Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«___»_____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «КІБЕРНЕТИЧНЕ ПРАВО»

для студентів

спеціальності	125 Кібербезпека
освітнього рівня	першого (бакалаврського)
освітньої програми	125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

Розробники:

Гулак Геннадій Миколайович, доктор технічних наук, доцент, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Мазур Наталія Петрівна, кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Мазур Наталія Петрівна, кандидат педагогічних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 23.08.2023 р. № 8

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2023 р.

Керівник освітньої програми _____ (підпис) Артем ПЛАТОНЕНКО

Робочу програму перевірено

___.___. 2023 р.

Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання	
	денна	заочна
Вид дисципліни	обов'язкова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	4 / 120	
Курс	2	
Семестр	3	
Кількість змістових модулів з розподілом:	4	
Обсяг кредитів	4	
Обсяг годин, в тому числі:	120	
Аудиторні	56	
Модульний контроль	8	
Самостійна робота	56	
Форма семестрового контролю	залік	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Кібернетичне право» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчального плану спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Кібернетичне право» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Навчальна дисципліна «Кібернетичне право» складається з чотирьох змістових модулів: «Теоретико-методологічні засади кібернетичного права»; «Правове регулювання суспільних відносин у сфері захисту даних»; «Правове регулювання суспільних відносин у інформаційних системах, інформаційних технологіях і засобах їх забезпечення»; «Кіберзлочинність. Міжнародні стратегії у сфері кібербезпеки». Обсяг дисципліни – 120 год (4 кредити).

Програма має на ***меті*** отримання студентами комплексу знань про систему кібернетичного права як галузі права, його сутність, поняття, методи та зміст, а також в застосуванні їх на практиці.

Основними завданнями вивчення дисципліни є:

- сформувати у студентів цілісні знання про загальні засади правового регулювання суспільних відносин в інформаційній (кібернетичній) сфері, про правовий режим інформації з обмеженим доступом, про правове регулювання суспільних відносин у сфері захисту інформації, про правове регулювання інформаційних відносин в окремих сферах діяльності, про відповідальність за правопорушення у сфері інформаційних відносин;
- виробити навики у студентів щодо застосування вимог нормативно-правових актів України в інформаційній (кібернетичній) сфері та методів кібернетичного права в практичній діяльності.

та ***набуття наступних фахових компетентностей***:

КФ-1 – Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.

КФ-8 – Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

3. Результати навчання за дисципліною

При вивченні курсу «Інформаційне та кібернетичне право» студенти повинні

знати:

– загальні засади правового регулювання суспільних відносин в інформаційній (кібернетичній) сфері;

– основи забезпечення правового режиму інформації з обмеженим доступом;

– основи правового регулювання суспільних відносин у сфері захисту інформації;

– основи правового регулювання інформаційних відносин в окремих сферах діяльності;

– відповідальність за правопорушення у сфері інформаційних відносин;

– основи організаційного забезпечення кібернетичної безпеки підприємств, установ, організацій;

уміти:

– демонструвати володіння предметною базою знань та сучасними техніками дослідження, створювати та інтерпретувати нові знання;

– застосовувати діючу законодавчу базу в галузі інформаційної безпеки для забезпечення необхідних дій професійної діяльності;

– застосовувати діючу законодавчу базу в галузі інформаційної безпеки та захисту інформації з обмеженим доступом у конкретній сфері діяльності, включаючи адекватні організаційні заходи;

– застосовувати системний підхід до розробки комплексу організаційних заходів, враховуючи особливості функціонування підприємства та вирішуваних ним завдань;

– організовувати діяльність підрозділів захисту інформації, включаючи особливості функціонування підприємства та вирішуваних ним завдань;

– розробляти нормативно-методичні матеріали з організації захисту інформації, включаючи особливості функціонування підприємства та вирішуваних ним завдань;

– проектувати та реалізовувати комплексну систему захисту інформації організації (підприємства) до вимог нормативних документів системи технічного захисту інформації;

