Державна наукова установа
«Інститут інформації, безпеки і права
Національної академії правових наук України»

ЗАТВЕРДЖЕНО
Директор ДНУ ІІБП НАПрН України
_____ В.І.Пилипчук
«09» вересня 2024р.

ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

РОБОЧА НАВЧАЛЬНА ПРОГРАМА

підготовки аспірантів із спеціальності 081 «Право»

Укладач: Фурашев В.М.,
кандидат технічних наук, старший науковий співробітник, доцент

Ухвалено Вченою радою
ДНУ ІІБП НАПрН України
Протокол №9 від 04.09.2024

Київ, 2024

Анотація: Навчальна програма дисципліни «Проблеми правового забезпечення інформаційної безпеки» містить відомості щодо мети та завдань дисципліни, її зв'язок з іншими навчальними дисциплінами, визначає розподіл навчального часу на різні види аудиторних занять та самостійну роботу Аспіранта. Наведено перелік тем лекцій і практичних занять, а також розкрито їх структуру. Містяться методичні рекомендації щодо вивчення дисципліни, перелік питань для самоконтролю аспіранта до кожної теми курсу, а також підготовки до підсумкового контролю (заліку), список нормативних актів, основної та додаткової літератури.

Abstract: The curriculum of the discipline «Legal foundations of information security» contains information about the aims and tasks of studying this subject, its links with other academic disciplines, determines the distribution of time for different types of classroom activities and independent work of the student. The list of topics of lectures and practical exercises is contained, as well as their structure is revealed. The methodological recommendations for studying the discipline are outlined, a list of questions for the self-control of the student on each topic of the course, as well as preparation for the final control, a list of normative acts, basic and additional literature is offered.

ЗМІСТ

1. Опис навчальної дисципліни

<table>
<tr><th>Галузь знань, напрям підготовки, освітньо-кваліфікаційний рівень</th><th>Загальні показники</th><th>Характеристика кредитного модуля</th></tr>
<tr><td>Галузь знань:
08 «Право»</td><td>Назва дисципліни, до якої належить кредитний модуль:
«Проблеми правового забезпечення інформаційної безпеки»</td><td>Форма навчання:
«Заочна»</td></tr>
<tr><td>Спеціальність:
081 «Право»</td><td>Кількість кредитів ECTS
« 4 »</td><td>Статус кредитного модуля
«II Вибіркова компонента»</td></tr>
<tr><td>-</td><td>Кількість розділів:
« 2 »</td><td>Цикл, до якого належить кредитний модуль:
«Навчальні дисципліни за напрямом дослідження»</td></tr>
<tr><td></td><td></td><td>Рік підготовки:
«2024-2025 н.р.»</td></tr>
<tr><td rowspan="3">Ступень вищої освіти:
«Доктор філософії»</td><td>Загальна кількість годин
« 120 »</td><td>Лекції: «18 год.»
Практичні: «18 год.»</td></tr>
<tr><td rowspan="2"></td><td>Самостійна робота аспіранта: «84 год.»</td></tr>
<tr><td>Вид та форма семестрового контролю:
«Залік»</td></tr>
</table>

2. Мета та завдання навчальної дисципліни

2.1. Вивчення правових основ інформаційної безпеки аспірантами спрямоване на досягнення:

а) *загальноосвітньої мети*:

- підвищення правової культури та ерудиції випускників, оволодіння ними основоположними знаннями у сфері інформаційної безпеки та основними правовими механізмами її забезпечення;
- одержання теоретичних і практичних знань, умінь, навичок та інших компетентностей, достатніх для продукування нових оригінальних ідей щодо розв'язання комплексних проблем у сфері правового забезпечення інформаційної безпеки;

б) *науково-методологічної мети*:

- набуття первісних знань та умінь ефективного та безпекового поводження з інформацією незалежно від її походження та виду;
- опанування необхідною науково-методологічною підготовкою, яка забезпечує розпізнавання об`єктів та носіїв інформаційної небезпеки, а також бачення проблем правового характеру у сфері забезпечення інформаційної безпеки, що реально або потенційно можуть виникнути під час здійснення професійних обов`язків за обраною спеціальністю та пошуку шляхів їх розв'язання, застосовуючи навички творчого мислення та самовдосконалення свого професійного рівня;
- розвитку критичного мислення, що базується на здатності вільно оперувати понятійними категоріями, логічними процедурами й методами прирощення нового наукового знання вирішення проблемних питань правового забезпечення інформаційної безпеки;

в) *виховної мети*:

- формування відданості ідеям істини, добра, справедливості і законності, почуття відповідальності перед людиною, суспільством і державою.

2.2. Основними завданнями вивчення дисципліни «Проблеми правового забезпечення інформаційної безпеки» є:

- комплексний розгляд витоків та джерел інформаційної небезпеки - властивостей інформації та впливу інформації на свідомість та поведінку людини, суспільства, а також сучасних механізмів та інструментаріїв маніпулювання свідомістю;
- комплексний розгляд трансформаційних процесів, які відбуваються в системах забезпечення інформаційної і кібернетичної безпеки у національних та міжнародної системах безпеки;
- опанування аспірантами структурою та основними положеннями національного законодавства як правової бази забезпечення інформаційної безпеки людини, суспільства, держави, особливо в умовах інформаційного суспільства;
- опанування аспірантами законодавче визначеним понятійним апаратом у сфері інформаційної безпеки та кібербезпеки;
- ознайомлення аспірантів з тенденціями, які очікуються у сфері інформаційної безпеки та кібербезпеки.

2.3. Згідно з вимогами освітньо-професійної програми аспіранти повинні:

знати:

- сутності основних понять, їх тотожностей та відмінностей у сфері інформаційної безпеки;
- взаємозв'язок інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;

- основи державної та міжнародної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки;
- основні принципи та правила поводження з інформацією;
- реальні та потенційні загрози у сфері інформаційної безпеки та законодавчі шляхи їх запобігання;
- основні методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;
- основні положення юридичної відповідальності за правопорушення в інформаційній сфері;
- зміст основних міжнародних договорів з питань інформаційної безпеки;
- основні проблеми правового забезпечення інформаційної безпеки;

вміти :

- орієнтуватися у цілях та завданнях інформаційних потоків та конкретної інформації;
- орієнтуватися у процесах які відбуваються у сферах забезпечення національної та міжнародної безпеки;
- орієнтуватися у національному та міжнародному законодавстві, з регулювання інформаційних правовідносин та відшукувати необхідні нормативно-правові акти, та інформаційно-правові положення чинного законодавства, що стосуються питань забезпечення інформаційної безпеки;
- застосовувати зазначені акти та інформаційно-правові положення у практичної діяльності, у тому числі, і під час розробки, впровадження та використання інформаційних технологій;
- знаходити протиріччя та не вирішені питання правового регулювання суспільних відносин у сфері забезпечення інформаційної безпеки з метою їх вирішення;
- орієнтуватися в положеннях адміністративного та кримінального права, які спрямовані на забезпечення інформаційної безпеки;

досвід:

- свідомого поводження з інформацією в умовах використання сучасних інформацйно-комунікаційних засобів та враховування отриманих знань у практичної діяльності за обраної спеціальності.

Згідно з вимогами освітньо-наукової програми навчальна дисципліна спрямована на формування таких **програмних компетентностей:**

Інтегральна компетентність (ІК) полягає у: здатності продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері права, застосовувати методологію наукової та педагогічної діяльності, проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

***Загальні компетентності (ЗК) зумовлюють*:**

ЗК01. Здатність генерувати нові ідеї (креативність).

