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

ЗАТВЕРДЖЕНО
Директор ДНУ ІІБП
НАПрН України
_____ В.Г. Пилипчук
«04» вересня 2024 р.

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

РОБОЧА НАВЧАЛЬНА ПРОГРАМА

підготовки аспірантів із спеціальності 081 «Право»

Укладач: Ткачук Т.Ю.,
доктор юридичних наук, професор

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

Київ, 2024

Анотація: Процес побудови правової держави та громадянського суспільства в Україні, насамперед, передбачає необхідність формування нового, вищого рівня правової свідомості та правової культури. Великого значення набувають правове виховання і правова освіта, адже без глибоких знань права та законодавства, прав, свобод та обов'язків людини і громадянина еволюційний розвиток жодного суспільства не відбувається, а тому зростає роль викладання навчальної дисципліни «Правове забезпечення кібербезпеки». Вивчення дисципліни особливої актуальності набуває з огляду на важливість тих процесів, які мають місце з початку російсько-української війни, а також євроатлантичного курсу нашої держави. Вивчення навчальної дисципліни дозволяє сформувати у здобувачів систему знань з провідних галузей національного права України (конституційного, адміністративного, інформаційного, цивільного, кримінального тощо).

Мета дисципліни – отримання здобувачами необхідних знань щодо правового забезпечення кібербезпеки, загроз кібербезпеці, основних методів, принципів, алгоритмів захисту інформації в кіберпросторі з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення загроз.

Завдання дисципліни: 1) розуміти зміст та особливості сучасних проблем нормативно-правового забезпечення кібербезпеки; 2) оволодіти термінологією з досліджуваного наукового напряму; 3) засвоїти основні правові механізми вирішення правових проблем теоретичного та прикладного характеру.

У результаті вивчення навчальної дисципліни здобувач повинен

знати:

- основні національні та міжнародні правові акти у сфері кібербезпеки;
- сучасні загрози кібербезпеці;
- методи і засоби захисту інформації у кіберпросторі;
- організаційно-правове забезпечення захисту інформації у кіберпросторі.

вміти:

- аналізувати правові акти у сфері кібербезпеки;
- застосовувати норми права на практиці;
- порівнювати норми права на предмет їх вразливості;
- ідентифікувати можливі загрози кібербезпеці;
- виявляти акції інформаційно-психологічного впливу.

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:
«Правове забезпечення кібербезпеки»</td><td>Форма навчання:
«Заочна»</td></tr>
<tr><td>Спеціальність:
081 «Право»</td><td>Кількість кредитів ECTS
« 4 »</td><td>Статус кредитного модуля
«ІІ 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 кредитного модуля

Метою викладання навчальної дисципліни є ознайомлення аспірантів з правовими основами, що визначають сутність, задачі, принципи та сучасні інформаційні технології кібербезпеки, методологічними та законодавчими основами організації, планування та впровадження систем захисту інформації на підприємствах, а також основними аспектами практичної діяльності по їх створенню, забезпеченню функціонуванню та оцінці ефективності з урахуванням сучасного стану та прогнозу розвитку методів, систем та засобів здійснення погроз зі сторони потенційних порушників.

Завданням вивчення дисципліни «Правове забезпечення кібербезпеки» є надання аспірантам необхідної теоретичної та практичної підготовки для того, щоб вміти:

1. Використовувати законодавчу та нормативно-правову бази, а також вимоги відповідних, в тому числі і міжнародних, стандартів та практик щодо безпечного здійснення професійної діяльності;
2. Аналізувати та виявляти кіберзагрози інформації;
3. Аналізувати наслідки кібератак; знати різні категорії вразливостей програмного та апаратного забезпечення і систем безпеки;
4. Описати правові принципи конфіденційності, цілісності та доступності відносно стану даних та заходів протидії кіберзагрозам;
5. Прогнозувати, виявляти та оцінювати можливі загрози інформаційному простору держави, суспільству організації та дестабілізуючі чинники в роботі систем управління;
6. Описати тактику, методи та процедури, які використовуються кіберзлочинцями;
7. Описати, як технології, продукти і процедури використовуються для захисту конфіденційності, забезпечення цілісності, забезпечують високу доступність;
8. Пояснити, як професіонали кібербезпеки використовують технології, процеси та процедури для захисту всіх компонентів мережної інфраструктури.
9. Розробляти моделі загроз інформації та моделі порушників інформаційної безпеки;
10. Знати різні типи зловмисного ПЗ (відомого як шкідливі програми) та їх симптоми; знати різні методи, якими нападники можуть проникнути в систему: соціальна інженерія, злам паролю WiFi, фішинг та використання вразливостей, тощо.