– надавати пропозицій для заключення угод і договорів з іншими установами, організаціями й підприємствами для проведення робіт в області захисту інформації;

– розробляти пропозицій по вдосконалюванню та підвищенню ефективності прийнятих технічних мір і організаційних заходів;

– застосовувати системний підхід до розробки комплексу організаційних заходів, включаючи особливості функціонування підприємства та вирішуваних ним завдань, включаючи особливості функціонування підприємства та вирішуваних ним завдань;

– організовувати діяльність підрозділів захисту інформації, включаючи особливості функціонування підприємства та вирішуваних ним завдань;

– проводити перевірки установ, організацій і підприємств по виконанню вимог правових норм і стандартів, що стосується ліцензування й сертифікації в області інформаційної безпеки, нормативно-технічної документації по захисту інформації, участь у підготовці відзивів і висновків на нормативно-методичні матеріали й технічну документацію;

– застосовувати вимоги нормативно-правових актів України в інформаційній (кібернетичній) сфері в практичній діяльності;

– застосовувати методи кібернетичного права при розробці положень, інструкцій, правил тощо в практичній діяльності;

досягти наступних ***програмних результатів навчання***:

ПРз-1: - готувати пропозиції до нормативних актів і документів з метою забезпечення встановленої політики інформаційної та/або кібербезпеки; - розробляти проектну документацію, щодо програмних та програмно-апаратних комплексів захисту

інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем; - виконувати аналіз реалізації прийнятої політики інформаційної та/або кібербезпеки;

ПРз-6: - вирішувати задачі управління процесами забезпечення неперервності бізнесу з використанням процедур резервування програмного забезпечення та безпосередньо інформаційних ресурсів; - вирішувати задачі корекції цілей, стратегій, планів забезпечення неперервності бізнесу після здійснення кібератак, збоїв та відмов різних класів; - створювати і впроваджувати плани процесу забезпечення неперервності бізнесу; - виконувати аналіз налаштувань елементів інформаційних систем та комунікаційного обладнання.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Теоретико-методологічні засади кібернетичного права							
Тема 1. Засади формування та становлення кібернетичного права. Роль та місце кібернетичного права в системі права держави	9	2	2				5
Тема 2. Поняття та зміст методу кібернетичного права	8	2		2			4
Модульний контроль	2						
Разом	**19**	**4**	**2**	**2**			**9**
Змістовий модуль 2. Правове регулювання суспільних відносин у сфері захисту даних							
Тема 3. Поняття та правовий режим інформаційних ресурсів	7	2	2				3
Тема 4. Теоретичні та методологічні основи захисту інформації	7	2		2			3
Тема 5. Структура законодавства в сфері захисту інформації. Державна система захисту інформації	5	2					3
Тема 6. Правове регулювання суспільних відносин у сфері захисту банківської та комерційної таємниці, персональних даних	11	2	2	2			6
Тема 7. Правове регулювання суспільних відносин у сфері охорони державної таємниці та захисту службової інформації	8		2				5
Модульний контроль	2						
Разом	**40**	**8**	**6**	**4**			**20**
Змістовий модуль 3. Правове регулювання суспільних відносин у інформаційних системах, інформаційних технологіях і засобах їх забезпечення							
Тема 8. Поняття та правовий режим інформаційних систем, інформаційних технологій і засобів їх забезпечення		2		2			3