ЗК02. Здатність розробляти наукові проєкти та управляти ними.

ЗК04. Здатність усно і письмово презентувати результати власного наукового дослідження українською та іноземною мовами, глибоко розуміти іншомовні наукові та професійні тексти за напрямом досліджень.

Спеціальні(фахові) компетентності (СК):

СК01. Здатність планувати та виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі права та дотичних до неї міждисциплінарних напрямах і можуть бути опубліковані у провідних наукових виданнях з права та суміжних галузей.

СК02. Здатність застосовувати методи правового і міждисциплінарного дослідження, виявляти їх евристичні можливості та межі, використовувати релевантний дослідницький інструментарій.

СК03. Здатність здійснювати науково-педагогічну діяльність у вищій освіті та проєктах правничої освіти у системі освіти дорослих.

СК04. Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру у сфері права та забезпечувати якість виконуваних досліджень; дотримання права інтелектуальної власності та стандартів академічної доброчесності.

СК05. Здатність моделювати оптимальні варіанти вирішення складних правових проблем, прогнозувати можливі наслідки їх реалізації.

СК06. Здатність здійснювати експертну діяльність у сфері права.

СК07. Здатність виявляти нові інституційні етичні виклики та етичні виклики в житті суспільства і пропонувати для них правові механізми розв'язання.

2.4 Згідно з вимогами освітньо-наукової програми навчальна дисципліна спрямована на формування таких **програмних результатів навчання:**

ПРН01. Мати передові концептуальні та методологічні знання у сфері права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень, отримання нових знань та здійснення інновацій.

ПРН03. Застосовувати у фаховій діяльності знання та розуміння системи права, історії світової та української правової думки, сучасної правової доктрини, а також основних напрямів та провідних тенденцій у розвитку права.

ПРН04. Формулювати і перевіряти гіпотези; використовувати для обґрунтування висновків належні аргументи, зокрема, результати теоретичного аналізу, прикладних досліджень, наявні наукові джерела; аналізувати досліджувану проблему з урахуванням широкого правового та загальносоціального контекстів.

ПРН05. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного наукового інструментарію, критично аналізувати результати власних досліджень і результати інших дослідників у контексті усього комплексу передових концептуальних і методологічних знань щодо досліджуваної проблеми з дотриманням стандартів академічної та професійної етики.

ПРН06. Розуміти загальні принципи та методи юридичної науки, а також методологію наукових досліджень, застосувати їх у власних дослідженнях у сфері права та у викладацькій практиці.

ПРН07. Застосовувати сучасні інструменти і технології пошуку, оброблення, аналізу й збереження даних та інформації, статистичні методи аналізу даних великого обсягу та складної структури, спеціалізовані програмне забезпечення, бази даних та інформаційні системи у науковій, викладацькій, правотворчій та правозастосовній діяльності.

ПРН10. Готувати правові висновки, пропозиції та рекомендації за результатами правового дослідження.

ПРН11. Здійснювати доктринальне тлумачення норм національного, міжнародного та права Європейського Союзу, здійснювати порівняльний аналіз правових явищ та процесів у різних правових системах.

3. Структура кредитного модуля

№ п\п	Змістовні модулі	Кількість годин				
		Всього	Лекції	Практ. занят.	Індив. занят.	Самост. робота
1	2	3	4	5	6	7
	Розділ 1. Сутність інформаційної безпеки у сучасності.					
1.1.	Трансформаційні процеси в системах забезпечення національної та міжнародної безпеки. ❑	6	2	-	-	4
1.2.	Інформація як джерело небезпеки. ❑	6	2	-	-	4
1.3.	Інформаційна та кібернетична безпека. ❑	6	2	2	-	2
1.4.	Об`єкти та суб`єкти інформаційної небезпеки. ❑	8	2	2	-	4
1.5.	Інформаційна діяльність, інформаційні ресурси як об'єкт небезпеки. ❑	11	-	2	-	9
	Тестування на останньому практичному (семінарському) занятті (до 25 хв.)					
	Всього за розділ:	**37**	**8**	**6**	**-**	**23**
	Розділ 2. Основні чинники, які формують та впливають на ефективність правового забезпечення інформаційної безпеки					
2.1.	Інформаційна безпека як об'єкт правовідносин. ❑	6	2	-	-	4
2.2.	Інформаційний суверенітет. ❑	8	-	2	-	6
2.3.	Інтернет і інформаційна безпека. ❑	6	-	2	-	4
2.4.	Національна та міжнародна безпека. ❑	10	2	-	-	8
2.5.	Державна політика у сфері інформаційної безпеки. ❑	10	-	2	-	8
2.6.	Правове забезпечення захисту інформації. ❑	11	2	2	-	7
2.7.	Особливості сучасних інформаційних суспільних відносин. ❑	9	-	2	-	7
2.8.	Правова відповідальність за правопорушення в інформаційній сфері. ❑	10	2	2	-	6
2.9.	Правові проблеми забезпечення інформаційної безпеки ❑	9	2	-	-	7
	Тестування на останньому практичному (семінарському) занятті (до 25 хв.)					
	Всього за розділ:	**79**	**10**	**12**	**-**	**57**
	Залік:	4	-	(2)	-	4
	Разом:	**120**	**18**	**18**	**-**	**84**

❑ Лекція викладається із застосуванням мультимедійних засобів навчання.

4. Лекційні заняття

Розділ І. Сутність інформаційної безпеки у сучасності.

Лекція 1:

Тема 1.1. Трансформаційні процеси в системах забезпечення національної та міжнародної безпеки.

Перелік основних питань:

1. Предмет інформаційної безпеки.
2. Завдання інформаційної безпеки.
3. Тенденції та їх витоки трансформації процесів організації та проведення локальних та регіональних міждержавних конфліктів та війн.
4. Відображення цих процесів у національних та міжнародних нормативно-правових, доктринальних та стратегічних актах.

Питання для самоперевірки:

1. Основні особливості сучасного періоду з точки зору безпеки людини.
2. Основні особливості сучасного періоду з точки зору безпеки суспільства.
3. Основні особливості сучасного періоду з точки зору безпеки держави.
4. Що є предметом інформаційної безпеки?
5. Основні завдання інформаційної безпеки.
6. Що таке війна?
7. Чим війна відрізняється від збройного конфлікту?
8. Основні види війн.
9. Основні цілі та завдання сучасних війн?
10. У зв`язку з чім відбуваються трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн?
11. Які основна спрямованість трансформаційних процесів організації та проведення локальних та регіональних конфліктів та війн?
12. Які основні базові положення Воєнної доктрини України, які відображають трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн?
13. Які основні базові положення Стратегії національної безпеки України, які відображають трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн?
14. Які основні базові положення Доктрини інформаційної безпеки України, які відображають трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн?
15. Які основні базові положення Стратегії кібербезпеки України, які відображають трансформаційні процеси організації та проведення локальних та регіональних конфліктів та війн?
16. Законодаче встановлені об`єкти кібербезпеки.
17. Законодаче встановлені об`єкти кіберзахисту.

Література: 1, 4, 5 – 8, 15, 17, 20, 24, 25.

Лекція 2:

Тема 1.2. Інформація як джерело небезпеки.

Перелік основних питань:

1. Природа інформації.
2. Загальне та законодавче визначення поняття «інформація».
3. Властивості інформації.
4. Вплив інформації на свідомість та поведінку людини.
5. Маніпулювання свідомістю - сутність та види маніпуляції.
6. Сутність та прояви інформаційного насильства. Проблемні питання правового запобігання здійсненню інформаційного насильства.