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.

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. ОСНОВНІ ПОЛОЖЕННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ.					
1.1.	Кіберпростір і кібербезпека: проблеми, перспективи, технології	16	4	2	-	10
1.2.	Загрози у сфері кібербезпеки	14	2	2	-	10
1.3.	Досвід правового забезпечення кібербезпеки у зарубіжних країнах	18	2	2	-	14
	Всього за розділ:	48	8	6	-	34
	Розділ 2. ТЕХНОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ					
2.1.	OSINT-розвідка: правові межі збирання та обробки інформації	28	4	4	-	20
2.2.	Правові основи захисту таємниць у кіберпросторі	14	2	2	-	10
2.3.	Правове забезпечення кібербезпеки об'єктів критичної інфраструктури в умовах повномасштабної війни	14	2	2	-	10
2.4.	Глобальні аспекти розвитку кіберпростору на основі досвіду протидії кіберзагрозам в умовах російсько-української війни	16	2	4	-	10
	Всього за розділ:	72	10	12	-	50
	Залік:			(2)		
	Разом:	**120**	**18**	**18**	**-**	**84**

4. Лекційні заняття

Розділ І.

Лекція 1: Кіберпростір і кібербезпека: проблеми, перспективи, технології

Перелік основних питань:
1. Законодавство про кібербезпеку
2. Система забезпечення кібербезпеки держави
3. Поняття кіберпростору
4. Актуальні проблеми кібербезпеки України в умовах російсько-української війни

Питання для самоперевірки:
1. *Визначіть поняття «кібербезпека».*
2. *Охарактеризуйте сутність забезпечення кібербезпеки.*
3. *Які існують життєво важливі інтереси особи, держави та суспільства в електронній сфері?*
4. *Назвіть та дайте основну характеристику основних законодавчих актів у сфері забезпечення кібербезпеки.*
5. *Що таке кіберпростір та основні його складові?*
6. *Політика держави щодо забезпечення кібербезпеки після початку повномасштабного наступу рф.*

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

Лекція 2: Загрози у сфері кібербезпеки

Перелік основних питань:
1. Поняття загроз у сфері кібербезпеки
2. Система загроз кібербезпеки держави
3. Протидія загрозам у сфері кібербезпеки

Питання для самоперевірки:
1. *Загрози у сфері кібербезпеки.*
2. *Зміст кіберзагроз.*
3. *Класифікація та ознаки кіберзагроз.*
4. *Основні характеристики кіберзагроз.*
5. *Дії у кіберпросторі та їх особливості.*
6. *Сутність, цілі та задачі кібердій.*
7. *Класифікація форм і способів дій у кіберпросторі*
8. *Кіберінциденти: передумови скоєння та наслідки.*

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

Лекція 3: Досвід правового забезпечення кібербезпеки у зарубіжних країнах

Перелік основних питань:
1. Правові засади забезпечення кібербезпеки у ЄС
2. Правова база НАТО у сфері кібербезпеки

2. Досвід США у протидії кіберзагрозам
3. Можливі напрями імплементації досвіду інших країн у сфері правового забезпечення кібербезпеки

Питання для самоперевірки:
1. Назвіть нормативні документи ЄС у сфері кібербезпеки.
2. Особливості забезпечення кібербезпеки НАТО.
3. Політика США у сфері кібербезпеки.
4. Досвід Латвії, Литви та Естонії у сфері забезпечення кібербезпеки.
5. Досвід Ізраїлю у сфері правового забезпечення кібербезпеки.
6. Міжнародні стандарти у сфері кібербезпеки.

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

Розділ ІІ.