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Тема 9. Правове регулювання суспільних відносин у сфері технічного захисту інформації		2	2				3
Тема 10. Правове регулювання суспільних відносин у сфері криптографічного захисту інформації			2				3
Тема 11. Правове регулювання суспільних відносин у сфері захисту інформації в інформаційно-телекомунікаційних системах		2	2	2			3
Тема 12. Правове регулювання баз даних, інформаційних систем, відносин, що формуються під час використання хмарних обчислень та віртуальних активів		2		2			4
Модульний контроль	2						
Разом		**8**	**6**	**6**			**16**
Змістовий модуль 4. Кіберзлочинність. Міжнародні стратегії у сфері кібербезпеки							
Тема 13. Правове забезпечення інформаційної безпеки		2		2			3
Тема 14. Міжнародний досвід правового регулювання суспільних відносин в кібернетичній сфері							3
Тема 15. Кіберзлочинність. Юридична відповідальність за правопорушення у галузі інформаційного законодавства		2	2	2			3
Модульний контроль	2						
Разом		**4**	**2**	**4**			**9**
Усього годин	**120**	**24**	**16**	**16**			**56**

5. Програма навчальної дисципліни

<u>Змістовий модуль 1</u>. Теоретико-методологічні засади кібернетичного права.

Тема 1. Засади формування та становлення кібернетичного права. Роль та місце кібернетичного права в системі права держави.

Засади формування та становлення кібернетичного права. Об’єкт та предмет кібернетичного права. Поняття та зміст системи права. Роль та місце кібернетичного права в системі права держави.

Тема 2. Поняття та зміст методу кібернетичного права.

Поняття методу кібернетичного права. Поняття та зміст методу науки інформаційного права. Поняття та зміст методу навчальної дисципліни «Кібернетичне право». Поняття та зміст методу інформаційного та кібернетичного права як галузі права.

<u>Змістовий модуль 2</u>. Правове регулювання суспільних відносин у сфері захисту

даних.

Тема 3. Поняття та правовий режим інформаційних ресурсів.

Види інформації. Поняття «інформаційні ресурси». Правовий режим інформаційних ресурсів. Правовий обіг інформації.

Тема 4. Теоретичні та методологічні основи захисту інформації.

Базові поняття у галузі інформаційної безпеки та кібербезпеки. Складові інформаційної безпеки. Характеристика інформації як предмета захисту. Інформація як об'єкт права власності. Сутність та цілі захисту інформації. Циклічна модель інформаційної безпеки. Потенційні загрози безпеки інформації та їх класифікація

Тема 5. Структура законодавства в сфері захисту інформації. Державна система захисту інформації.

Загальна характеристика законодавчих актів в сфері захисту інформації. Захист інформації як об'єкт адміністративно-правового регулювання. Система органів регулювання технічного захисту інформації України. Взаємодія суб'єктів системи технічного захисту інформації.

Тема 6. Правове регулювання суспільних відносин у сфері захисту банківської та комерційної таємниці, персональних даних.

Поняття «банківська таємниця». Правовий режим банківської таємниці. Поняття «комерційна таємниця» та її правовий режим.

Поняття «персональні дані». Правовий режим персональних даних. Загальний регламент про захист персональних даних (GDPR).

Тема 7. Правове регулювання суспільних відносин у сфері охорони державної таємниці та захисту службової інформації.

Поняття «державна таємниця». Правовий режим державної таємниці.

Поняття «службова інформація». Правовий режим службової інформації.

<u>Змістовий модуль 3</u>. Правове регулювання суспільних відносин у інформаційних системах, інформаційних технологіях і засобах їх забезпечення.

Тема 8. Поняття та правовий режим інформаційних систем, інформаційних технологій і засобів їх забезпечення.

Інформаційні системи та технології. Правовий режим інформаційних систем, інформаційних технологій та засобів їх забезпечення.

Тема 9. Правове регулювання суспільних відносин у сфері технічного захисту інформації.

Загальні положення про технічний захист інформації. Організація захисту інформації з обмеженим доступом від витоку каналами побічних електромагнітних випромінювань та наводок.

Організація захисту інформації з обмеженим доступом у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок. Вимоги щодо порядку категоріювання об'єктів інформаційної діяльності. Основні положення щодо створення комплексу технічного захисту інформації.

Тема 10. Правове регулювання суспільних відносин у сфері криптографічного захисту інформації.