Питання для самоперевірки:

1. У чому полягає сутність поняття «інформація»?
2. Яким чином людина сприймає інформацію?
3. Як законодавство визначає поняття «інформація» та чим це обумовлено?
4. Назовить основні, з точки зору інформаційної безпеки, властивості інформації.
5. Чому говоримо, що інформація апріорі небезпечна?
6. Розкрийте сутність поняття «маніпуляція».
7. Назовить види маніпуляції та розкрийте їх сутність.
8. Розкрийте сутність поняття «насиліе».
9. У чому полягають тотожності та відмінності маніпулювання та інформаційного насильства?
10. У зв`язку з чим виникають проблеми із запобіганням інформаційного насильства правовими методами?

Література: 1, 6, 7, 28, 29.

Лекція 3:

Тема 1.3. Інформаційна та кібернетична безпека.

Перелік основних питань:

1. Визначення поняття «інформаційна безпека».
2. Сутність та визначення понять «кібернетика» та «кібернетичний».
3. Кібернетика як об`єкт небезпеки.
4. Визначення поняття «кібернетична безпека» (кібербезпека).
5. Застосування термінів «інформаційна безпека» та «кібербезпека».

Питання для самоперевірки:

1. Зробить оцінку відображення терміну “інформаційна безпека” у законодавстві України?
2. Коли та у якому законодавчому акті України вперше було надане визначення поняття «інформаційна безпека»?
3. Чому кібернетика є об`єктом небезпеки?
4. У чому полягає сутність поняття «інформаційний простір»? Визначьте його властивості.
5. У чому полягає сутність поняття «кібернетичний простір» («кіберпростір»)? Визначьте його властивості.
6. Розкрійте сутність поняття «кібербезпека»
7. У чому полягають тотожності та відмінності понять «інформаційна безпека» та «кібербезпека»?

8. Означьте межу коректності застосування термінів «інформаційна безпека» та «кібербезпека».
9. Розкрийті взаємозв`язок інформаційної безпеки та кібербезпеки.
10. Зробить експрес-оцінку сучасного стану забезпеченості інформаційної безпеки та кібербезпеки в Україні.

Література: 1, 4, 7, 21, 23, 24, 25.

Лекція 4:

Тема 1.4. Об`єкти та суб`єкти інформаційної небезпеки.

Перелік основних питань:

1. Визначення об'єктів інформаційної небезпеки та їх обґрунтування.
2. Ієрархія об'єктів інформаційної небезпеки.
3. Сутність, поняття та правове визначення інформаційної діяльності.
4. Складові інформаційної діяльності.
5. Інформаційна діяльність як об`єкт небезпеки.

Питання для самоперевірки:

1. Що розуміється під поняттями «об'єкт» та «суб`єкт»?
2. Що розуміємо під поняттям «інформаційна небезпека»?
3. За якими критеріями або показниками визначаються об'єкти інформаційної небезпеки?
4. Розкриття сутності інформаційної діяльності.
5. Розкриття складових інформаційної діяльності.
6. Визначте основні напрями інформаційної діяльності.
7. Визначте основні види інформаційної діяльності.
8. Визначення суб`єктів інформаційної діяльності.
9. Чому інформаційна діяльність є об`єктом небезпеки?
10. Визначте ієрархію об'єктів інформаційної небезпеки.
11. Як розуміти поняття «інформаційне забруднення».
12. Що розуміємо під поняттям «інформаційний проду́кт»?

Література: 1, 4, 5 - 7, 11, 15, 20, 25, 31.

Розділ ІІ. Основні чинники, які формують та впливають на ефективність правового забезпечення інформаційної безпеки

Лекція 5:

Тема 2.1. Інформаційна безпека як об'єкт правовідносин.

Перелік основних питань:

1. Сутність понять «суспільні відносини» та «правовідносини».
2. Життєво важливі інтереси в інформаційній сфері.
3. «Національні інтереси» - поняття та сутність.
4. «Національні інтереси в інформаційній сфері» - поняття та сутність.
5. Взаємозв`язок інформаційної безпеки з правовідносинами.

Питання для самоперевірки:

1. В чому полягає сутність супільних відносин?
2. В чому полягає сутність правовідносин?
3. Хто є суб`єктами правовідносин?
4. Які основні ознаки правовідносин?
5. У якому випадку суспільні відносини «переходять» до категорії правовідносин?
6. Що розуміємо під поняттям «життєво важливі інтереси»?
7. Що розуміємо під поняттям «інформаційна сфера»?
8. Що розуміємо під поняттям «життєво важливі інтереси» в інформаційної сфері?
9. Що розуміємо під поняттям «національні інтереси»?
10. Що розуміємо під поняттям «національні інтереси» в інформаційної сфері?

Література: 1, 6, 10, 14, 17, 18, 21, 24, 27, 32.

Лекція 6:
Тема 2.4. Національна та міжнародна безпека.

Перелік основних питань:

1. Поняття «національна безпека» та «міжнародна безпека».
2. Складові національної та міжнародної безпеки.
3. Характерні особливості та вплив кожної складової національної та міжнародної безпеки на стан забезпечення загальної безпеки.
4. Реальні та потенційні загрози в інформаційній сфері.
5. Сутність понять «інформаційний вплив», «інформаційна операція», «інформаційна війна», «інформаційна зброя».
6. Роль та значення корупції для забезпечення національної та міжнародної безпеки.

Питання для самоперевірки:

1. Що розуміємо під поняттям «національна безпека»?
2. Визначити основні показники національної безпеки
3. Що розуміємо під поняттям «міжнародна безпека»?
4. Визначити основні складові національної безпеки.
5. Які є системи міжнародної безпеки? Які є гарантії та забезпечення їх виконання в системі міжнародної безпеки?
6. Які загрози в інформаційної сфері вбачаються реальними на даному етапі розвитку України?
7. Які загрози в інформаційної сфері вбачаються потенційними на даному етапі розвитку України?
8. Якій взаємозв`зв'язок національної та міжнародної безпеки на сучасному етапі розвитку людства?
9. Які загрози в інформаційної сфері вбачаються реальними в системі забезпечення міжнародної безпеки?
10. Які загрози в інформаційної сфері вбачаються потенційними в системі забезпечення міжнародної безпеки?
11. У чому полягає сутність поняття «інформаційний вплив»?
12. У чому полягає сутність поняття «інформаційна операція»?
13. У чому полягає сутність поняття «інформаційна війна»?
14. У чому полягає сутність поняття «інформаційна зброя»?
15. Що розуміємо під поняттям «корупція»?
16. Яку роль відіграє корупція в системах забезпечення національної та міжнародної безпеки?

Література: 1, 3, 4 – 8, 14, 16, 17 - 19, 25, 28, 30.

Лекція 7:

Тема 2.6. Правове забезпечення захисту інформації.

Перелік основних питань:

1. Сутність та визначення понять «інформаційна безпека» та «безпека інформації».
2. Нормативно-правова база забезпечення захисту інформації.
3. Основна спрямованість національного законодавства у сфері забезпечення захисту інформації.
4. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».
5. Основні положення Закону України «Про захист персональних даних».

