ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ І.І. МЕЧНИКОВА

ЕКОНОМІКО-ПРАВОВИЙ ФАКУЛЬТЕТ

КАФЕДРА ЗАГАЛЬНОПРАВОВИХ ДИСЦИПЛІН ТА
МІЖНАРОДНОГО ПРАВА

МІЖНАРОДНЕ ПРАВО ІНТЕРНЕТУ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Рівень вищої освіти : другий (магістерський)

Спеціальність: 081 «Право»

2022

УДК 341.23:004.735

Рекомендовано до друку:
Вченою радою
економіко-правового факультету,
(протокол № 5 від «26» січня 2022 р.)

Рецензенти:

Миколенко О. І., докт. юрид. наук, професор, завідувач кафедрою адміністративного та господарського права

Стрельцова Є. Д., докт. юрид. наук, доцент, завідувачка кафедрою загальноправових дисциплін та міжнародного права

Нігреєва О.О.

Міжнародне право Інтернету: методичні рекомендації до вивчення навчальної дисципліни для здобувачів другого (магістерського) рівня вищої освіти денної форми навчання спеціальності 081 «Право» / О. О. Нігреєва / Одеській національний університет імені І. І. Мечникова. Одеса: СПД Жмай, 2022. 32 с.

ЗМІСТ

1. ПОЯСНЮВАЛЬНА ЗАПИСКА

Робоча програма дисципліни «Міжнародне право Інтернету» складена відповідно до освітньо-професійної програми підготовки магістрів (другого рівня вищої освіти) за спеціальністю 081 «Право».

Предметом вивчення навчальної дисципліни є положення відповідно до структури курсу, що складається з 6 тем, які демонструють особливості дії міжнародного права для врегулювання відносин, які складаються у зв'язку із використанням Інтернету і, навіть ширше, кіберпростору. Зважаючи на універсальний характер Інтернету та відсутність державних кордонів, ефективне міжнародно-правове регулювання у цій сфері є особливо актуальним.

Міждисциплінарні зв'язки: «Міжнародне публічне право», «Міжнародне приватне право», «Проблеми взаємодії міжнародного права з правовою системою України», «Міжнародний захист прав людини».

Метою дисципліни є надання студентові ґрунтовних теоретичних знань сучасного міжнародного-правового регулювання відносин, які виникають у зв'язку із використанням Інтернету, та вироблення навичок їхнього практичного застосування. Дисципліна орієнтує на формування сучасного юридичного мислення та системи спеціальних знань у галузі ІТ-права, вміння аналізувати складні питання та продукувати оригінальні рішення, які забезпечують високу конкурентоспроможність та стабільне положення на ринку юридичних послуг.

Завданнями дисципліни є:

– опанування студентами інструментарію міжнародного права та ключових понять Інтернет-права;

– вивчення основних положень та інститутів міжнародного права, які регулюють відносини, що складаються у зв'язку з використанням Інтернету;

– розвиток навичок роботи з першоджерелами, зокрема, міжнародними договорами, рішеннями міжнародних організацій, як-то: розуміння студентами основних понять, орієнтація у змісті договору, його тлумачення;

– формування у студентів вміння комплексного та глибокого аналізу спірних та проблемних ситуацій, що обумовлені специфікою кіберпростору та потребують оригінальних правових рішень;

– розуміння студентами основних тенденцій розвитку міжнародного права щодо регулювання відносин у кіберпросторі.

Міжнародне право взагалі та курс «Міжнародне право Інтернету» зокрема являють собою досить складні навчальні дисципліни. Це обумовлено великим обсягом матеріалу, який мають засвоїти студенти. Крім того, багато положень міжнародного права є дискусійними, що, як наслідок, спричиняє наявність різних, а іноді й цілковито протилежних точок зору з