Загальні положення про криптографічний захист інформації. Правовий режим криптографічного захисту інформації: ліцензійні умови провадження господарської діяльності, надання послуг в галузі криптографічного захисту інформації; порядок проведення сертифікації засобів криптографічного захисту інформації; державна експертиза в сфері криптографічного захисту інформації.

Електронний цифровий підпис. Правовий режим використання електронного цифрового підпису.

Тема 11. Правове регулювання суспільних відносин у сфері захисту інформації в інформаційно-телекомунікаційних системах.

Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Організація діяльності служби захисту інформації в автоматизованій системі.

Організація проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. Організація захисту службової інформації від несанкціонованого доступу під час оброблення в автоматизованих системах. Організація захисту інформації WEB-сторінки від несанкціонованого доступу.

Тема 12. Правове регулювання баз даних, інформаційних систем, відносин, що формуються під час використання хмарних обчислень та віртуальних активів

Інтернет. Суб'єкти та об'єкти правовідносин у мережі Інтернет. Правове регулювання інтернет-відносин. Моделі застосування хмарних технологій. Особливості правового регулювання суспільних відносин під час використання хмарних технологій.

Правове регулювання віртуальних активів. Інформаційна (цифрова) економіка.

Змістовий модуль 4. Кіберзлочинність. Міжнародні стратегії у сфері кібербезпеки.

Тема 13. Правове забезпечення інформаційної безпеки

Поняття та види інформаційної безпеки. Інформаційна безпека у структурі національної безпеки. Система забезпечення інформаційної безпеки. Методи забезпечення інформаційної безпеки. Загрози інформаційній безпеці України. Основні положення Стратегії інформаційної безпеки України. Основні положення Стратегії кібербезпеки України.

Тема 14. Міжнародний досвід правового регулювання суспільних відносин в кібернетичній сфері.

Історичний розвиток протидії кібернетичній злочинності у світі. Стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших.

Тема 15. Кіберзлочинність. Юридична відповідальність за правопорушення у галузі інформаційного законодавства

Класифікація кіберзлочинів відповідно до Конвенції Ради Європи про кіберзлочинність. Загальна характеристика юридичної відповідальності за порушення норм інформаційного законодавства. Поняття, ознаки, склад і види інформаційних правопорушень. Адміністративна відповідальність за порушення законодавства про інформацію. Кримінально-правова відповідальність у сфері інформаційних правовідносин.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;

- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни, де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	4	4	4	4	2	2
Відвідування семінарських занять	1	1	1	3	3	3	3	1	1
Відвідування практичних занять	1	1	1	2	2	3	3	2	2
Відвідування лабораторних занять	1								
Робота на семінарському занятті	10	1	10	3	30	3	30	1	10
Робота на практичному занятті	10	1	10	2	20	3	30	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10								
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25	1	25
Виконання ІНДЗ	30								
Разом		-	54	-	89	-	100	-	65
Максимальна кількість балів: 308									
Розрахунок коефіцієнта: 308/100=3,08									

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
Змістовий модуль 1. Теоретико-методологічні засади кібернетичного права		**9**	**5**
1	Засади формування та становлення кібернетичного права. Роль та місце кібернетичного права в системі права держави	5	3
2	Поняття та зміст методу кібернетичного права	4	2
Змістовий модуль 2. Правове регулювання суспільних відносин у сфері захисту даних		**20**	**5**
3	Поняття та правовий режим інформаційних ресурсів	3	1