Питання для самоперевірки:

1. Що розуміємо під поняття «безпека інформації»?
2. У чому полягає основна відмінність понять «інформаційна безпека» та «безпека інформації»?
3. Окреслити склад основної системоутворюючої законодавчої бази в сфері захисту інформації.
4. У чому полягає основна спрямованість національного законодавства у сфері забезпечення захисту інформації.
5. Що є об`єктом захисту в інформаційно-телекомунікаційних системах?
6. Хто є суб'єктами відносин, пов'язаних із захистом інформації в інформаційно-телекомунікаційних системах?
7. Що розуміємо під поняттям «персональні дані»?
8. Що є первинними джерелами відомостей про фізичну особу?
9. Що розуміємо під поняттям «володілець персональних даних»?
10. Що розуміємо під поняттям «розпорядник персональних даних»?
11. Що розуміємо під поняттям «суб'єкт персональних даних»?
12. Умови поширення персональних даних.
13. Основні законодавчі вимоги щодо організації забезпечення захисту персональних даних.

Література: 1, 2, 9, 10, 12, 13, 15, 17, 18, 22, 26, 27, 29.

Лекція 8:

Тема 2.8. Правова відповідальність за правопорушення в інформаційній сфері.

Перелік основних питань:

1. Поняття кіберзлочинності.
2. Про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. № 994-575.
3. Основні положення правового забезпечення захищеності інформації та відповідальності за її порушення.
4. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення.
5. Кримінально-правове забезпечення розвитку інформаційного суспільства.
6. Основні положення нормативно-правових актів міжнародного права та ЄС у сфері забезпечення інформаційної безпеки.

Питання для самоперевірки:

1. Що розуміємо під поняттям «злочин»?
2. Що розуміємо під поняттям «злочинність»?
3. Які основні ознаки злочинності?
4. Що розуміємо під поняттям «кіберзлочинність»?
5. Що розуміємо під поняттям «комп`ютерна злочинність»?
6. У чому полягають тотожності та відмінності понять «кіберзлочинність» та «комп`ютерна злочинність»?
7. Яка класифікація комп`ютерної злочинності прийнятв у Євросоюзі?
8. Спрямованість кіберзлочинів, за які в Україні передбачена кримінальна відповідальність.
9. У яких випадках особа, яка здійснела правопорушення в інформаційної сфері, не підлягає юридичній відповідальності?

Література: 1, 3, 5, 6, 9, 10, 12, 13, 16, 19, 21, 28, 29.

Лекція 9:

Тема 2.9. Правові проблеми забезпечення інформаційної безпеки.

Перелік основних питань:

1. Права і свобода людини, громадянина та їх обов'язки в інформаційній сфері.
2. Права суспільства та обов'язки держави в інформаційній сфері.
3. Дилема забезпечення прав і свобод людини, громадянина та прав суспільства із забезпеченням інформаційної безпеки.

Питання для самоперевірки:

1. У чому полягають права і свобода людини, громадянина та їх обов'язки в інформаційній сфері?
2. Яким чином гарантується дотримання встановлених державою прав і свобод людини, громадянина?
3. У чому полягають обов'язки людини, громадянина в інформаційній сфері?
4. Яким чином держава контролює виконання людино, громадянином своїх обов`язків в інформаційної сфері?
5. Чим та підставі чого встановлюються обов'язки людини, громадянина в інформаційній сфері?
6. В чому полягають права суспільства в інформаційній сфері?
7. В чому полягають обов'язки держави в інформаційній сфері?
8. Чому говоримо «права і свобода людини, громадянина та їх обов'язки», «права суспільства» та «обов'язки держави»?
9. Сутність поняття «цензура».
10. Причини та сутність правових проблем забезпечення інформаційної безпеки.

Література: 1, 5 - 8, 14, 28.

5. Теми практичних (семінарських) занять

Семінарське заняття 1:

Тема 1.3. Інформаційна та кібернетична безпека.

Питання для розгляду:

1. Визначення поняття «інформаційна безпека».
2. Сутність та визначення понять «кібернетика» та «кібернетичний».
3. Кібернетика як об`єкт небезпеки.
4. Визначення поняття «кібернетична безпека» (кібербезпека).
5. Застосування термінів «інформаційна безпека» та «кібербезпека».

Завдання на СРС:

1. Відображення терміну «інформаційна безпека» у законодавстві України.
2. Законодавче визначення поняття «інформаційна безпека».
3. Зв`язок сутності понять «кібернетика» та «небезпеки».
4. Сутність поняття «інформаційний простір» та його властивості.
5. Сутність поняття «кібернетичний простір» («кіберпростір») та його властивості.
6. Сутність та визначення поняття «кібербезпека».
7. Взаємозв`язок інформаційної безпеки та кібербезпеки.
8. Ознаки коректності застосування термінів «інформаційна безпека» та «кібербезпека».
9. Основні трансформаційні процеси систем забезпечення інформаційної безпеки та кібербезпеки в Україні.

Література: 1, 4, 5 –8, 15, 17, 20, 23, 24, 25.

Семінарське заняття 2:

Тема 1.4. Об`єкти та суб`єкти інформаційної небезпеки.

Питання для розгляду:

1. Визначення об'єктів інформаційної небезпеки та їх обґрунтування.
2. Ієрархія об'єктів інформаційної небезпеки.
3. Сутність, поняття та правове визначення інформаційної діяльності.
4. Складові інформаційної діяльності.
5. Інформаційна діяльність як об`єкт небезпеки.

Завдання на СРС:

1. Сутність та визначення понять «об'єкт» та «суб`єкт».
2. Сутність поняття «інформаційна небезпека».
3. Критерії/показниками віднесення до об'єктів інформаційної небезпеки.
4. Сутність та визначення поняття «інформаційна діяльність».
5. Складові інформаційної діяльності.
6. Основні напрями інформаційної діяльності.
7. Основні види інформаційної діяльності.
8. Суб`єкти в інформаційної діяльності.
9. Зв`язок інформаційної діяльності з небезпекою.
10. Ієрархія об'єктів інформаційної небезпеки.
11. Сутність поняття «інформаційне забруднення».
12. Сутність та визначення поняття «інформаційний проду́кт».

Література: 1, 6, 7, 28, 29, 31.

Семінарське заняття 3:

Тема 1.5. Інформаційна діяльність, інформаційні ресурси як об`єкт небезпеки

Питання для розгляду:

1. Маніпулювання свідомістю, сутність та види маніпуляції.
2. Взаємозв'язок інформаційної діяльності та інформаційної безпеки.
3. Роль та місце маніпулювання в національних системах державного управління та політичних системах, а також у формуванні та здійсненні міжнародних стосунків.
4. Поняття «інформаційний ресурс».
5. Законодавче визначення типів та видів інформаційних ресурсів.
6. Законодавче забезпечення доступу до інформаційних ресурсів.
7. Законодавче обмеження доступу до інформаційних ресурсів.

Завдання на СРС:

1. Сутність, поняття та правове визначення поняття «інформаційна діяльність».
2. Складові інформаційної діяльності.
3. Засоби та їх структура здійснення інформаційної діяльності.
4. Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.
5. Сутність та визначення поняття «інформаційний ресурс».
6. Значення інформаційних ресурсів.
7. Властивості інформресурсів.
8. Функції інформаційного ресурсу.
9. Інформаційні ресурси спільного користування
10. Національні електронні інформаційні ресурси та їх склад
11. Інформаційні ресурси науково-технічної інформації
12. Законодавче забезпечення доступу до інформаційних ресурсів.
13. Визначення поняття «режим доступу до інформації».
14. Головні характеристики режиму доступу до інформації.
15. Інформація з обмеженим доступом.
16. Законодавче обмеження доступу до інформаційних ресурсів.