Лекція 4: OSINT-розвідка: правові межі збирання та обробки інформації

Перелік основних питань:
1. Правові підстави застосування технології OSINT
2. Можливості технології OSINT у забезпеченні кібербезпеки держави
3. Можливості технології OSINT у протидії дезінформації, фейкам та розслідуванні військових злочинів
4. Методи та інструменти OSINT

Питання для самоперевірки:
1. *Визначіть правові підстави застосування технології OSINT.*
2. *Охарактеризуйте можливості технології OSINT у забезпеченні кібербезпеки держави.*

Охарактеризуйте можливості технології OSINT у протидії дезінформації, фейкам. та розслідуванні військових злочинів
та розслідуванні військових злочинів
3. *Пошук інформації про особу з допомогою інструментів OSINT.*
4. *технологія OSINT у протидії російській агресії*

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

Лекція 5: Правові основи захисту таємниць у кіберпросторі

Перелік основних питань:
1. Правові засади інформації з обмеженим доступом
2. Види таємниць
3. Ризики та вразливості таємної інформації
4. Кіберзахист інформації з обмеженим доступом

Питання для самоперевірки:
1. *Поняття інформації з обмеженим доступом.*
2. *Види інформації з обмеженим доступом.*
3. *Правові засади визначення таємної інформації.*
4. *Загрози таємній інформації.*
5. *Принципи забезпечення цілісності таємної інформації.*

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

Лекція 6: Правове забезпечення кібербезпеки об'єктів критичної інфраструктури

Перелік основних питань:

1. Законодавство про критичну інфраструктуру
2. Кіберзагрози об'єктам критичної інфраструктури в умовах війни
3. Попередження та протидія кіберзагрозам на об'єктах критичної інфраструктури: досвід російсько-української війни

Питання для самоперевірки:

1. *Законодавство про критичну інфраструктуру.*
2. *Потенційні кіберзагрози об'єктам критичної інфраструктури.*
3. *Правові засади визначення таємної інформації.*
4. *Система заходів попередження кіберзагрозам на об'єктах критичної інфраструктури .*
5. *Протидія кіберзагрозам на об'єктах критичної інфраструктури.*

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

Лекція 7: Глобальні аспекти розвитку кіберпростору

Перелік основних питань:

1. Розвиток штучного інтелекту та IoT як передумова появи нових правовідносин
2. Розвиток законодавства про кібербезпеку
3. Місце та роль України в глобальній системі розвитку кібербезпеки

Питання для самоперевірки:

1. *Тенденції розвитку інформаційних та кібертехнологій.*
2. *Особливості високотехнологічних війн.*
3. *Існуючі системи підготовки фахівців з кібербезпеки та кібероборони у провідних країнах світу.*
4. *Особливості практичної складової підготовки фахівців з кібербезпеки та кібероборони у провідних країнах світу.*
5. *Зміст системи підготовки військових фахівців та наукових досліджень за високотехнологічними напрямами.*
6. *Вимоги до знань фахівців з кібербезпеки та кібероборони.*
7. *Основні фактори, які впливають на розвиток і впровадження високотехнологічних розробок в інтересах національної безпеки і оборони в Україні.*
8. *Принципово-інноваційні рішення побудови системи кібербезпеки та кібероборони.*

Література: 1, 2, 5 – 9, 15, 18, 24, 27, 31, 32.

5. Практичні заняття

Розділ 1.
ОСНОВНІ ПОЛОЖЕННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ.

Практичне заняття 1:

Створити базу даних нормативно-правових актів та органів державного регулювання в сфері кібербезпеки в Україні. База даних повинна додатково містити (за можливістю) посилання на офіційні сайти державних органів в мережі Internet та нормативно-правових актів на сайті Верховної Ради України. Обов'язково до кожного розділу БД та запису – анотація.

Бути готовим відповіти на запитання по темі роботи та коротко охарактеризувати основні елементи створеної бази даних.

Завдання на СРС:

Детально ознайомитись зі змістом стандартів ISO/IEC 27001:2005 та ISO/IEC 27001:2013. Виконати порівняльний аналіз версій 2005 та 2013 років. Результати аналізу викласти у вигляді таблиці у звіті до практичної роботи.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Практичне заняття 2:

Класифікуйте інформаційні активи, що знаходяться на вашому пристрої (мобільному телефоні, ноутбуці, домашньому ПК і т.д.), сформулюйте потенційні загрози інформації, визначіть методи та засоби їх уникнення. Представити у вигляді таблиці відповідності «інформація-загрози-методи і засоби уникнення».

