

30. Конвенція Ради Європи №108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». URL: https://zakon.rada.gov.ua/laws/show/994_326#Text

31. Кримінальна конвенція про боротьбу з корупцією від 27 січня 1999 року (ETS 173). URL: https://zakon.rada.gov.ua/laws/show/994_101#Text

32. Міжнародний пакт про громадянські і політичні права : прийнятий 16 грудня 1966 року. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

33. ООН, Генеральна Асамблея, Резолюція про право на приватність у цифрову еру (Resolution on the right to privacy in the digital age), A/RES/68/167, Нью-Йорк, 18 грудня 2013 року; та ООН, Генеральна Асамблея, Переглянутий проект Резолюції про право на приватність у

цифрову еру, А/С.3/69/L.26/Rev.1, Нью-Йорк, 19 листопада 2014 року.
URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/449/47/PDF/N1344947.pdf?OpenElement>

34. Про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: Угода від 27 червня 2014 р. № 984_011 (ратифіковано із заявою Законом № 1678-VII від 16.09.2014). *Офіційний вісник України*. – 2014. – № 75. – Ст. 83.

35. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#n6

36. Угода про створення групи держав по боротьбі з корупцією (GRECO). URL: https://zakon.rada.gov.ua/laws/show/994_145#Text

37. Цивільна конвенція про боротьбу з корупцією від 4 листопада 1999 року. URL: https://zakon.rada.gov.ua/laws/show/994_102#Text

38. Рішення Конституційного Суду України №2-рп/2012 від 20 січня 2012 року. URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>

39. «Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації» затверджений Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014 р. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14?test=n6NMfJRw7UpVmUn6ZilPzapnHI41gs80msh8Ie6#n11

40. «Типовий порядок обробки персональних даних» затверджений Наказом Уповноваженого Верховної Ради України з прав людини № 1/02-14 від 08.01.2014 р. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14?test=n6NMfJRw7UpVmUn6ZilPzapnHI41gs80msh8Ie6#n11

41. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних: Наказ Уповноваженого Верховної Ради України з прав людини 08.01.2014 № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

42. Про затвердження документів у сфері захисту персональних даних : наказ Уповноваженого Верховної Ради України з прав людини від 08 січня 2014 року № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text

43. Про затвердження особливостей здійснення публічних закупівель товарів, робіт і послуг для замовників, передбачених Законом України “Про публічні закупівлі”, на період дії правового режиму воєнного стану в Україні та протягом 90 днів з дня його припинення або скасування :

Постанова Кабінету Міністрів України від 12 жовтня 2022 р. № 1178.
URL: <https://zakon.rada.gov.ua/laws/show/1178-2022>

44. Стратегія інформаційної безпеки : Затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n14>

45. ISO 27001:2013 URL: ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements

46. ISO 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines. URL: <https://www.iso.org/standard/71670.html>

47. ISO/IEC 29100:2011 Information technology - Security techniques – Privacy framework URL: <https://www.iso.org/standard/45123.html>

48. ISO 31000 Менеджмент ризиків. URL: <https://www.iso.org/ru/iso-31000-risk-management.html>

49. ДСТУ 7731:2015 Інформаційні технології. Методи захисту. Основні положення щодо забезпечення невторчання в особисте життя (ISO/IEC 29100:2011, MOD) URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66872

50. ДСТУ ISO/IEC 27000:2015 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник (ISO/IEC 27000:2014, IDT) URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=66893

51. НД ТЗІ 3.7-003-05 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>

Основні рекомендовані джерела інформації:

52. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти: науково-практичний посібник. К.: «К.І.С.», 2021 157с. URL: <https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69>

53. Вишня В., Гариш О., Рижков Е. Основи інформаційної безпеки. Навчальний посібник. Дніпро. 2020. 128 с.

54. Вінник О. М. Господарське право [Текст] : курс лекцій : (заг. частина) / Вінник О. М. ; НДІ приват. права і підприємництва ім. Ф. Г. Бурчака НАПрН України. Київ : Ліра-К, 2017. 239 с.

55. Гуржій Т. О., Петрицький А. Л. Правовий захист персональних даних : монографія. Київ: Київ. нац. торг.-екон. унт, 2019. 216 с.

56. Інформаційна безпека: навчальний посібник / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарев та ін. Львів : Видавництво Львівської політехніки, 2019. 580 с.

57. Ковалів М.В., Єсімов С.С., Ярема О.Г. Інформаційне право України : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 416 с.

58. Кормич Б.А., Федотов О.П., Аверочкіна Т.В. Правове регулювання інформаційної діяльності: навчально-методичний посібник. Одеса, 2018. 150 с.

59. Нашинець-Наумова А.Ю. Інформаційне право: навчальний посібник. К. : Київ. ун-т ім. Б. Грінченка, 2020. 136 с.

60. Остроухов В.В., Присяжнюк М.М., Фермагей О.І., Чеховська М.М. Інформаційна безпека. К.: Ліра-К. 2021. 412 с.