Література: 1, 4, 7, 21, 24, 25.

Семінарське заняття 4:

Тема 2.2. Інформаційний суверенітет.

Питання для розгляду:

1. Поняття та сутність інформаційного суверенітету.
2. Шляхи та механізми становлення, розвитку та забезпечення інформаційного суверенітету.
3. Проблемні питання правового забезпечення інформаційного суверенітету

Завдання на СРС:

1. Розкриття сутності та визначення поняття «суверенітет».
2. Розкриття сутності та поняття «інформаційний суверенітет».
3. Основа інформаційного суверенітету.
4. Механізми забезпечення національного інформаційного суверенітету.
5. Окреслення сучасних чинників, які впливають на ступень інформаційної суверенності будь-якої держави.
6. Визначення сучасних та потенційних проблемних питань забезпечення інформаційного суверенітету.
7. Можливі шляхи вирішення проблемних питань забезпечення інформаційного суверенітету.

Література: 1, 4, 5 - 7, 11, 15, 20, 25.

Семінарське заняття 5:
Тема 2.3. Інтернет і інформаційна безпека.

Питання для розгляду:

1. Глобалізація інформаційного простору.
2. Соціальні мережі.
3. Особливості та проблеми реалізації інформаційних правовідносин в Інтернет.

Завдання на СРС:

1. Сутність та визначення поняття «Інтернет».
2. Властивості мережі Інтернет.
3. Розкриття витоків глобалізації інформаційного простору.
4. Оцінка позитивних та негативних наслідків глобалізації інформаційного простору.
5. Вплив глобалізації інформаційного простору на процеси забезпечення інформаційної безпеки людини, громадянина, суспільства та держави.
6. Вплив глобалізації інформаційного простору на процеси забезпечення міжнародної безпеки.
7. Тенденції та спрямованість подальшої глобалізації інформаційного простору.
8. Сутність поняття «соціальна мережа»
9. Оцінка позитивних та негативних наслідків створення та функціонування соціальних мереж.
10. Вплив функціонування соціальних мереж процеси забезпечення інформаційної безпеки людини, громадянина, суспільства та держави.
11. Розкриття особливостей встановлення та реалізації правовідносин в Інтернет.
12. Розкриття проблемних питань встановлення та реалізації правовідносин в Інтернет.

Література: 1, 6, 10, 14, 17, 18, 21, 24, 27, 32.

Семінарське заняття 6:
Тема 2.5. Державна політика у сфері інформаційної безпеки.

Питання для розгляду:

1. Законодавчо визначені складові національної безпеки.
2. Основна спрямованість конкретної складової національної безпеки.
3. Головний чинник забезпечення необхідного стану кожної складової національної

безпеки.
4. Основний чинник, який приманний всім складовим національної безпеки.
5. Реальні та потенційні загрози інформаційній безпеці.
6. Правова база забезпечення інформаційної безпеки (структура системи правового забезпечення інформаційної безпеки, коротка характеристика базових законодавчих актів забезпечення інформаційної безпеки).
7. Права та обов'язки суб'єктів забезпечення інформаційної безпеки.
8. Структурна схема забезпечення інформаційної безпеки.

Завдання на СРС:
1. Сутність та визначення поняття «національна безпека».
2. Розкриття основних показників національної безпеки.
3. Сутність та визначення поняття
4. Сутність та визначення поняття «міжнародна безпека».
5. Розкриття основних складових національної безпеки.
6. Системи міжнародної безпеки.

Гарантії та забезпечення їх виконання в системі міжнародної безпеки.
7. Реальні загрози в інформаційної сфері на даному етапі розвитку України.
8. Потенційні загрози в інформаційної сфері на даному етапі розвитку України.
9. Сучасний взаємозв`зв'язок систем національної та міжнародної безпек.
10. Реальні загрози в інформаційної сфері в системі забезпечення міжнародної безпеки.
11. Потенційні загрози в інформаційної сфері в системі забезпечення міжнародної безпеки.
12. Сутність поняття «інформаційний вплив».
13. Сутність поняття «інформаційна зброя», «інформаційна війна», «інформаційна операція».
14. Сутність та визначення поняття "корупція".
15. Роль корупції в системах забезпечення національної та міжнародної безпеки.

Література: 1, 3, 4 – 8, 14, 16, 17 - 19, 25, 28, 30.

Семінарське заняття 7:
Тема 2.6. Правове забезпечення захисту інформації.

Питання для розгляду:
1. Сутність та визначення понять «інформаційна безпека» та «безпека інформації».
2. Нормативно-правова база забезпечення захисту інформації.
3. Основна спрямованість національного законодавства у сфері забезпечення захисту інформації.
4. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах».
5. Основні положення Закону України «Про захист персональних даних».

Завдання на СРС:
1. Сутність понять «безпека інформації» та «безпечність інформації».
2. Основна відмінність понять «інформаційна безпека» та «безпека інформації».
3. Склад основної системоутворюючої законодавчої бази в сфері захисту інформації.
4. Основна спрямованість національного законодавства у сфері забезпечення захисту інформації.
5. Об`єкти захисту в інформаційно-телекомунікаційних системах?

6. Суб'єкти відносин, пов'язаних із захистом інформації в інформаційно-телекомунікаційних системах?
7. Сутність та визначення поняття «персональні дані»
8. Первинні джерела відомостей про фізичну особу.
9. Сутність та визначення поняття «володілець персональних даних».
10. Сутність та визначення поняття «розпорядник персональних даних».
11. Сутність та визначення поняття «суб'єкт персональних даних».
12. Умови поширення персональних даних.
13. Основні законодавчі вимоги щодо організації забезпечення захисту персональних даних.

Література: 1, 2, 9, 10, 12, 13, 15, 17, 18, 22, 26, 27, 29.

Семінарське заняття 8:

Тема 2.7. Особливості сучасних інформаційних суспільних відносин.

Питання для розгляду:

1. Інформаційно-комунікаційні технології (ІКТ) як об'єкт і предмет правового регулювання.
2. Безпека глобальних інформаційних систем та мереж. Комп'ютерний тероризм: сутність, визначення, прояви.
3. Посилення відповідальності за комп'ютерний тероризм.
4. Інтернет і право: об'єкти та суб`єкти правовідносин.
5. Особливості та проблеми реалізації інформаційних правовідносин в Інтернет. Інформаційна інфраструктура: проблеми правового регулювання.
6. Витоки та сутність кіберсоціалізації. Мережна мобілізація: питання демократії та безпеки. Наслідки кіберсоціалізації.
7. Сутність поняття «кіберцивілізація».
8. Потенційні загрози кіберцивілізації для людства.
9. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки.
10. Правові основи розвитку інформаційних технологій і забезпечення інформаційної безпеки.

Завдання на СРС:

1. Визначення поняття «інформаційна технологія».
2. Визначення поняття «інформаційно-комунікаційна технологія».
3. Що розуміється під поняттям «глобальні інформаційні системи та мережи».
4. Сутність безпеки глобальних інформаційних систем та мереж.
5. Сутність та поняття «комп'ютерний тероризм».
6. Шляхи та засоби боротьби з комп'ютерним тероризмом.
7. Сутність поняття «інформаційна інфраструктура».
8. Об'єкти та суб`єкти правовідносин в мережі Інтернет.
9. Чім викликані та в чому полягають особливості та проблеми реалізації інформаційних правовідносин в Інтернет?
10. Сутність мережної мобілізації.
11. Що мається на увазі під поняттям «кіберсоціалізація»?
12. Наслідки кіберсоціалізації з точки зору розвитку національного та загальносвітового суспільства.
13. Наслідки кіберсоціалізації з точки зору забезпечення інформаційної безпеки.
14. Що мається на увазі під поняттям «кіберцивілізація»?
15. Власне бачення етапності досягнення кіберцивілізації.