Практичне заняття 3:

Проведіть аудит кібербезпеки вашої організації або компанії. Створіть план дій для виявлення потенційних уразливостей та створіть план для їх виправлення.

Завдання на СРС:

Створіть план відновлення після кібератаки. Виконайте тестування на практиці, щоб переконатися, що план працює.

Розробіть план навчання персоналу з питань кібербезпеки. Створіть матеріали для навчання та підготуйте презентацію.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Розділ 2.
ТЕХНОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Практичне заняття 4:

1. Охарактеризуйте наступні інструменти OSINT: OSINT-фреймворк, Shodan, Metagoofil, CrowdTangle, Maltego, Google Dorks.
2. Базові правила роботи з пошуку інформації в Google.

Завдання на СРС:

Підготуйте розгорнуту доповідь на тему «Як OSINT-розвідка може допомогти українським військовим».

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Практичне заняття 5:

Дайте характеристику основним технологіям osint-розвідки у протидії «fake news» та розробіть механізми протидії.

Завдання на СРС:
Опишіть інструменти OSINT-розвідки для пошуку інформації про особу. Дайте правову оцінку своїм діям.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Практичне заняття 6:

Розробіть локальний нормативний акт про кіберзахист на об'єкті критичної інфраструктури (на вибір).

Завдання на СРС:
Проаналізуйте приклади кібератак на об'єкти критичної інфраструктури в Україні протягом останніх 5 років. Визначіть типи, шкоду, прогалини, можливі шляхи їх попередження

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Практичне заняття 7:

Підготуйте доповідь на тему:
«Історія кібервоєн»; «Кіберзброя у російсько-українській війні»; «Технології кіберзахисту майбутнього»; «права роботів: досвід і перспективи розвитку в національних правових системах»

Завдання на СРС:
Проаналізуйте приклади використання штучного інтелекту у військових конфліктах. Розробіть можливі організаційно-правові заходи контролю за використанням штучного інтелекту у військових конфліктах.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

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.

Розділ 1.
ОСНОВНІ ПОЛОЖЕННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ.

Завдання на самостійне опрацювання:
Детально ознайомитись зі змістом стандартів ISO/IEC 27001:2005 та ISO/IEC 27001:2013. Виконати порівняльний аналіз версій 2005 та 2013 років. Результати аналізу викласти у вигляді таблиці у звіті до практичної роботи.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Завдання на самостійне опрацювання:
Створіть план відновлення після кібератаки. Виконайте тестування на практиці, щоб переконатися, що план працює.
Розробіть план навчання персоналу з питань кібербезпеки. Створіть матеріали для навчання та підготуйте презентацію.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Розділ 2.
ТЕХНОЛОГІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Завдання на самостійне опрацювання:
Підготуйте розгорнуту доповідь на тему «Як OSINT-розвідка може допомогти українським військовим у боротьбі з російськими загарбниками».

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Завдання на самостійне опрацювання:
Опишіть інструменти OSINT-розвідки для пошуку інформації про особу. Дайте правову оцінку своїм діям.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Завдання на самостійне опрацювання:
Проаналізуйте приклади кібератак на об'єкти критичної інфраструктури в Україні протягом останніх 5 років. Визначіть типи, шкоду, прогалини, можливі шляхи їх попередження

Література: 5, 9, 28, 31, 32, 48, 56, 68.

Завдання на самостійне опрацювання:
Проаналізуйте приклади використання штучного інтелекту у військових конфліктах. Розробіть можливі організаційно-правові заходи контролю за використанням штучного інтелекту у військових конфліктах.

Література: 5, 9, 28, 31, 32, 48, 56, 68.

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.

1. Незаконне використання програмного забезпечення – це …
1) промислове шпигунство;
2) крадіжка і копіювання;
3) несанкціонована модифікація;
4) піратство.

2. З якою метою зловмисники можуть використовувати програмні оболонки операційних систем?
1) для аналізу мережного обміну;
2) для первинного аналізу структури захищеного програмного продукту;
3) для аналізу мережного обміну;
4) для аналізу використання системами захисту системних функцій.

