Повна назва: Правове забезпечення кібербезпеки

Статус: Нормативна

Метою викладання навчальної дисципліни «Правове забезпечення кібербезпеки» є оволодіння студентами основоположними знаннями у сфері правових механізмів та інструментів забезпечення кібербезпеки; набуття первинних знань та умінь ефективного та безпекового поводження в кіберпросторі. Важливою складовою є набуття навичок самостійної роботи, необхідних для подальшого поглиблення й оновлення правових знань, що безпосередньо формує правосвідомість і правову культуру фахівця, підвищення правової ерудиції студентів.

Завдання:

- засвоїти сутність основних понять, їх тотожностей та відмінностей у сфері правового забезпечення кібербезпеки;
- взаємозв'язок кібербезпеки з інформаційною безпекою, національною безпекою та правами людини;
- основи державної та міжнародної політики у сфері забезпечення кібербезпеки та зміст основних положень нормативно-правових актів у сфері кібербезпеки;
- реальні та потенційні загрози у кіберпросторі та законодавчі шляхи їх запобігання;
- основні положення юридичної відповідальності (дисциплінарної, адміністративної, кримінальної) за правопорушення, які вчиняються з використанням електронно-обчислювальних машин (комп`ютерів), систем та комп`ютерних мереж та мереж електрозв`язку;
- зміст основних міжнародних договорів з питань кібербезпеки;
- основні проблеми правового забезпечення кібербезпеки.

Загальні компетентності:

- ✓ Здатність до абстрактного мислення, аналізу та синтезу.
- ✓ Здатність застосовувати знання у практичних ситуаціях.
- ✓ Здатність вчитися та оволодівати сучасними знаннями.
- ✓ Здатність працювати в команді.
- ✓ Здатність діяти на основі етичних міркувань (мотивів).
- ✓ Здатність реалізувати свої права та свої обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного

демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

✓ Здатність зберігати та приумножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку права, його місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій.

Фахові компетентності:

- засвоїти основні фундаментальні поняття і закони нормативно-правового забезпечення кібербезпеки для їх використання в практичній діяльності;
- розуміти взаємозв'язок інформаційної безпеки з інформаційним суверенітетом, національною безпекою та правами людини;
- знати основи державної та міжнародної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки та кібербезпеки;
- знати основні закони, принципи та правила поводження з інформацією;
- виявляти реальні та потенційні загрози у сфері інформаційної безпеки та кібербезпеки та законодавчі шляхи їх запобігання;
- знати основні методи маніпулювання свідомістю людини, впливу на суспільну думку з використанням сучасних інформаційно-комунікаційних технологій;
- знати основні положення юридичної відповідальності за правопорушення в сфері кібербезпеки, зміст основних міжнародних договорів з цього питання;
- розуміти основні проблеми правового забезпечення інформаційної безпеки та кібербезпеки;
- здатність аналізувати правові проблеми, формувати та обґрунтовувати правові позиції;
- здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності;
- здатність до логічного, критичного і системного аналізу документів, розуміння їх правового характеру і значення.

Результати вивчення дисципліни «Правове забезпечення кібербезпеки»:

Знання та розуміння:

- розробляти та кваліфіковано застосовувати нормативно-правові акти, реалізовувати норми матеріального й процесуального права в професійній діяльності;
- надавати оцінку чинним нормативно-правовим актам, виявляти колізії та прогалини у правовому регулюванні;
- визначати переконливість аргументів у процесі оцінки заздалегідь невідомих умов та обставин.
- здійснювати аналіз суспільних процесів у контексті аналізованої проблеми і демонструвати власне бачення шляхів її розв'язання.
- проводити збір і інтегрований аналіз матеріалів з різних джерел.
- застосовувати базові знання основних закономірностей юридичного мислення та пізнання, поняття і категорії, методології правової науки;
- використовувати базові знання технологій та методів (аналіз юридичних документів, способи розв'язування юридичних задач, стандарти для різної ділової документації);
- використовувати базові знання про інформаційні ресурси, де вони розміщені, як можна отримати до них доступ і як можна їх використовувати з метою підвищення ефективності професійної діяльності.
- виявляти знання і розуміння основних сучасних правових доктрин, психологічних концепцій, цінностей та принципів функціонування національної правової системи.

<u>Застосування знань та розумінь(уміння)</u>

- Здатність формулювати власні обґрунтовані судження на основі аналізу відомої проблеми.
- Здатність оцінювати недоліки і переваги аргументів, аналізуючи відому проблему.
- Складати та узгоджувати план власного дослідження і самостійно збирати матеріали за визначеними джерелами.
- Здатність використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин.
- Здатність самостійно визначати ті обставини, у з'ясуванні яких потрібна допомога, і діяти відповідно до отриманих рекомендацій.
- Здатність володіти базовими навичками риторики.
- Здатність пояснювати характер певних подій та процесів з розумінням професійного та суспільного контексту.
- Здатність розуміння сутності та змісту основних правових інститутів і норм фундаментальних галузей права.

- Здатність пояснювати природу та зміст основних правових явищ і процесів.
- Здатність застосовувати набуті знання у різних правових ситуаціях, виокремлювати юридично значущі факти.
- Здатність готувати проекти необхідних актів застосування спеціальних знань відповідно до правової ситуації у сфері правового забезпечення кібербезпеки.
- Здатність надавати консультації у сфері правового забезпечення кібербезпеки.