одного питання. Отже, у процесі вивчення курсу принципову роль відіграють лекційні заняття, у рамках яких студенти за допомогою викладача знайомляться з найважливішими положеннями міжнародного права, що регулюють відносини, які складаються у зв'язку із використанням Інтернету, та можуть зорієнтуватись у розумінні складних дискусійних тем та питань. Більш поглибленому вивченню та засвоєнню матеріалу сприяють практичні заняття, основний час яких присвячується розв'язанню задач із міжнародного права Інтернету та заслуховуванню доповідей та рефератів. Для якісного вивчення та закріплення матеріалу вкрай необхідною є наполеглива самостійна робота студента. Задля полегшеного структурованого опанування навчальною дисципліною студенти мають користуватися питаннями для самостійної роботи та заліку, наведеними у методичних рекомендаціях. Корисним для вивчення матеріалу є також надання відповідей на питання запропонованих контрольних робіт, які мають зорієнтувати та підготовити студента для підсумкового контролю наприкінці курсу. Звісно, що у процесі самостійної підготовки студенти повинні користуватися не тільки курсом лекцій, але й підручниками та іншими джерелами, зазначеними у списку рекомендованої літератури. Підсумковою формою контролю знань є складання заліку.

У результаті вивчення навчальної дисципліни студент повинен

А) знати:

- основні положення теорії міжнародного публічного права, чинне законодавство України, що стосується регулювання відносин у кіберпросторі;
- перелік джерел міжнародного права Інтернету, їх визначення та особливості;
- особливості архітектури Інтернету, її рівні та суб'єктів управління;
- основні права людини, що мають прояв у кіберпросторі, та механізми їх захисту;
- форми співробітництва держав у боротьбі із кіберзлочинністю;

Б) уміти:

- орієнтуватися у сучасних підходах до визначення міжнародно-правового режиму кіберпростору;
- коректно застосовувати міжнародно-правову юридичну термінологію;
- розрізняти поняття кібервійни та кібертероризму;
- уміти визначати особливості міжнародного співробітництва щодо протидії міжнародній кіберзлочинності;
- ефективно та доречно користуватися міжнародними актами при вирішенні юрисдикційних питань щодо Інтернет-відносин.

2. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7
Змістовий модуль 1. Теоретичні основи						
1. Міжнародне право Інтернету: поняття та основні характеристики	22	2	2			18
2. Міжнародно-правові питання управління Інтернетом	24	4	2			18
Змістовий модуль 2. Захист прав людини та держави від порушень у кіберпросторі						
3. Права людини та Інтернет	24	4	2			18
4. Право міжнародної безпеки та Інтернет	22	2	2			18
5.Відповідальність за скоєння кіберзлочинів: питання юрисдикції та міжнародне співробітництво	21	2	2			17
Змістовий модуль 3. Окремі інститути міжнародного права Інтернету						
6. Міжнародно-правові аспекти обігу кріптоактивів	22	2	2			18
Усього годин	135	16	12			107

3. ЗМІСТ ЛЕКЦІЙ, ПЛАНИ СЕМІНАРСЬКИХ ЗАНЯТЬ, МЕТОДИЧНІ ВКАЗІВКИ ДЛЯ САМОСТІЙНОЇ РОБОТИ СТУДЕНТІВ

Тема 1. Міжнародне право Інтернету: поняття та основні характеристики

Лекція

Поняття мережі Інтернет, її розмежування із кіберпростором. Структура (архітектура) Інтернету, учасники, принципи організації. Поняття міжнародного права Інтернету, його місце у системі міжнародного права та національного права. Кіберправо як комплексне транснаціональне право. Особливості суспільних відносин, що складаються у зв'язку із використанням Інтернету та підпадають під міжнародно-правове регулювання. Предмет міжнародного права Інтернету, його об'єкти, суб'єкти та джерела. Інтернет між global common та загальною спадщиною людства.

Семінарське заняття

1. Поняття мережі Інтернет та кіберпростору.
2. Поняття міжнародного права Інтернету, його місце у системі міжнародного права та національного права.
3. Предмет та об'єкти міжнародного права Інтернету.
4. Суб'єкти міжнародного права Інтернету.
5. Джерела міжнародного права Інтернету.

Контрольні запитання до семінарського заняття

1. Визначте міжнародно-правовий режим кіберпростору.
2. Які основні принципи побудови Інтернету Ви знаєте?
3. Охарактеризуйте кіберправо, зокрема у контексті теорії транснаціонального права.
4. Яка роль «м'якого права» у регулюванні міжнародних відносин, що складаються в Інтернеті?
5. Яку роль відіграють кодекси поведінки соціальних мереж у регулюванні Інтернет-відносин?