№ з/п	Назва теми	Кількість годин	Бали
4	Теоретичні та методологічні основи захисту інформації	3	1
5	Структура законодавства в сфері захисту інформації. Державна система захисту інформації	3	1
6	Правове регулювання суспільних відносин у сфері захисту банківської та комерційної таємниці, персональних даних	6	1
7	Правове регулювання суспільних відносин у сфері охорони державної таємниці та захисту службової інформації	5	1
Змістовий модуль 3. Правове регулювання суспільних відносин у інформаційних системах, інформаційних технологіях і засобах їх забезпечення		**16**	**5**
8	Поняття та правовий режим інформаційних систем, інформаційних технологій і засобів їх забезпечення	3	1
9	Правове регулювання суспільних відносин у сфері технічного захисту інформації	3	1
10	Правове регулювання суспільних відносин у сфері криптографічного захисту інформації	3	1
11	Правове регулювання суспільних відносин у сфері захисту інформації в інформаційно-телекомунікаційних системах	3	1
12	Правове регулювання баз даних, інформаційних систем, відносин, що формуються під час використання хмарних обчислень та віртуальних активів	4	1
Змістовий модуль 4. Кіберзлочинність. Міжнародні стратегії у сфері кібербезпеки		**9**	**5**
13	Правове забезпечення інформаційної безпеки	3	1
14	Міжнародний досвід правового регулювання суспільних відносин в кібернетичній сфері	3	1
15	Кіберзлочинність. Юридична відповідальність за правопорушення у галузі інформаційного законодавства	3	3
	Разом	**56**	**20**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв’язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп’ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі заліку, умовою отримання

якого є отриманням студентом 60 балів (з врахуванням коефіцієнту) за результатами поточного контролю.

Орієнтовний перелік питань для самоконтролю

1. Визначення «кібернетичне (інформаційне) право»
2. Принципи кібернетичного (інформаційного) права
3. Базовий принцип інформаційного права
4. Об’єкт інформаційного права
5. Предмет інформаційного права
6. Визначення (поняття) «метод інформаційного права»
7. Складові методу інформаційного права
8. Методи інформаційного права як науки
9. Методи інформаційного права як галузі права
10. Методи інформаційного права як навчальної дисципліни
11. Визначення «імперативного методу правового регулювання інформаційних відносин»
12. Визначення «диспозитивного методу правового регулювання інформаційних відносин»
13. Складові імперативного методу правового регулювання інформаційних відносин
14. Складові диспозитивного методу правового регулювання інформаційних відносин
15. Практичне значення застосування імперативного та диспозитивного методів
16. Класифікація відносин в інформаційній сфері та їх склад
17. Визначення «інститут інформаційного права»
18. Склад основних інститутів інформаційного права відповідно до процесу створення інформації
19. Склад основних інститутів інформаційного права відповідно до процесу поширення інформації
20. Склад основних інститутів інформаційного право відповідно до процесу забезпечення мінімізації збитку від несанкціонованого поширення, використання і знищення інформації
21. Склад інституту захисту інформації
22. Визначення «захист інформації»
23. Основні принципи інформаційних відносин
24. Основні напрями державної інформаційної політики
25. Основні види інформаційної діяльності
26. Види інформації за змістом
27. Види інформації за порядком доступу
28. Види інформації з обмеженим доступом
29. Визначення «захист інформації в інформаційно-телекомунікаційній системі»
30. Визначення «комплексна система захисту інформації»
31. Визначення «технічний захист інформації»
32. Суб’єкти відносин, пов’язаних із захистом інформації в інформаційно-телекомунікаційних системах
33. Визначення «інформаційний ресурс»
34. Визначення «національний інформаційний ресурс»
35. Визначення «інформаційний продукт (продукція)»
36. Суб’єкти інформаційних відносин
37. Правовий режим інформаційних ресурсів
38. Мета організаційно-правового забезпечення захисту інформації
39. Зміст організаційно-правового забезпечення захисту інформації
40. Система документів організаційно-правового забезпечення захисту інформації
41. Джерела кібернетичних загроз
42. Різновиди кіберзлочинів
43. Зміст Конвенції Ради Європи про кіберзлочинність
44. Мета Конвенції Ради Європи про кіберзлочинність
45. Об’єкти кіберзлочинів відповідно до Конвенції Ради Європи про кіберзлочинність