Формування суджень:

- формування розуміння та сприйняття етичних норм поведінки відносно інших людей;
- креативність, здатність до системного мислення;
- адаптивність і комунікабельність;
- турбота про якість виконуваної роботи;
- виявляти готовність переглядати свої судження і міняти образ дій за наявності переконливих аргументів.

- **Програма навчальної дисципліни**

-

Назви кредитів і тем	Кількість годин					
	денна форма					
	Усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
Кредит 1. Теоретичні аспекти правового забезпечення інформаційної безпеки						
Тема 1. Інформація як об'єкт правового регулювання.	7	2				4
Тема 2. Інформаційна безпека як об'єкт правовідносин.	7	2				4
Тема 3. Національна та міжнародна безпека.	7	2				4
Тема 4. Правове забезпечення захисту інформації.	7	2				4
Тема 5. Правові проблеми забезпечення інформаційної безпеки.	7	2				4
Разом за кредитом 1	35	10				20
Кредит 2. Правові основи забезпечення кібербезпеки України						

Тема 6. Кібербезпека як одна з головних складових національної безпеки держави.	8	2				5
Тема 7. Нормативно-правові засади кібербезпеки як складова частина механізму забезпечення національної безпеки України: еволюція та сучасний стан.	8	2				4
Тема 8. Міжнародні правові акти у сфері кібербезпеки, учасником яких є Україна.	9	2	1			6
Разом за кредитом 2	25	6	1			15
Кредит 3. Адміністративно-правове регулювання відносин у сфері кібербезпеки						
Тема 9. Нормативно-правові акти органів виконавчої влади у сфері кібербезпеки та протидії кіберзлочинам.	9	2	2			7
Тема 10. Нормативно-правові акти спеціальних суб'єктів, що забезпечують реалізацію державної політики у сфері кібербезпеки.	9	2	2			7
Тема 11. Правова відповідальність за правопорушення в кіберпросторі.	8	2	2			5
Разом за кредитом 3	26	6	6			19
Кредит 4. Нормативно-правові основи протидії кіберзлочинності.						
Тема 12. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Категорії та особливості.	9	2	2			6
Тема 13. Злочини, що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у сфері електронної комерції та платіжної інфраструктури.	9	2	2			5
Тема 14. Проблемні питання правового регулювання протидії незаконним операціям з інформацією, що дозволяє ідентифікувати фізичну особу під час доступу до автоматизованих систем та платіжних інструментів.	8	2	2			5
Тема 15. Злочини, що вчиняються з використання електронно-обчислювальних машин (комп'ютерів) у сфері порушення авторських і суміжних прав, а також обігу інформації.	8	2	2			5

Разом за кредитом 4	34	8	8			21
Атестація						
Усього годин	**120**	**30**	**15**			**75**

Кількість годин (кількість кредитів ЄКТС): На вивчення навчальної дисципліни відводиться 120 години / 4 кредитів ECTS. Види робіт: Контроль за рівнем засвоєння матеріалу та знань студентів проводиться у таких формах: усна відповідь на семінарських заняттях та доповнення відповіді іншого студента, підготовка і захист доповіді, письмові роботи. Протягом IX семестру здійснюється поточний та підсумковий контроль. Поточний контроль здійснюється надання усних відповідей на семінарських заняттях, перевірки виконаних завдань самостійної роботи, тестовий зріз знань. Підсумковий контроль з дисципліни «Правове забезпечення кібербезпеки» здійснюється у формі заліку. Критерії оцінювання: аргументована, логічна, повна відповідь; вільне володіння матеріалом всього навчального курсу; оперування відповідними понятійними інструментами, вміння встановити зв'язок між теоретичною «базою» та практикою; залучення до відповіді самостійно опрацьованої літератури; вміння аналізувати нормативні документи та вміти користуватися юридико-психологічними знаннями для вирішення конкретних правових норм і задач.

Критерії оцінювання та засоби діагностики результатів навчання

№	Вид діяльності (завдання)	Максимальна кількість балів
1	Усна відповідь на семінарському занятті	32 (3*4 +5*4)
2	Письмова доповідь	7
3	Наукова доповідь	6
4	Тестовий зрізь знань	25
4	Залік (VII семестр)	30
	Всього	**100**

Викладач: Бердиченко Ірина Олегівна, кандидат юридичних наук, викладач кафедри цивільного та кримінального права і процесу ЧНУ ім. Петра Могили. Професор Міжнародної Кадрової Академії. Працювала в слідчих підрозділах та кіберполіції. На цей час перебуває на державній службі в Міністерстві внутрішніх справ, де очолює підрозділ з упровадження програми інформатизації системи МВС.

Автор низки наукових праць з питань ІТ-права, кримінального права та кримінального процесу, у тому числі опублікованих у наукових періодичних виданнях іноземних держав. Особисто підготовлено навчальний посібник на тему: «Правове забезпечення кібернетичної безпеки

України». В 2016 році захистила дисертацію за спеціальністю 12.00.08 (кримінальне право та кримінологія; кримінально-виконавче право), науковий ступінь – кандидат юридичних наук. Сфера наукових інтересів – ІТ-право, кримінальне право, кримінальний процес, адміністративне право, авторське право, інформаційне право.