Методичні вказівки до вивчення питань теми

Використання Інтернету стає усе більш актуальним, якщо не сказати, незамінним, у багатьох сферах людського буття. Правове регулювання відносин, які виникають у зв'язку з його застосуванням, однак, часто залишається недосконалим, особливо, коли мова йде про регулювання міжнародних відносин. Адже, як відомо, міжнародна правотворчість є доволі складним та довготривалим процесом. Водночас ціла низка інститутів сучасного міжнародного права може бути, хоча і з певними модифікаціями, застосована для регулювання Інтернет-відносин. Проте, перш ніж перейти до їх розгляду, слід зупинитися на розмежуванні таких понять, як «Інтернет», «кіберпростір», «віртуальна реальність», «всесвітнє павутиння» тощо, які часто використовуються як синоніми, хоча й не є ідентичними. Це особливою мірою стосується поняття кіберпростору, яке є ширшим, ніж поняття Інтернету. Його можна розглядати саме як «простір», хоча й не в його класичному фізичному розумінні. Мережа Інтернет − тільки одна з мереж, що може забезпечувати його функціонування. Цікаво у цьому аспекті проаналізувати відповідні дефініції у Законах України «Про основні засади забезпечення кібербезпеки України» (2017) та «Про електронні комунікації» (2021). У цьому курсі термін «Інтернет» як найбільш поширений буде застосовуватися скоріше як синонім більш широкого терміну «кіберпростір», адже ми будемо вивчати не тільки норми, які регулюють безпосередньо функціонування мережі, але й ті, що забезпечують регулювання різноманітних відносин, що виникають у зв'язку із використанням Інтернету (та інших аналогічних мереж) у кіберпросторі.

Міжнародне право Інтернету проходить тільки етап свого становлення як автономної структурної одиниці міжнародного права. Як правило, частіше за все питання, які входять до його предмета, розглядають у рамах міжнародного інформаційного права, що дозволяє наразі розуміти його як інститут відповідної галузі. Разом з тим необхідно розмежовувати його із більш широким поняттям кіберправа, якому через змішаний публічно-правовий характер відносин, що часто потребують одночасного регулювання засобами як міжнародного, так і національного права, приписують характер комплексного транснаціонального права. Варто зупинитися на розгляді цієї дискусійної юридичної категорії.

Повноцінне уявлення про міжнародне право Інтернету може дати здобувачам звернення до таких його характеристик, як предмет, об'єкти, суб'єкти та джерела. Слід розуміти, що Інтернет як мережа сам є об'єктом міжнародного права. Зважаючи на новітній характер міжнародного права Інтернету, йому властиві нетипові суб'єктний склад (велике місце серед суб'єктів займають міжнародні нерядові організації) та джерельна база (невелика кількість міжнародних договорів та практична відсутність міжнародних звичаїв зумовлюють дуже важливе значення «м'яко-правових» інструментів).

Рекомендована література та нормативні матеріали

1. Пазюк А. В. Міжнародне інформаційне право: теорія та практика: монографія. Дніпропетровськ: Середняк Т. К., 2015. 447 с. С. 205−311.
2. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: автореф. дис…. канд. юрид. наук:12.00.11. Київ, 2009. 21 с.
3. Нігреєва О. Щодо питання про міжнародно-правовий режим кіберпростору. *Матер. Міжн. наук.-практ. конф. «IT право: проблеми і перспективи розвитку в Україні*» (Львів, 27.11. 2020). URL: http://aphd.ua/publication-785/
4. Segura-Serrano, Antonio. Internet Regulation and the Role of International Law. *Max Planck Yearbook of United Nations Law,* Volume 10, 2006. P. 191−272.
5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 (дата оновлення: 15.12.2021). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
6. Про електронні комунікації: Закон України від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text .

Тема 2. Міжнародно-правові питання управління Інтернетом

Лекція

Історія виникнення Інтернету та формування регулювання у цій сфері. Суб'єкти управління Інтернетом. Принципи управління Інтернетом. Моделі управління Інтернетом. Особливості зміни моделі саморегулювання Інтернету на модель національно- та міжнародно-правового регулювання. Глобальне адміністративне право та кіберпростір. Особливості здійснення національної юрисдикції в кіберпросторі, екстериторіальна юрисдикція. Роль США в управлінні кореневими серверами. Правовий базис здійснення екстериторіальної юрисдикції США стосовно управління Інтернетом. Доктрина «політичного питання» у контексті здійснення екстериторіальної юрисдикції. Статус ІКАНН. Особливості взаємодії ІКАНН та локальних Інтернет-реєстраторів. Особливості адміністрування національних доменів «укр» та «ua».