16. Реальні та потенційні загрози кіберцивілізації для людства.
17. Основні положення закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки».

Література: 1, 3, 5, 6, 10,12, 13, 16, 19, 21, 28, 29.

Семінарське заняття 9:

Тема 2.8. Правова відповідальність за правопорушення в інформаційній сфері.

Питання для розгляду:

1. Поняття кіберзлочинності.
2. Про кіберзлочинність: Конвенція Ради Європи від 23.11.01 р. № 994-575.
3. Основні положення правового забезпечення захищеності інформації та відповідальності за її порушення (*у відповідності до Кримінального, Кримінального процесуального, Цивільного, Господарського кодексу України та Кодексу України про адміністративні правопорушення).*
4. Адміністративно-правовий захист інформації: проблеми та шляхи вирішення.
5. Кримінально-правове забезпечення розвитку інформаційного суспільства.
6. Основні положення нормативно-правових актів міжнародного права та ЄС у сфері забезпечення інформаційної безпеки.

Завдання на СРС:

1. Сутність та визначення поняття «злочин».
2. Сутність та визначення поняття «злочинність»?
3. Основні ознаки злочинності.
4. Сутність та визначення поняття «кіберзлочинність».
5. Сутність та визначення поняття «комп`ютерна злочинність»?
6. Тотожності та відмінності понять «кіберзлочинність» та «комп`ютерна злочинність».
7. Класифікація комп`ютерної злочинності прийнятв у Євросоюзі.
8. Спрямованість кіберзлочинів, за які в Україні передбачена кримінальна відповідальність.
9. Випадкі коли особа, яка здійснела правопорушення в інформаційної сфері, не підлягає юридичній відповідальності.

Література: 1, 5 - 9, 14, 28.

6. Самостійна робота

Самостійна робота аспіранта передбачає самостійне, на основі зазначених питань для самоперевірки за результатами лекційних занять; питань, віднесених до СРС та нижченаведених питань, а також рекомендованої літератури, опрацювання та засвоєння окремих положень дисципліни. Особливу увагу слід звернути на першоджерела. Покращенню засвоєння такого матеріалу і з'ясуванню питань, що складають певні ускладнення у вивченні в

процесі самостійної роботи аспіранта сприяють індивідуальні консультації. Перевірка рівня засвоєння матеріалу таких тем проводиться в процесі обговорення питань із логічно споріднених тем дисципліни на аудиторних заняттях.

Тема 1.2. Інформація як джерело небезпеки.

Завдання для самостійної роботи аспіранта:

1. Історичні етапи поглядів на розуміння поняття «інформація».
2. Трансформація ролі та значення інформації на різних етапах розвитку людства.
3. Перспективи розвитку та механізми здійснення інформаційного насильства.
4. Механізми впливу інформації на поведінку людини.

Література: 1, 6, 7, 28, 29.

Тема 1.4. Об`єкти та суб`єкти інформаційної небезпеки.

Завдання для самостійної роботи аспіранта:

1. В чому полягають тотожності та відмінності об`єктів інформаційної небезпеки та інформаційної безпеки?
2. Об`єкти інформаційної діяльності.
3. Суб`єкти інформаційної діяльності.
4. Чому інформаційна діяльність є апріорі небезпечною з точки національної безпеки?
5. Спрямованість розвитку інформаційної діяльності.

Література: 1, 6, 7, 28, 29, 31.

Тема 1.5. Інформаційна діяльність, інформаційні ресурси як об`єкт небезпеки.

Завдання для самостійної роботи аспіранта:

1. Сутність та прояви інформаційного насильства.
2. Проблемні питання правового запобігання здійсненню інформаційного насильства.
3. Засоби та їх структура здійснення інформаційної діяльності.
4. Особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.
5. Типи інформаційних ресурсів.
6. Види інформаційних ресурсів.
7. Роль та значення інформаційних ресурсів у розвитку людства.
8. Напрями та перспективи збереження і розвитку інформаційних ресурсів.
9. Тенденції змін у системі доступу до інформаційних ресурсів.

Література: 1, 4, 7, 21, 24, 25.

Тема 2.2. Інформаційний суверенітет.

Завдання для самостійної роботи аспіранта:

1. Загальне розуміння поняття «суверенітет».
2. Чинники які впливають на інформаційний суверенітет.
3. Оцінка стану національного інформаційного суверенітету у сучасних умовах.

Література: 1, 5, 7, 9, 10, 14, 18, 20, 24, 27, 32.

Тема 2.3. Інтернет і інформаційна безпека.

Завдання для самостійної роботи аспіранта:

1. Витоки глобалізації інформаційного простору.
2. Механізми та засоби глобалізації інформаційного простору.
3. Основні принципові наслідки глобалізації інформаційного простору.
4. Витоки та наслідки соціальних мереж.
5. Перспективи розвитку соціальних мереж.

Література: 1, 6, 10, 14, 17, 18, 21, 24, 27, 32.

Тема 2.5. Державна політика у сфері інформаційної безпеки.

Завдання для самостійної роботи аспіранта:

1. Розуміння поняття «національна безпека» у сучасних умовах.
2. Розуміння ролі та місця інформаційної безпеки в системі національної безпеки.
3. Основні положення Стратегії інформаційної безпеки України, затвердженої Указом Президента України від 28.12.2021 р. № 685/2021.
4. Основні положення Стратегії кібербезпеки України, затвердженої Указом Президента України від 26.08.2021 р. № 44/2021.
5. Основні положення Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 р. № 392/2020
6. Основні положення Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. № 537- V.

Література: 1, 3, 4 – 8, 14, 16, 17 - 19, 25, 28, 30.

Тема 2.6. Правове забезпечення захисту інформації.

Завдання для самостійної роботи аспіранта:

1. Структура нормативно-правової бази забезпечення захисту інформації.
2. Основні положення Закону України «Про електронні комунікації» від 16.12.2020 р. № 1089- IX.
3. Основні положення Закону України «Про інформацію» від 02.10.92 р. № 2657-XII.

Література: 1, 2, 9, 10, 12, 13, 15, 17, 18, 22, 26, 27, 29.

Тема 2.7. Особливості сучасних інформаційних суспільних відносин.

Завдання для самостійної роботи аспіранта:

1. Розкриття поняття «інформаційно-комунікаційна технологія» (ІКТ).
2. Розкриття понять «глобальна інформаційна система» та «глобальна мережа».
3. Природа тероризму.
4. Розкриття поняття «соціалізація»
5. Поняття об`єктності та суб`єктності в системі правовідносин.
6. Розкриття поняття «інформаційна технологія».
7. Розкриття поняття «інформаційна інфраструктура».

Література: 1, 3, 5, 6, 10,12, 13, 16, 19, 21, 28, 29.

Тема 2.8. Правова відповідальність за правопорушення в інформаційній сфері.

Завдання для самостійної роботи аспіранта:

1. Основні положення Конвенції Ради Європи « Про кіберзлочинність від 23.11.01 р. № 994-575.
2. Основні положення розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України.

Література: 1, 5 - 9, 14, 28.

7. Контрольні роботи.