46. Класифікація кіберзлочинів відповідно до Конвенції Ради Європи про кіберзлочинність
47. Зміст злочинів проти конфіденційності, цілісності і доступності комп'ютерних даних та систем відповідно до Конвенції Ради Європи про кіберзлочинність
48. Зміст злочинів, пов'язаних з використанням комп'ютерів, відповідно до Конвенції Ради Європи про кіберзлочинність
49. Визначення «злочину» відповідно до Кримінального кодексу України
50. Кримінальна відповідальність за скоєння кіберзлочинів
51. Адміністративна відповідальність за скоєння правопорушень
52. Визначення «адміністративного правопорушення» відповідно до Кодексу України про адміністративні правопорушення
53. Зміст методу семантичного аналізу

Шкала відповідності оцінок

Рейтингова оцінка	**Сума балів за всі види навчальної діяльності**	**Значення оцінки**
A	90-100	Відмінно — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	Дуже добре - достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	Добре - в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	Задовільно - посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	Достатньо - мінімально можливий допустимий рівень знань (умінь)
FX	35-59	Незадовільно з можливістю повторного складання - незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	Незадовільно з обов'язковим повторним вивченням курсу - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7. Навчально-методична картка дисципліни

Разом: 120 год., лекції – 24 год., семінарські заняття – 16 год., практичні роботи – 16 год., модульний контроль – 8 год., самостійна робота – 56 год.

Модулі (назви, бали)	Змістовий модуль 1 Теоретико-методологічні засади кібернетичного права (54 бали)		Змістовий модуль 2. Правове регулювання суспільних відносин у сфері захисту даних (89 балів)					Змістовий модуль 3. Правове регулювання суспільних відносин у інформаційних системах, інформаційних технологіях і засобах їх забезпечення (100 балів)					Змістовий модуль 4. Кіберзлочинність. Міжнародні стратегії у сфері кібербезпеки (65 балів)	
Лекції (теми, бали)	Засади формування та становлення кібернетичного права. Роль та місце кібернетичного права в системі права держави (1 бал)	Поняття та зміст методу кібернетичного права (1 бал)	Інформація та її види. Поняття та правовий режим інформаційних ресурсів (1 бал)	Теоретичні та методологічні основи захисту інформації (1 бал)	Структура законодавства в сфері захисту інформації. Державна система захисту інформації (1 бал)	Правове регулювання суспільних відносин у сферах захисту банківської, комерційної, державної таємниць, службової інформації та персональних даних (1 бал)		Поняття та правовий режим ІС, ІТ і засобів їх забезпечення (1 бал)	Правове регулювання суспільних відносин у сфері технічного та криптографічного захисту інформації (1 бал)		Правове регулювання суспільних відносин у сфері захисту інформації в інформаційно-телекомунікаційних системах (1 бал)	Правове регулювання суспільних відносин при застосуванні хмарних технологій (1 бал)	Інформаційна безпека. Міжнародний досвід правового регулювання суспільних відносин в кібернетичній сфері (1 бал)	Кіберзлочинність. Класифікація правопорушень у сфері ІТ. Відповідальність за правопорушення у сфері ІТ (1 бал)
Семінарські заняття (теми, бали)	Поняття та система кібернетичного права (11 балів)		Організаційне забезпечення захисту інформації на підприємствах та організаціях (11 балів)			Організація захисту комерційної таємниці та персональних даних на підприємствах, установах та організаціях. (11 балів)	Організація охорони державної таємниці та службової інформації на підприємствах, установах та організаціях (11 балів)		Організація ТЗІ на підприємствах, установах та організаціях (11 балів)	Організація КЗІ на підприємствах, установах та організаціях (11 балів)	Організація захисту інформації в інформаційно-телекомунікаційних системах (11 балів)			Класифікація правопорушень у сфері ІТ. Відповідальність за правопорушення у сфері ІТ (11 балів)
Практичні роботи (теми, бали)		Система методів і принципів інформаційного права (11 балів)		Застосування методів кібернетичного права під час здійснення організаційних заходів щодо захисту інформації на підприємствах, установах та організаціях		Організація захисту банківської таємниці на підприємствах, установах та організаціях (11 балів)		Поняття та правовий режим ІС, ІТ і засобів їх забезпечення (11 балів)			Правове регулювання інформаційних відносин у сфері телекомунікацій в Україні (11 балів)	Організація захисту інформації в мережі Інтернет (11 балів)	Міжнародний досвід правового регулювання суспільних відносин в кібернетичній сфері (11 балів)	Семантичний аналіз відповідності статей Конвенції Ради Європи про кіберзлочинність статтям КК України та Кодексу України про АП (11 балів)
Самостійна робота	Самостійна робота 1 (5 балів)		Самостійна робота 2 (5 балів)					Самостійна робота 3 (5 балів)					Самостійна робота 4 (5 балів)	
Модульний контроль	Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)					Модульна контрольна робота 3 (25 балів)					Модульна контрольна робота 4 (25 балів)	
Підсумковий контроль (вид, бали)	Залік (100 балів)													