Семінарське заняття

1. Історія виникнення Інтернету та формування регулювання у цій сфері.

2. Суб’єкти та принципи управління Інтернетом.
3. Моделі управління Інтернетом.
4. Особливості здійснення національної юрисдикції в кіберпросторі, екстериторіальна юрисдикція.
5. Роль США та ІКАНН в управлінні Інтернетом.

Контрольні запитання до семінарського заняття

1. Охарактеризуйте основні моделі управління Інтернетом та визначте найбільш ефективну з них, на Ваш погляд.
2. Які принципи управління Інтернетом Ви знаєте? Які з них є найбільш значущими, на Ваш погляд?
3. Що таке глобальне адміністративне право? Визначите його ключові ознаки та особливості.
4. Визначте правовий статус ІКАНН.

Методичні вказівки до вивчення питань теми

Формування певного міжнародно-правового регулювання відносин, пов’язаних із використанням кіберпростору безпосередньо залежить від моделі управління Інтернетом зокрема та кіберпростором узагалі. Для того, щоб правильно зрозуміти його еволюцію та перспективи розвитку, необхідно звернутися до історії утворення мережі Інтернет та етапів розширення, які вона пройшла до теперішнього часу. У цьому контексті слід приділити увагу суб’єктам та принципам управління мережею. Серед них особливу роль відіграють поки що міжнародні неурядові організації, так як ІКАНН (Інтернет-корпорація з асигнування назв та номерів), Рада з архітектури Інтернету, Консорціум всесвітнього павутиння тощо. Саме це вплинуло на те, що провідною моделлю управління Інтернетом з моментом його виникнення була саме модель саморегулювання. Проте невпинне зростання кількості питань, які потребують державного втручання (захист прав людини у мережі, кібербезпека та кіберзлочинність тощо), невблаганно спричинює зміну моделі управління Інтернетом. Наразі існує декілька пропозицій щодо того, якою вона має бути. Цікаво, аби студенти дослідили їх та сформували власну позицію.

Із моделлю управління пов’язане також питання здійснення національної юрисдикції у кіберпросторі. У цьому зв’язку студенти мають орієнтуватися у різновидах юрисдикції, знати особливості здійснення не тільки територіальної, але й екстериторіальної юрисдикції. Адже саме її прояви можна спостерігати, аналізуючи роль, яку відіграють США у питаннях управління Інтернетом (за межами власної території), з огляду на

те, що переважна кількість кореневих серверів, які утворюють основу мережі, та ІКАНН, організація, яка управляє ними, знаходяться на території США.

Для того, щоб краще розуміти функціонування Інтернету та системи доменних імен, необхідно звернути увагу на правовий статус на функції ІКАНН, вивчити принципи її взаємодії із регіональними та локальними Інтернет-реєстраторами. У цьому зв'язку цікаво звернутися до питання адміністрування національних доменів «укр» та «ua» та з'ясувати правовий статус і принципи роботи об'єднання підприємств «Український мережевий інформаційний центр» та ТОВ «Хостмастер».

Рекомендована література та нормативні матеріали

1. Мицик В. В., Бурменський М. В., Гнатовський М. М. Міжнародне публічне право: підручник. Харків : Право. Т. 2. Основні галузі. 2018. 624 с. С. 54−73; 578−580.
2. Пазюк А. В. Міжнародне інформаційне право: теорія та практика: монографія. Дніпропетровськ: Середняк Т. К., 2015. 447 с. С. 205−311.
3. Спасибо І. А. Щодо історії виникнення глобальної мережі Інтернет. *Право та інновації.* 2014. № 3 (7). С. 15−25.
4. Segura-Serrano, A. Internet Regulation and the Role of International Law. *Max Planck Yearbook of United Nations Law.* Volume 10. 2006. P. 191−272.
5. Declaration by the Committee of Ministers on Internet Governance Principles: Adopted by the Committee of Ministers of the Council of Europe on 21 September 2011. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cc2f6
6. NETmundial Multistakeholder Statement: April, 24th 2014. URL: https://netmundial.br/netmundial-multistakeholder-statement/

Тема 3. Права людини та Інтернет

Лекція

Інтернет як засіб для здійснення прав людини. Особливості здійснення основних прав та свобод людини в Інтернеті. Права «цифрового покоління». Право на доступ до Інтернету як фундаментальне право людини. Право людини на інформацію та право на розвиток. Інтернет-права та свободи людини у контексті Конвенції про захист прав людини та основних свобод 1950 р. Практика ЄСПЛ. Специфіка реалізації прав інтелектуальної власності в Інтернеті. Механізми та засоби правового захисту прав людини в Інтернеті. Питання відповідальності власників сайтів та Інтернет-провайдерів.