3. Для чого хакери використовують програми-емулятори ?
1) для обходу захистів програм шляхом прив'язок до електронних ключів;
2) для модифікації інтерфейсу захищених програм;
3) для статистичного аналізу систем захисту.

4. Що таке кібервійна?
1) це інтернет-конфлікт, який передбачає втручання до інформаційних систем інших країн;
2) це імітаційне програмне забезпечення для пілотів військово-повітряних сил, яке дозволяє їм практикуватися за змодельованими сценаріями війни;
3) це напад, здійснений групою хакерів-аматорів
4) це набір індивідуальних засобів захисту, розроблений для солдатів, які беруть участь у ядерній війні.

5. Як ще називають конфіденційність інформації?
1) приватність;
2) точність;
3) достовірність;
4) узгодженість.

6. Який метод використовується для перевірки цілісності даних?
1) контрольна сума;
2) шифрування;
3) резервне копіювання;
4) аутентифікація.

7. Що з наведеного є прикладом «хактивізму»?

1) група захисників навколишнього середовища запускає атаку відмови в обслуговуванні проти нафтової компанії, відповідальної за великий витік нафти;

2) підліток зламує веб-сервер місцевої газети і публікує на ньому зображення улюбленого персонажа з мультфільму;

3) злочинці використовують Інтернет у спробі викрасти гроші з банку одна країна намагається викрасти секрети безпеки іншої країни шляхом проникнення до державних мереж.

8. Яка мотивація хакера у білому капелюсі?

1) виявлення слабких місць систем і мереж для підвищення рівня їх захисту;

2) точне налаштування мережевих пристроїв для покращення їх ефективності та продуктивність використання будь-якої вразливості з метою незаконної особистої вигоди;

3) використання будь-якої вразливості з метою незаконної особистої вигоди вивчення операційних систем різних платформ для розробки нової системи

9. У чому причина того, що внутрішні загрози безпеці можуть заподіяти більшу шкоду для організації, аніж зовнішні загрози?

Внутрішні користувачі мають прямий доступ до пристроїв інфраструктури

1) Внутрішні користувачі мають кращі навички хакерства;

2) Внутрішні користувачі можуть отримати доступ до корпоративних даних без аутентифікації;

3) Внутрішні користувачі можуть отримати доступ до пристроїв інфраструктури через Інтернет;

10. Які три методи можуть бути використані для забезпечення конфіденційності інформації?

1) двофакторна аутентифікація;
2) логін та пароль;
3) шифрування даних;
4) резервне копіювання;
5) налаштування прав доступу для файлів;
6) контроль версій.

8. Рейтингова система оцінювання результатів навчання

Успішність аспіранта з вивчення кредитного модуля «Правове забезпечення кібербезпеки» 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 «Правове забезпечення кібербезпеки». 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.

Критерії залікового оцінювання: виходячи з розміру шкали $R_E = 60$.

Переведення значення рейтингових оцінок в європейську систему оцінювання (ECTS) і традиційні оцінки для внесення їх до екзаменаційної (залікової) відомості та залікової книжки 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
Практичне заняття	Залік	
40	60	100

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

1. **Базова:**
2. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
3. Конвенція про кіберзлочинність: ратифікована із застереженнями і заявами Законом № 2824-IV від 07.09.2005 URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
4. Загальна декларація прав людини. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
5. Конвенція про захист прав людини і основоположних свобод. URL:https://zakon.rada.gov.ua/laws/show/995_004#Text
6. Кодекс України про адміністративні правопорушення від 7 грудня 1984 року № 8073-X. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text
7. Кримінальний кодекс України від 5 квітня 2001 року№ 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
8. Про основні засади забезпечення кібербезпеки України: Закон України №2163 від 5 жовтня 2017 року URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" Указ Президента України від 26 серпня 2021 року № 447/2021 URL: https://www.president.gov.ua/documents/4472021-40013
10. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI URL: https://zakon.rada.gov.ua/laws/show/2939-17#top
11. Про захист персональних даних: Закон України від 1 червня 2010 року № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
12. Про інформацію: закон України від 2 жовтня 1992 року № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
13. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
14. Про національну безпеку України: Закон України 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
15. Про особливості надання публічних (електронних публічних) послуг: Закон України від 15 липня 2021 року № 1689-IX URL: https://zakon.rada.gov.ua/laws/show/1689-20#Text
16. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: затв. постановою Кабінету Міністрів України від 19 червня 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text
17. Порядок проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом: затв. постановою Кабінету Міністрів України від 11 листопада 2020 р. № 1176. URL: https://zakon.rada.gov.ua/laws/show/1176-2020-%D0%BF#n8
18. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: затв. Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text
19. Regulation (EU, Euratom) 2023/2841 of the European Parliament and of the Council of 13 December 2023 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union Document 32023R2841 URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302841
20. Положення про захист інформації та кіберзахист у платіжних системах: затв. Постановою Правління Національного банку України 19.05.2021 № 43. URL: https://zakon.rada.gov.ua/laws/show/v0043500-21#Text