61. Посібник з європейського права у сфері захисту персональних даних (2018 р.) перекладено українською. URL: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ukr.pdf

Додаткові рекомендовані джерела інформації:

62. Асірян С.Р., Алексанян К.А. GDPR як стандарт захисту персональних даних в Європейському Союзі. Право і суспільство. 2021. № 6. 298-302.

63. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти. К. 2021. 160 с. URL: <https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69>

64. Беца О. Захист персональних даних для Apple, «смерть реклами» для Facebook. За що сваряться техногіганти. URL: <https://ms.detector.media/it-kompanii/post/26723/2021-02-26-zakhystpersonalnykh-danykh-dlya-apple-smert-reklamy-dlya-facebook-za-shchosvaryatsya-tekhnogiganty/>

65. Белова Ю. Д. Цивільні правовідносини щодо персональних даних. Дисертація на здобуття наукового ступеня доктора філософії. 081 Право. Хмельницький університет управління та права імені Леоніда Юзькова. Хмельницький, 2021. 248 с.

66. Белова Ю. Д. Цивільні правовідносини щодо персональних даних: автореф. дис. ... д.філософ : 081 - Право. Право. 2021.

67. Белова Ю. Згода та інші підстави виникнення цивільних правовідносин щодо персональних даних. Юридичний вісник. 2020. № 3. С. 348-355.

68. Богарада Сергій, Територія застосування GDPR. URL: <https://legalitgroup.com/teritoriya-zastosuvannya-gdpr/>

69. Брайчевський С.М. Персональні дані та мультимедіа. Інформація і право. 2020. № 4 (35). С. 82-91.

70. Булавіна С., Давидова Т. Право на приватність у системі покоління прав людини. Історико-правовий часопис. 2018. № 1. С. 10-14. URL: <http://evnuir.vnu.edu.ua/handle/123456789/15120>

71. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ.ун-т внутріш. справ, 2020. 128 с.

72. Волоха Д. Згода на обробку персональних даних: свято бюрократії чи спосіб захиститися? 2019. URL: <https://khpg.org/1573588054>.

73. Газізова Ю. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606

74. Гронь О.В., Погореленко А.К. Проблеми захисту персональних даних у контексті сучасної комунікації. Науковий вісник Ужгородського

національного університету. Серія: Міжнародні економічні відносини та світове господарство. 2018. 19 (1). С. 102-108.

75. Давлатов Ш.Б. Правові підстави використання колекторами персональних даних. Законодавство України про фінансові послуги: питання адаптації до права Європейського Союзу: матер. Науково-практичного круглого столу (Суми, 15 січня 2021 р.). Суми : Сумський державний університет, 2021. С. 42-45.

76. Захист персональних даних у контексті продажу та просування в інтернеті: національні та європейські вимоги. URL: <https://legalitygroup.com/zahist-personalnih-danih-u-konteksti-prodazhu-taprosuvannya-v-interneti-natsionalni-ta-yevropejski-vimogi/>

77. Інформаційна безпека особи, держави та суспільства в сучасну цифрову епоху. НАУДС. URL: <https://pdp.nacs.gov.ua/courses/informatsiina-bezpeka>

78. Інформаційна безпека: навчальний посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселічник, А. П. Бондарев, С. С. Войтусік, А. Я. Горпенюк, О. А. Немкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко, І. Я. Тишик. Львів : Видавництво Львівської політехніки, 2019. 580 с.

79. Корня А. Захист персональних даних у процесі використання таргетованої реклами та прямого маркетингу. URL: https://uz.ligazakon.ua/ua/magazine_article/EA012761

80. Олексюк Л. Кращі практики управління кібербезпекою. Оглядовий звіт. Проєкт ЄС –ПРООН. 130 с.

81. Микуліна М.М. Щодо відповідності принципів захисту фізичних осіб при обробці персональних даних. Актуальні проблеми управління інформаційною безпекою держави : зб. тез наук. доп. наук.-практ. конф. (Київ, 30 березня 2018 р.). Київ : Нац. акад. СБУ, 2018. С. 314-318.

82. Мукоїда Р.В., Аносенков А.А. Правове забезпечення захисту персональних даних в Україні. Кібербезпека в Україні: правові та організаційні питання: матеріали міжн. наук. практ. конф., м. Одеса, 26 листопада 2020 р. Одеса : ОДУВС, 2021. С. 12-17.

83. Некіт К.Г. Персональні дані та індустриальні дані як об'єкти права власності: оцінка перспектив. Часопис цивілістики. 2020. Вип. 36. С. 57-64.