8. Рекомендовані джерела

Базова:

1. Бурячок В.Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа]; за заг. ред. д-ра техн, наук, професора В. Б. Толубка. - К.: ДУТ, 2015- 288 с.

2. Присяжнюк М.М., Марущак А.І., Мельник Д.С., Остроухов В.В., Гуцалюк М.В., Ткаченко О.П. Організаційно-правові основи забезпечення кібербезпеки: підручник; за заг. ред. М.М. Присяжнюка. - К.: Видавництво Ліра-К, 2023 – 320 с.

3. Селезньова О.М. Теоретико-методологічні основи інформаційного права України : [монографія] / О. М. Селезньова. - Чернівці: Місто, 2014. - 408 с.

4. Загальна теорія держави і права: [Підр. для студентів юрид. вищих навчальних закладів] / М.В. Цвік, О.В. Петришин, Л.В. Авраменко та ін.; За ред. д-ра юрид. наук, проф., акад. АПрН України М.В. Цвіка, д-ра юрид. наук, проф., акад. АПрН України О.В. Петришина. — Харків: Право, 2011. — 584 с.

5. Баранов О.А. Інститути інформаційного права / О.А. Баранов // Правова інформатика. - 2006. -№ 3. -С. 39-45.

6. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи [Текст]/О.А. Баранов. - К.: Видавничий дім “СофтПрес”, 2005. — 316 с.

7. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 [Електронний ресурс]. Режим доступу: http://zakon5. rada.gov. ua/laws/show/994_5 75.

8. Орлов Ю.Ю. Реалізація вимог міжнародної Конвенції про кіберзлочинність у законодавстві України [Текст]. - // Науковий вісник Національної академії внутрішніх справ. - 2011. -№6. - С. 3-9.

9. Кодекс України про адміністративні правопорушення (статті 1 - 212-20). Верховна Рада УРСР; Кодекс України, Закон, Кодекс від 07.12.1984 № 8073-X [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/la-ws/show/80731-10.

10. Кримінальний кодекс України. Верховна Рада України; Кодекс України, Кодекс, Закон від 05.04.2001 № 2341-III [Електронний ресурс]. Режим доступу: http://zakon3. rada. gov. ua/laws/show/2341-14.

11. Закон України «Про Національну програму інформатизації» [Електронний ресурс]. Режим доступу: http://zakon3.rada.gov.ua/laws/show/74/98-ep.

12. Закон України «Про інформацію», Верховна Рада України; Закон від 02.10.1992 №2657-XII [Електронний ресурс]. Режим доступу: http://zakon3. rada.gov. ua/laws/show/2657-12.

13. Бєлєвцева В.В. Правовий режим інформаційних ресурсів / В.В. Бєлєвцева // Інформація і право. - 2011. -№3(3). - С. 41-46.