21. Баранов О. А. Трансформація: соціальна & цифрова & правова: монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату. Одеса: Видавничий дім «Гельветика», 2022. 272 с.

22. Технологія OSINT: інструменти та методи для захисту інформаційної безпеки: практ. посіб. / Т. Ю. Ткачук, Н. І. Ткачук, І. М. Ничитайло А. І. Старосєк. Київ: НА СБУ, 2023. 180 с.

23. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: Монографія / Т.Ю. Ткачук. – К. : ТОВ «Видавничий дім «АртЕк», 2018. – 411 с.

24. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія /І.В. Арістова, О.А. Баранов, О.П. Дзьобань та ін.; за заг. ред. проф. К.І. Бєлякова. Київ: КВІЦ, 2019. 344с.

25. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів закладів вищої освіти. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2024 . – 678 с.

26. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи; Одеса : Фенікс, 2020. 404 с.

27. Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.Біленчук П. Д., Обіход Т. В. Кібербезпека і засоби запобігання та протидії кіберзлочинності й кібертероризму. Часопис Київського університету права. 2018. № 3. С. 235-239. URL: http://nbuv.gov.ua/UJRN/Chkup_2018_3_54

28. Білявська Ю., Микитенко Н, Шестак Я. Кібербезпека та захист інформації під час пандемії COVID-19. Товари і ринки. 2021. № 1. С. 34-46. URL: http://nbuv.gov.ua/UJRN/tovary_2021_1_5

29. Гуцалюк М. В. Напрями посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю. Інформація і право. 2021. № 4. С. 141-147. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_16

30. Дзюндзюк В. Б., Котух Є. В. Кібербезпека як один з пріоритетів національної політики. Державне будівництво. 2020. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2020_2_4

31. Діденко А. С. Мета, завдання та принципи державної політики у сфері протидії кіберзлочинності. Право і Безпека. 2020. № 1. С. 53-59. URL: http://nbuv.gov.ua/UJRN/Pib_2020_1_9

32. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. Інформація і право. 2021. № 4. С. 129-134. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_14.

33. Малишева Н. Р. Кібербезпека космічної діяльності та можливості її забезпечення засобами міжнародного права. Правова держава. 2021. Вип. 32. С. 245-257. URL: http://nbuv.gov.ua/UJRN/PrDe_2021_32_28

34. Лісовський П.М., Лісовська Ю.П. Дипломатія: кібербезпека та шляхетність переговорів. Ліра-К. 2021р. 222 с.

35. Основи кібергігієни. Дія. Цифрова освіта. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene

36. Попередній аналітичний звіт комітету Верховної ради України з питань цифрової трансформації про контроль за виконанням Закону України «Про основні засади кібербезпеки в Україні» Березень 2020 року. URL: https://www.ua.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cyber security_02.pdf

37. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Науковий вісник Ужгородського національного університету. Серія : Право. 2021. Вип. 64. С. 386-391. URL: http://nbuv.gov.ua/UJRN/nvuzhpr_2021_64_74

38. Скибун О. Ж. Кібербезпека систем електронних комунікацій органів державної влади України. Вісник Національної академії державного управління при Президентові України. Серія : Державне управління. 2021. № 1. С. 30-39. URL: http://nbuv.gov.ua/UJRN/vnaddy_2021_1_6