Проведення повноцінних контрольних робіт навчальною програмою не передбачається. Перевірка ступеня засвоєння навчального матеріалу проводяться по закінченню вивчення кожного розділу модуля на останньому аудиторному занятті шляхом тестування у письмової формі. Для цього розроблені тестові завдання з охопленням матеріалу розділу. Тестове завдання включає одне питання на яке потрібне надати чітку та лаконічну відповідь, яка розкриває суть поставленого питання. На виконання тестового завдання відводиться 20 хвилин в кінці заняття. Після перевірки робіт проводиться їх аналіз в аудиторії. Аспіранти мають можливість звернути увагу на ті питання, розв'язання яких викликало у них певні складності. Викладач має можливість дати аспіранту конкретне індивідуальне завдання з відпрацювання недостатньо засвоєного матеріалу.

8. Рейтингова система оцінювання результатів навчання

Успішність аспіранта з вивчення кредитного модуля «Проблеми правового забезпечення інформаційної безпеки» оцінюється за семестровим рейтингом. Сума набраних рейтингових балів при семестровому контролі переводиться в оцінки за системою оцінювання ECTS (європейська система оцінювання), що передбачає семибальну шкалу **A, B, C, D, E, Fx, F** оцінок.

Рейтинг аспіранта формується поступово протягом одного навчального року на підставі оцінювання знань, які він отримав з дисципліни «Проблеми правового забезпечення інформаційної безпеки». Оцінювання проводиться за критерієм правильності та повноти, логіки та системності розкриття відповідної теми. Даний рейтинг складається з балів, що він отримує за:

а) відповіді на практичних заняттях, включаючи тематичні доповіді за відповідними темами;
б) самостійну роботу;
в) відповідь на заліку;

Система рейтингових (вагових) балів та критерії оцінювання:

1. *Робота на практичних заняттях*

Формою перевірки рівня підготовленості аспірантів під час практичних занять згідно тем робочої навчальної програми є:

- оцінювання знань аспірантів на практичних заняттях;
- оцінювання виконаних завдань у процесі самостійної роботи аспірантів.

Критерії оцінювання:

5 – високий (поглиблений) рівень підготовки з питань практичного заняття, підготовка доповідей та повідомлень. Вміння працювати групами, аналізувати відповідні законодавчі акти та практично вирішувати ситуаційні завдання;

4 – добрий рівень підготовки. Вміння аналізувати;

3 – задовільний рівень підготовки. Недостатній рівень засвоєння матеріалу, обмеження знань виключно інформацією підручника;

2 – незадовільний рівень підготовки. Дуже низький рівень засвоєння знань, відсутня ініціатива в обговоренні питань практичного заняття;

1 – незадовільний рівень підготовки. Відсутність знань з матеріалу теми, повна пасивність на практичних заняттях.

Заохочувальні та штрафні бали за:

+ *5 балів* – підготовку тематичних доповідей у презентаційній формі;

+ *3 бали* – активну участь на практичних заняттях, у підготовці додаткових наукових та практичних матеріалів.

- *1 бал* – відсутність на практичному занятті без поважної причини.

Розмір шкали рейтингу **R = 100 балів.**

Розмір стартової шкали **R_C = 40 балів.**

Рейтингова шкала з дисципліни складає **$R = R_C + R_E$ = 95-100 балів**

Умови допуску до заліку: стартовий рейтинг $R_C > 40$ балів.

Переведення значення рейтингових оцінок в європейську систему оцінювання (ECTS) і традиційні оцінки для внесення їх до залікової відомості здійснюється відповідно до таблиці:

Таблиця переведення рейтингової оцінки з навчальної дисципліни RD

RD = RC + RE	**Оцінка ECTS**	**Оцінка ECTS**	**Традиційна залікова оцінка**
RD = 95 - 100	A	Відмінно	Зараховано
RD = 85 - 94	B	Дуже добре	
RD = 75 - 84	C	Добре	
RD = 65 - 74	D	Задовільно	
RD = 60 - 64	E	Достатньо	
RD = менш ніж 60	F_X	Незадовільно	Незараховано
RC < 40%	F	Недопущено	Недопущено

Приклад для заліку

Поточне тестування та самостійна робота										Сума балів
Змістовний розділ 1				Змістовний розділ 2					Залік	
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9		
5	8	5	8	5	8	5	8	5	40	97

9. Методичні рекомендації

1. Викладач розпочинає заняття з нагадування про актуальність даної теми та для наступного її практичного засвоєння аспірантами шляхом надання розуміння на конкретних прикладах, що дана сфера забезпечення життєдіяльності суспільства, встановлення та правового регулювання суспільних відносин, яка у сучасних умовах починає займати визначальні позиції, з одного боку, є невід`ємною складовою як інформаційного права, так й національної безпеки, а з іншого боку - має самостійний характер.

2. Вивчення даної дисципліни слід розглядати з позиції сутності інформаційної безпеки, правових питань інформаційної безпеки, правової охорони та захисту інформації в комп'ютерних системах. Зазначений комплекс знань дозволить аспіранту розуміти природу інформації та її властивостей, усвідомлювати сутність інформаційної небезпеки та шляхів її запобігання та усунення. Заняття спрямовується на засвоєння та поглиблення отриманих на лекції знань та напрацювання базових практичних навичок за даною темою.

3. Напередодні заняття зорієнтувати аспірантів, щоб вони мали необхідну літературу та довідковий матеріал.

4. Викладач оголошує тему, мету та навчальні питання даного заняття.

5. У вступному слові нагадати про важливість даного матеріалу, його зв'язок з наступними темами курсу.

6. Викладення змісту розглядуваного навчального питання проводиться у формі доповіді.

7. У разі неточностей у відповіді, доцільно їх усунути шляхом уточнення тими аспірантами, які виявили таке бажання.

8. При розгляді питань домагатись від аспірантів активності в обговорені матеріалу. Для закріплення розглянутого питання, після його обговорення, бажано провести опитування 2-3 аспірантів.

Після розгляду кожного учбового питання викладач підводить підсумок, а в кінці заняття проводить його аналіз в цілому.

10. Рекомендована література

Базова

1. Фурашев В., Радзієвська О. Правове забезпечення інформаційної безпеки : курс лекцій. Київ; Одеса : Фенікс, 2022. 158 с.
2. Господарський кодекс України : Закон України від 16.01.2003 р. № 436-IV : станом на 27 липня 2023. URL: https://zakon.rada.gov.ua/laws/main/436-15#Text (дата звернення: 16.08.2023).
3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи від 28.01.03 р. : URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 16.08.2023).
4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 16.08.2023).
5. Захист прав, свобод та безпеки людини в інформаційному суспільстві: навчальний посібник/ Пилипчук В.Г. та ін. Київ-Одеса : Фенікс, 2021, 273 с.