14. «Типова інструкція з діловодства у центральних органах виконавчої влади, Раді міністрів Автономної Республіки Крим, місцевих органах виконавчої влади», зате, постановою Кабінету Міністрів України від ЗО листопада 2011 р. № 1242 [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov.ua/laws/show/1242-2011-n/page.

15. Закон України «Про електронні документи та електронний документообіг», Верховна Рада України; Закон від 22.05.2003 № 851-IV [Електронний ресурс]. Режим доступу: http://zakon5. rada. gov. ua/laws/show/851-15.

16. «Про затвердження Типового порядку здійснення електронного документообігу в органах виконавчої влади», Кабінет Міністрів України; Постанова, Порядок, Форма типового документа [...] від 28.10.2004 № 1453 [Електронний ресурс]. Режим доступу: http://zakon3. rada.gov. ua/laws/show/1453-2004-n.

17. Закон України «Про електронний цифровий підпис», Верховна Рада України; Закон від 22.05.2003 № 852-IV [Електронний ресурс]. Режим доступу: http://zakon5.rada.gov. ua/laws/show/852-15.

18. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. - Київ: ДСТСЗІСБ України, 1999. - 26 с.

19. Правовий захист інформації: Навчальний посібник / Н.І. Логінова, Р.Р. Дробожур. -

Одеса: Фенікс, 2015. - 264 с., іл.

20. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика: монографія / О.А. Баранов. - Київ: Едельвейс, 2014. - 497 с.

21. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : монографія /Д.В. Дубов. - К. : НІСД, 2014. - 328 с.

22. Стратегія кібербезпеки України. Затверджено Указом Президента України від 1 лютого 2022 року № 37/2022. [Електронний ресурс] — Режим доступу: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text .

Додаткова:

1. Брижко В.М. Домінанта праворозуміння та основ понятійно-категоріального апарату інформаційного права [Текст]. // "Інформація і право". - 2011. -№3(3). — С. 5-17.

2. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. І голов, ред. В.Т. Бусел. -К; Ірпінь: ВТФ «Перун», 2005.- 1728 с.

3. Стельмаховська О.І, Шорошев В.В. Міжнародні норми щодо захисту авторських і суміжних прав в мережі Internet [Текст]. - // Науково-технічний журнал «Захист інформації». - 2011. -№1, - С. 5-11.

4. Корнеева Т. Права людини в інформаційному суспільстві. Комунікаційні права: четверте покоління прав людини: тлумачний словник української мови / Т. Корнеева; за ред. проф. В.С. Калачника. - Х. : Прапор, 2002. - 992 с.

5. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. / В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський // Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. — К.: КНТ, 2006. - 280 с. (Серія: Національна і міжнародна безпека).

6. Ліпкан В.А. / В.А. Ліпкан // Національна безпека України. - Навчальний посібник - Кондор- 2006.-552 с.

7. Селезньова О.М. Інститути інформаційного права / О.М. Селезньова // Науковий вісник Херсонського державного університету. Серія «Юридичні науки». - 2014. - Вип. 3. -Т. 2. - С. 240-244.

8. Баранов О.А. Методи інформаційного права / О.А. Баранов // Правова інформатика. - 2007. -№ 4. - С. 8-12.

9. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України /ДВ. Дубов, М.А. Ожеван. — К. : НІСД, 2011. -31с.

10. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В.Дубов, М.А.Ожеван.- К: НІСД 2011. - 30 с.

9. Інформаційні ресурси

1. Законодавство України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/main/index
2. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/index
3. Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України [Електронний ресурс]. – Режим доступу: https://cert.gov.ua
4. Інформаційний перелік документів Фонду нормативних документів у сфері технічного та криптографічного захисту інформації. [Електронний ресурс] – Режим доступу: http://www.dsszzi. gov. ua/dsszzi/control/uk/publish/article?art_id=89740&cat_id=89734