39. Сліпченко Т. О. Кібербезпека як складова системи захисту національної безпеки: європейський досвід. Актуальні проблеми правознавства. 2020. Вип. 1. С. 128-133. URL: http://nbuv.gov.ua/UJRN/aprpr_2020_1_22

40. Сопілко І. М. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Юридичний вісник. Повітряне і космічне право. 2021. № 2. С. 110-115. URL: http://nbuv.gov.ua/UJRN/Npnau_2021_2_16

41. Стежко С. М., Фица В. М. Кібербезпека як важливий фактор забезпечення життєдіяльності вітчизняної енергетичної галузі. Інформація і право. 2021. № 4. С. 113-120. URL: http://nbuv.gov.ua/UJRN/Infpr_2021_4_12

42. Філінович В. В. Кібербезпека та Інтернет речей: правовий аспект. Юридичний вісник. Повітряне і космічне право. 2020. № 4. С. 122-127. URL: http://nbuv.gov.ua/UJRN/Npnau_2020_4_19

Допоміжна:

43. Посібник НАТО з розвідки з використанням відкритих джерел (NATO Open Source Intelligence Handbook) URL: https://web.archive.org/web/20201107103435/http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf

44. Перлрос Н. Ось таким, як мені кажуть, буде кінець світу: перегони кіберозброєнь. Фоліо. 2022. 576 с.

45. Ланде Д.В., Правові питання конкурентної розвідки. Інформація і право. 2(33)/2020. С. 51-68

46. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. [Видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с.

47. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Компьютерная конкурентная разведка. К.: ТОВ "Інжиніринг", 2021. 354 с.

48. Курочкін О. О. Особливості застосування відкритих даних в розвідувальній діяльності. Державна прикордонна служба України, 2018. https://dpsu.gov.ua/ua/about/publications/osoblivosti-zastosuvannya-vidkritih-danih-v-rozviduvalniy-diyalnosti/

49. Коломієць І. В. Застосування відкритих даних у забезпеченні кібербезпеки держави. Інформаційна безпека, 2019. http://nbuv.gov.ua/UJRN/ib_2019_1_8

50. Шаповал О. О. Використання відкритих даних в процесі забезпечення національної безпеки. Юридичний вісник, 2018. http://nbuv.gov.ua/UJRN/yurvis_2018_3_14

51. Томашівська Н. О., Гавриш А. А. Використання відкритих даних для забезпечення ефективності державного управління. Науковий вісник Луганського національного університету імені Тараса Шевченка, 2020. http://nbuv.gov.ua/UJRN/Nvlshu_2020_16_8

52. Michael Bazzell Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.

53. Sean-Philip Oriyano OSINT and the Reconnaissance Phase of a Cyber Attack.

54. John Sammons The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics.

55. Johnny Long Google Hacking for Penetration Testers.

56. Christopher Hadnagy Social Engineering: The Science of Human Hacking.

100 . Український центр кібербезпеки - на сайті можна знайти багато корисної інформації про кібербезпеку, включаючи OSINT: https://cybersecurity.ua/

57. Інтернет-ресурс "Діяльність з відкритими даними" - портал, який надає доступ до відкритих даних в Україні: https://data.gov.ua/

58. Блог "Open Source Intelligence в Україні" - це блог, де публікуються новини і корисна інформація про використання OSINT в Україні: http://osint.com.ua/

59. Український центр дослідження діяльності РФ - на сайті можна знайти аналітичні матеріали та дослідження, включаючи використання OSINT в роботі: https://ucdr.org.ua/

60. Ресурс "Інтернет-дослідження та OSINT" - це сторінка на Facebook, де публікуються матеріали про використання OSINT в Україні: https://www.facebook.com/OSINT.in.ua/

61. Асоціація журналістів-розслідувачів - на сайті можна знайти корисну інформацію про використання OSINT в розслідуваннях: https://investigation.org.ua/

62. Український інститут майбутнього - на сайті можна знайти дослідження, включаючи аналіз даних за допомогою OSINT: https://uifuture.org/

63. Український криптологічний альманах - журнал, в якому публікуються статті про кібербезпеку, включаючи OSINT: http://almanah.ukrcrypto.com/

64. Блог "CyberTalents" - на сайті можна знайти багато корисної інформації про кібербезпеку, включаючи OSINT: https://cybertalents.com.ua/