6. Н. Уханова. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства : монографія. Київ-Одеса: Фенікс, 2022. 140 с.
7. Національна безпека: світоглядні та теоретико-методологічні засади : монографія / за заг. ред. О. П. Дзьобаня. Харків : Право, 2021. 776 с.
8. В.П. Горбулін, О.Г. Додонов , Д.В. Ланде. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія. К.: Інтертехнологія, 2009. 164 с.
9. Кодекс України про адміністративні правопорушення : Закон України від 28.06.96 р. № 254к/96-ВР : станом на 13 липня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 16.08.2023).
10. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР : станом на 03 вересня 2019 р. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 16.08.2023).
11. Стратегія воєнної безпеки України : Указ Президента України від 25.03.2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n9 (дата звернення: 16.08.2023).
12. Кримінальний Кодекс України : Закон від 05.04. 2001 р. № 2341-III : станом на 13 липня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 16.08.2023).
13. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія. Київ: КВІЦ, 2019. 344 с.
14. Ященко В.А., Пилипчук В.Г., Довгань О.Д., Лебединська О.В. Основи демократичного цивільного контролю над сектором безпеки і оборони : навчально-методичні матеріали (для тренінгу). К.: Видавничий дім «АртЕк». 2019. 106 с.
15. Про інформацію : Закон України від 02.10.92 р. № 2657-XII : станом на 21 березня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 16.08.2023).
16. Про запобігання корупції : Закон України від 14.10.2014 р. № 1700-VII : станом на 02 травня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1700-18#Text (дата звернення: 16.08.2023).
17. Про засади внутрішньої і зовнішньої політики : Закон України від 01.07.2010 р. № 2411-VI : станом на 13 грудня 2022 р. (дата звернення: 16.08.2023). https://zakon.rada.gov.ua/laws/show/2411-17#Text (дата звернення: 16.08.2023).
18. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 29 липня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 16.08.2023).
19. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575.: URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 16.08.2023).
20. Про національну безпеку : Закон України від 21.06.2021 р. № 2469-VIII : станом на 24 лютого 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 16.08.2023).
21. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 р. № 537- V : станом на 09 січня 2007 р. URL: https://zakon.rada.gov.ua/laws/show/537-16#Text (дата звернення: 16.08.2023).
22. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 28 липня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 16.08.2023).
23. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX: станом на 13 липня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1089-20#n2246 (дата звернення: 16.08.2023).
24. Стратегія кібербезпеки України : Указ Президента України від 26.08.2021 р. № 44/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7 (дата звернення: 16.08.2023).

25. Стратегія національної безпеки України : Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 16.08.2023).
26. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435- IV: станом на 10 серпня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 16.08.2023).

Допоміжна

27. Господарський процесуальний кодекс України : Закон України від 06.11.91 р. № 1798- XII: станом на 09 серпня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/1798-12#Text (дата звернення: 16.08.2023).
28. Правове регулювання організації та діяльності суб'єктів сектора безпеки і оборони : збірник документів і матеріалів / уклад.: Беланюк М.В., Доронін І.М., Лебединська О.В., Радзієвська О.Г., Пилипчук В.Г., Шамара О.В., Фурашев В.М. К.: Видавничий дім «АртЕк». 2020. 756 с.
29. Юридична відповідальність за правопорушення в інформаційній сфері: теорія і практика : монографія / за ред. К. І. Бєлякова. К.: 2016. 293 с.
30. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI: станом на 23 серпня 2023 р. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 16.08.2023).
31. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI: станом на 13 грудня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 16.08.2023).
32. Про Національну програму інформатизації : Закон України від 01.12.2022р. № 2807-IX: станом на 01 грудня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 16.08.2023).

11. Орієнтирові питання до заліку

1. Визначення сутності інформації.
2. Основні показники класифікації носіїв інформації.
3. Засоби передачі та сприйняття інформації.
4. Основні властивості інформації які визначають її небезпечність.
5. Розкриття сутності інформаційної небезпеки.
6. Особисте бачення ролі та місця інформаційної безпеки у життєдіяльності суспільства у сучасних умовах.
7. Визначення поняття «інформаційна безпека».
8. Особисте бачення трансформації ролі та місця інформаційної безпеки в системі національної безпеки.
9. Особисте бачення трансформації ролі та місця інформаційної безпеки в системі національної безпеки.
10. Розкриття сутності безпечності інформації.
11. Основні чинники, які впливають на небезпечність інформації.

12. Розкриття визначення поняття «безпека інформації».
13. Основні суб`єкти створення небезпечної інформації.
14. Основні чинники визначення об'єктів інформаційної небезпеки.
15. Основні чинники визначення ієрархії об'єктів інформаційної небезпеки.
16. Головний принцип, який забезпечує необхідний рівень інформаційної безпеки
17. Об'єкти інформаційної небезпеки та їх обґрунтування.
18. Коротка характеристика прав і свобод людини, громадянина та їх обов'язків в інформаційній сфері.
19. Коротка характеристика прав суспільства в інформаційній сфері.
20. Коротка характеристика обов'язків держави в інформаційній сфері.
21. Основна об`єктивна причина складності правового забезпечення інформаційної безпеки.
22. Основні суб`єктивні причини складності правового забезпечення інформаційної безпеки.
23. Коротке обґрунтування визначення кібернетики як об`єкту небезпеки.
24. Сутність поняття «кібернетична безпека» (кібербезпека).
25. Чинники які визначають взаємозв`язок понять «інформаційна безпека» та «кібербезпека».
26. Чинники які визначають застосування термінів «інформаційна безпека» та «кібербезпека».
27. Сутність, поняття та правове визначення інформаційної діяльності.
28. Складові інформаційної діяльності.
29. Особисте розуміння співвідношення понять «національна безпека», «інформаційна безпека» та «кібернетична безпека».
30. У чому полягають основні відмінності у сутності понять «інформаційна безпека» та «кібербезпека».
31. Чинники які визначають взаємозв`язок інформаційної діяльності та інформаційної безпеки.
32. Сутність інформаційного насильства.
33. Суб`єкти інформаційної діяльності та їх вплив на процеси забезпечення інформаційної безпеки.
34. Основні чинники які визначають особливості здійснення інформаційної діяльності в умовах постіндустріального суспільства.
35. Сутність маніпуляції.
36. Найбільше розповсюджені види маніпуляції.
37. Суб`єкти інформаційної діяльності та їх вплив на процеси забезпечення кібербезпеки.

38. Особливості маніпулювання свідомістю у сучасних умовах.
39. Наведіть приклади проявів інформаційного насильства.
40. Коротка оцінка ролі маніпулювання в системі державного управління.
41. Коротка оцінка місця маніпулювання в політичної системі.
42. Коротка оцінка ролі та місце маніпулювання в системі міжнародних відносин.
43. Трансформація ролі та значення інформації на різних етапах розвитку людства.
44. Перспективи розвитку та механізми здійснення інформаційного насильства.
45. Механізми впливу інформації на поведінку людини.
46. В чому полягають тотожності та відмінності об`єктів інформаційної небезпеки та інформаційної безпеки?
47. Чому інформаційна діяльність є апріорі небезпечною з точки національної безпеки?
48. Спрямованість розвитку інформаційної діяльності.
49. Роль та значення інформаційних ресурсів у розвитку людства.
50. Тенденції змін у системі доступу до інформаційних ресурсів.
51. Оцінка стану національного інформаційного суверенітету у сучасних умовах.
52. Чинники які впливають на інформаційний суверенітет.
53. Витоки глобалізації інформаційного простору.
54. Механізми та засоби глобалізації інформаційного простору.
55. Основні принципові наслідки глобалізації інформаційного простору.
56. Витоки та наслідки соціальних мереж.
57. Перспективи розвитку соціальних мереж.
58. Структура нормативно-правової бази забезпечення захисту інформації.
59. Розкриття поняття «інформаційно-комунікаційна технологія» (ІКТ).
60. Розкриття понять «глобальна інформаційна система» та «глобальна мережа».
61. Природа тероризму.
62. Розкриття поняття «соціалізація»
63. Поняття об`єктності та суб`єктності в системі правовідносин.
64. Розкриття поняття «інформаційна технологія».
65. Розкриття поняття «інформаційна інфраструктура».