Семінарське заняття

1. Особливості здійснення основних прав та свобод людини в Інтернеті.
2. Право на доступ до Інтернету, право на інформацію та право на розвиток як фундаментальні права людини.
3. Інтернет-права та свободи людини у контексті Конвенції про захист прав людини та основних свобод 1950 р.
4. Специфіка реалізації прав інтелектуальної власності в Інтернеті.
5. Механізми та засоби правового захисту прав людини в Інтернеті.

Контрольні запитання до семінарського заняття

1. Які перспективи визнання права на доступ до Інтернету невід'ємним правом людини? Які механізми його захисту?
2. У чому полягає принцип мережевої нейтральності? Які «за» та «проти» його закріплення у міжнародному праві Інтернету?
3. Наведіть перелік Інтернет-прав людини, на які поширюється режим Конвенції про захист прав людини та основних свобод 1950 р.
4. Охарактеризуйте моделі відповідальності Інтернет-провайдерів, застосовані у різних країнах світу. Яка з них, на Вашу думку, більш ефективна?

Методичні вказівки до вивчення питань теми

Права людини проголошені однією з основних цінностей сучасного світу. Їх ефективний захист не стає менш актуальним, якщо ці права порушують в Інтернеті. З цього приводу Рада Європи у низці документів наголошує на тому, що права людини онлайн дорівнюють правам людини оффлайн, а отже, можуть бути так само захищені.

Слід звернути увагу на те, що поява та поширення Інтернету прискорили формування так званого «цифрового» покоління прав людини. У його контексті особливого значення отримало право на доступ до Інтернету. Хоча воно ще не визнане невід'ємним правом людини на універсальному рівні (є тільки регіональні або поодинокі національні спроби), стає очевидним, що від доступу до Інтернету у наш час залежить також реалізація цілої низки інших прав людини. Отже, право на доступ до Інтернету відіграє подвійну роль самостійного права та засобу для здійснення інших прав людини. У цьому контексті воно також безпосередньо пов'язане з правом людини на доступ до інформації та правом на розвиток. Ісі ці категорії є дуже багатогранними, що ускладнює їх чітку правову регламентацію та обумовлює актуальність подальших досліджень. Суміжним зі згаданим правом на доступ

є й принцип мережевої нейтральності, відповідно до якого Інтернет-провайдери не мають надавати перевагу одному контенту поряд з іншим. Важливо звернути увагу на спроби деяких країн, зокрема, США, усе більше обмежувати застосування цього принципу.

Захисту Інтернет-прав людини приділено особливу увагу на європейському рівні, зокрема, завдяки зусиллям Ради Європи та ЄСПЛ. Практика останнього свідчить про те, що низка статей Європейської конвенції про захист прав людини і основоположних свобод 1950 р. може бути застосована також до порушень в Інтернеті. У цьому зв'язку протягом підготовки студенти мають зосередитися на положеннях ст. 8−11, 14 конвенції та ст. 1 Протоколу № 12 до конвенції, а також відповідних рішеннях суду.

Для більш повного розуміння теми варто звернутися також до специфічних аспектів реалізації прав інтелектуальної власності в Інтернеті. Для цього необхідно згадати основні об'єкти права інтелектуальної власності, що мають свій прояв у мережі. Серед них найбільше питань викликає визначення правової природи та регулювання сайтів та доменних імен.

Нарешті, одним із важливіших питань теми є питання про механізми та засоби для захисту прав людини, що були порушені у кіберпросторі. Серед механізмів виокремлюють судовий захист, захист в адміністративному порядку та самозахист, які, безсумнівно, можуть поєднуватися між собою. Необхідно також знати більш конкретні засоби захисту порушених прав, до яких, наприклад, можна віднести роз'яснення, розслідування, виправлення контенту, видалення/поновлення контенту тощо. У зв'язку з останніми постає питання відповідальної особи: автора контенту, власника сайту, Інтернет-провайдера. Найбільше питань викликає відповідальність останніх, адже у країнах світу застосовуються різні моделі правового інституту відповідальності провайдерів. Важливо ознайомитися з ними та визначити модель, характерну для України.