65. Український центр стандартів, якості та сертифікації - на сайті можна знайти матеріали про кібербезпеку та стандарти, включаючи використання OSINT: https://ukrmetrtest.com.ua/

66. Асоціація журналістів-розслідувачів - на сайті можна знайти корисну інформацію про використання OSINT в розслідуваннях: https://investigation.org.ua/

67. Український інститут майбутнього - на сайті можна знайти дослідження, включаючи аналіз даних за допомогою OSINT: https://uifuture.org/

68. Український криптологічний альманах - журнал, в якому публікуються статті про кібербезпеку, включаючи OSINT: http://almanah.ukrcrypto.com/

69. Блог "CyberTalents" - на сайті можна знайти багато корисної інформації про кібербезпеку, включаючи OSINT: https://cybertalents.com.ua/

70. Український центр стандартів, якості та сертифікації - на сайті можна знайти матеріали про кібербезпеку та стандарти, включаючи використання OSINT: https://ukrmetrtest.com.ua/

71. Мироненко В. Армія кібервоїнів: міжнародно-правовий досвід у сфері боротьби з кіберзлочинністю. MIND. 28 лютого 2024 https://mind.ua/openmind/20270195-armiya-kibervoyiniv-mizhnarodno-pravovij-dosvid-u-sferi-borotbi-z-kiberzlochinnistyu

11. Орієнтовні питання до заліку

1. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України.
2. Національний кіберпростір: сучасні виклики та кіберзагрози.
3. Основні напрямки розбудови національної системи кібербезпеки.
4. Державна політика у сфері кібербезпеки в Україні.
5. Правові основи забезпечення кібербезпеки України.
6. Принципи застосування законодавства у сфері кібербезпеки.
7. Основні положення Закону України «Про основні засади забезпечення кібербезпеки України».
8. Принципи забезпечення кібербезпеки.
9. Кіберзагроза: поняття та правовий зміст.
10. Класифікація кіберзагроз та їх зміст.
11. Захист прав, свобод і законних інтересів громадян України у кіберпросторі.
12. Об'єкти кібербезпеки.
13. Об'єкти кіберзахисту.
14. Правові та організаційні засади створення та функціювання національної системи захисту критичної інфраструктури.
15. Суб'єкти забезпечення кібербезпеки: поняття та види.
16. Правовий статус основних суб'єктів національної системи кібербезпеки: Державної служби спеціального зв'язку та захисту інформації України, Національної поліції України, Служби безпеки України, Міністерства оборони України та Генерального штабу Збройних Сил України, розвідувальних органів, Національного банку України.
17. Державно-приватна взаємодія у сфері кібербезпеки.
18. Інформаційна безпека та її місце в системі національної безпеки України.
19. Нормативно-правове регулювання відносин щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.
20. Нормативно-правове забезпечення інформаційної безпеки в Україні.
21. Основні положення Указу Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України".
22. Забезпечення захисту прав і свобод людини в інформаційній сфері.
23. Технологія blockchain як складова інформаційної безпеки.
24. Кібербезпека та захист персональних даних.
25. Правове регулювання відносин, пов'язаних із захистом і обробкою персональних даних.
26. Захист персональних даних: міжнародні стандарти та законодавство України.
27. Правовий статус суб'єктів відносин, пов'язаних із персональними даними.
28. Кібербезпека та інтернет речей: правове регулювання.
29. Правове регулювання відносин, пов'язаних із забезпеченням доступу до публічної інформації.
30. Інформаційна безпека у системі електронного урядування.
31. Захист інформації в системах електронного документообігу.
32. Захист інформації та кіберзахист у платіжних системах.
33. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.
34. Правові аспекти регулювання відносин у соціальних мережах.
35. Відповідальність за порушення законодавства у сфері кібербезпеки.
36. Поняття та види кіберзлочинів.
37. Кримінальна відповідальність за кіберзлочини.
38. Поняття та види форм адміністративно-правової протидії кіберзлочинності в Україні.
39. Фінансове забезпечення заходів кібербезпеки.
40. Контроль за законністю заходів із забезпечення кібербезпеки України.
41. Напрями зовнішньополітичної діяльності України у сфері кібербезпеки.
42. Міжнародне співробітництво у сфері кібербезпеки.