84. Петік М., Мядзветська Ю. Неочевидні нюанси GDPR. Що треба знати про принцип Privacy by Design, щоб не отримати штраф на \$16 мільйонів. URL: <https://dou.ua/lenta/articles/gdpr-and-privacy-by-design/>

85. Право на приватність / Українська гельсінська спілка з прав людини. URL: <https://helsinki.org.ua/articles/pravo-na-pryvattnist/>

86. Право на приватність та інші права людини і захист ПД. URL: <http://zpd.inf.ua/page10.html#top>

87. Рекомендації Уповноваженого Верховної Ради України з прав людини щодо забезпечення захисту персональних даних під час укладення Україною міжнародних договорів, які передбачають транскордонний обмін даними. URL: <https://www.ombudsman.gov.ua/storage/app/media/transkordonna-peredacha-personalnyh-danyh.pdf>

88. Рекомендації Уповноваженого Верховної Ради України з прав людини щодо належного захисту персональних даних під час створення реєстраційних форм і опитувань, зокрема за допомогою Google форм. URL: <https://www.ombudsman.gov.ua/storage/app/media/vykorystannya-onlain-form.pdf>

89. Сировой М. Конфіденційність в Україні – на критичному рівні. Як захистити свої персональні дані? / Інформаційний портал «Права людини в Україні». URL: <https://khpg.org/1548965232>

90. Тарасюк А.В. Вплив Загального регулювання захисту даних на контролерів та процесорів персональних даних – резидентів України. Інформація і право. 2018. №1(24). С. 28-35.

91. Шадська У. Право на приватне життя: історія, розвиток, українські реалії. Zmina. 2021. URL: <https://zmina.info/columns/pravo-na-pryvatne-zhyttya-istoriya-rozvytok-ukrayinski-realiyi/>

92. Що таке приватність? / Інформаційний портал «Права людини в Україні». URL: <https://khpg.org/1604922460>

93. Яворська О.С. Захист особи у зв'язку з опрацюванням її персональних даних: досвід ЄС. Конституційні цінності: правова природа та практика реалізації : збірник тез Міжнародної науково-практичної конференції (м. Хмельницький, 17 травня 2019 року). [у 2-х част.]. Частина 2. Хмельницький, 2019. С. 290-294.

94. Яковлев Р.В. Принципи мінімізації та точності персональних даних під час використання технології розподіленого реєстру (адміністративно-правовий аспект). ScienceRise. Juridical Science. 2019. № 4. С. 16-24. Режим доступу: http://nbuv.gov.ua/UJRN/srjusc_2019_4_5

95. A Practical Guide to Personal Data Breach Notifications under the GDPR. URL: https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

96. Confessore N. Cambridge Analytica and Facebook: The Scandal and the Fallout So Far, The New York Times. URL: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal/fallout.html>

97. European Data Protection Board. URL: Guidelines, Recommendations, Best Practices | European Data Protection Board (europa.eu)

98. Guidelines 01/2021 on Examples regarding Personal Data Breach Notification. URL: Guidelines 01/2021 on Examples regarding Personal Data Breach Notification

99. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020 URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2019_04_dataprotection_by_design_and_by_default_v2.0_en.pdf

100. ISO 37001:2016. Система управління заходами боротьби з корупцією вимоги із рекомендаціями для використання: офіційний збірник / НАЗК. URL: https://wiki.nazk.gov.ua/wp-content/uploads/2021/11/22.-ISO-37001_2016_ukr.pdf

101. Japp-Henk Hoepman. Privacy Design Strategies (The Little Blue Book). April 19, 2022. URL: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf>

102. My data are mine. Why we should have ownership rights on our personal data: report. URL: <https://www.generationlibre.eu/wp-content/uploads/2018/01/Rapport-Data-2018-EN-v2.pdf>.

103. Principles of the GDPR and what they mean, Amara ingenieria de marketing. URL: <https://www.amara-marketing.com/travel-blog/7-principles-of-the-gdpr-and-what-they-mean>

104. Strategic Privacy by Design, Second Edition. URL: <https://iapp.org/resources/article/strategic-privacy-by-design/>

105. Warren, Samuel D., and Louis D. Brandeis. The Right to Privacy. Harvard Law Review. 1890. Vol. 4. № 5. P. 193–220. URL: <https://doi.org/10.2307/1321160>

Розділ 7. Програмне забезпечення навчальної дисципліни

1. Загальне програмне забезпечення:

Пакет програмних продуктів Microsoft Office, до якого входить програмне забезпечення для роботи з різними типами документів: текстами, електронними таблицями, презентаціями, базами даних тощо. Мережеві сервіси Google.

Основними й найбільш використовуваними складовими пакету Microsoft Office є:

1. Microsoft Word.
2. Microsoft Excel.
3. Microsoft Power Point.

2. Спеціалізоване програмне забезпечення комп'ютерної підтримки освітнього процесу:

- Правові основи діяльності в сфері інформаційних технологій та інформаційної безпеки: Дистанційний курс з дисципліни для студентів спеціальності 122 «Комп'ютерні науки» ОПП «Комп'ютерні науки» [Електронний ресурс]. URL: <http://www.el.puet.edu.ua>
- Презентації Microsoft PowerPoint з тем курсу;
- Інформаційно-правова система «ЛІГА:ЗАКОН»; інформаційно-правова система із законодавства України «Право» (Компанія «Інформаційно-аналітичний центр «БІТ») або аналоги (зокрема, Офіційний портал Верховної Ради України, підсистема «Законодавство України»).
- пакети тестів до тем навчальної дисципліни для студентів денної та заочної форм навчання, розміщені в системі Open test / та або Moodle чи альтернативних платформах.