Рекомендована література та нормативні матеріали

1. Посібник з прав людини для Інтернет-користувачів та пояснювальний меморандум: Рекомендація CM/Rec (2014) Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум. Київ : Інжиніринг, 2015. 56 с. URL: https://rm.coe.int/16802e3e96
2. Правове регулювання відносин у мережі Інтернет : монографія / за ред. С. В. Глібка, К. В. Єфремової. Харків : Право, 2016. 360 с. С. 166−193.
3. Швидка Т., Ніколенко А. Законодавче закріплення права на доступ до Інтернету. *Підприємництво, господарство і право*. 2021. № 5. С. 145−150.
4. Конвенція про захист прав людини і основоположних свобод 1950 р. URL: http://zakon1.rada.gov.ua/laws/show/995_004 .

5. Поощрение, защита и осуществление прав человека в Интернете от 14.07.2014: Резолюция № 26/13, Совет по правам человека. URL: https://digitallibrary.un.org/record/775322?ln=ru
6. Резолюція Генеральної Асамблеї ООН про право на розвиток № A/ RES/67/171 від 20.12.2012. URL: http://daccess-dds-ny.un.org/ doc /UNDOC/GEN/N12/488/88/PDF/N1248888.pdf?OpenElement

Тема 4. Право міжнародної безпеки та Інтернет

Лекція

Поняття міжнародної безпеки та її складові, загрози міжнародній безпеці у кіберпросторі. Кібербезпека як складова національної та міжнародної безпеки Особливості застосування сили (як правомірного, так і неправомірного) у кіберпросторі. Різновиди кібератак, питання їх атрибуції. Питання здійснення збройного нападу та самооборони. Розрізнення понять гібридної війни, інформаційної війни, кібервійни та кібертероризма. Особливості застосування міжнародного гуманітарного права до Інтернет-відносин. Специфіка засобів ведення збройних конфліктів із застосуванням кіберпростору. Поняття та види кіберзброї. Перспективи притягнення до міжнародно-правової відповідальності за здійснення міжнародних злочинів, зокрема, агресії, із застосуванням Інтернету.

Семінарське заняття

1. Кібербезпека як складова національної та міжнародної безпеки.
2. Особливості застосування сили (як правомірного, так і неправомірного) у кіберпросторі.
3. Розрізнення понять гібридної війни, інформаційної війни та кібервійни.
4. Розрізнення понять кібервійни та кібертероризма.
5. Особливості застосування міжнародного гуманітарного права до Інтернет-відносин.

Контрольні запитання до семінарського заняття

1. Як можна кваліфікувати кібератаки, що здійснюються у мережі Інтернет?
2. Чи припустимо здійснення права на самооборону у відповідь на кібератаки? Якщо так, за яких обставин?
3. Що є «зброєю» у кіберконфліктах?
4. Які визначальні ознаки відрізняють кібервійну та кібертероризм?

5. Охарактеризуйте правовий статус учасників кіберконфліктів з точки зору міжнародного гуманітарного права.

Методичні вказівки до вивчення питань теми

Питання національної та міжнародної безпеки мають для більшості держав першочергове значення. Якщо традиційно основним компонентом безпеки вважали саме військовий, то наразі концепт безпеки включає ще й інші складові. Серед них питання кібербезпеки стає дедалі більш актуальним, адже кількість кібератак, яких зазнає більшість країн світу, зростає щороку. У світі переважають два основні підходи до кібербезпеки: її розгляд у розрізі військової безпеки або цивільної безпеки. Переважає перший, що можна спостерігати і в Україні. Так, у 2021 р. у системі Міністерства оборони України було вирішено створити кібервійська.

Основними питаннями, які постають у контексті міжнародного права стосовно міжнародної кібербезпеки, є питання щодо кваліфікації кібератак як збройних нападів та можливості застосування збройної сили у порядку самооборони. Вичерпної відповіді на них поки що немає, адже у зв'язку із кібератаками виникає низка складних теоретичних та практичних питань, пов'язаних із їх атрибуцією певним суб'єктам, із визначенням критеріїв, які могли б допомогти встановити поріг, коли певна кібератака дійсно може бути порівняна із застосуванням збройної сили, тощо. У цьому контексті студентам важливо вміти розрізняти кібератаку та кіберінцидент.

Крім того, дуже часто здійснення масових та систематичних кібератак пов'язують із терміном «кібервійна», а той, у свою чергу, плутають із поняттями «гібридна війна» та «інформаційна війна». Важливо вміти відрізняти ці терміни та розуміти, що вони не визначені у нормах міжнародного права.

Не менш важливо розмежовувати поняття кібервійни та кібертероризму, адже вони відрізняються за суб'єктами скоєння, рівнем агресивності та шкодою і, у результаті, тягнуть різні юридичні наслідки для винних. Адже, як відомо, агресія є міжнародним злочином, а тероризм − злочином міжнародного характеру.

Нарешті, проведення військових операцій у кіберпросторі викликає питання щодо можливості застосування до них норм міжнародного гуманітарного права. На думку спеціалістів Міжнародного комітету Червоного Хреста, це є можливим. Однак потрібно розуміти, що перенесення норм міжнародного гуманітарного права на операції у кіберпросторі не може бути автоматичним та породжує низку теоретичних і практичних запитань, як-то: визначення статусу учасників таких операцій, вдосконалення переліку заборонених засобів та методів ведення війни тощо.

Рекомендована література та нормативні матеріали

1. Пазюк А. В. Міжнародне інформаційне право: теорія та практика: монографія. Дніпропетровськ: Середняк Т. К., 2015. 447 с. С. 205−311.
2. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека”. *Правова інформатика*. 2014. № 2(42). С. 54−62
3. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *The Journal of Eastern European Law*. 2018. № 53. С.26-37.
4. Грицун О. О. Правовий аналіз використання кіберпростору у воєнних цілях. *Актуальні проблеми міжнародних відносин*. 2015. Вип. 124 (Ч. І). С. 112−121.
5. Яцишин М.Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право.* 2018. № 4(27). С. 22−31
6. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 (дата оновлення: 15.12.2021). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

Тема 5. Відповідальність за скоєння кіберзлочинів: питання юрисдикції та міжнародне співробітництво

Лекція

Транснаціональне кримінальне право та кіберпростір. Поняття транснаціонального злочину (конвенційного злочину, злочину міжнародного характеру), його відмінність від міжнародного злочину. Поняття та види кіберзлочинів. Нові види кіберзлочинів (кардинг, фішинг, вішинг, скімінг, шимінг, рефайлінг, грумінг тощо). Юрисдикційні питання стосовно притягнення до відповідальності за скоєння кіберзлочинів. Універсальна юрисдикція. Особливості притягнення до відповідальності за кібертероризм. Міжнародне співробітництво в боротьбі із кіберзлочинністю (зокрема, у рамках міжнародних організацій). Форми співпраці за Конвенцією про кіберзлочинність 2001 р.

Семінарське заняття

1. Транснаціональне кримінальне право у кіберпросторі.
2. Поняття та види кіберзлочинів.
3. Юрисдикційні питання стосовно притягнення до відповідальності за кіберзлочини.
4. Особливості притягнення до відповідальності за кібертероризм.

5. Міжнародне співробітництво в боротьбі із кіберзлочинністю (зокрема, у рамках міжнародних організацій).

Контрольні запитання до семінарського заняття

1. Що таке транснаціональне кримінальне право? Які його відмінності від міжнародного кримінального права?
2. Які нові види кіберзлочинів Ви знаєте? Що таке кардинг, фішинг, вішинг, скімінг шимінг, рефайлінг тощо?
3. У чому проблема кодифікації норм щодо тероризму у міжнародному праві? Хто може притягати до відповідальності за кібезтероризм?
4. Які форми взаємної правової допомоги держав у боротьбі із кіберзлочинністю є більш ефективними?

Методичні вказівки до вивчення питань теми

Людській історії з давніх часів були відомі злочини, які мали міжнародний характер. Однак в останні десятиріччя на тлі глобалізаційних процесів їх кількість значно зросла, що обумовило формування та відокремлення такої підгалузі міжнародного кримінального права, як транснаціональне кримінальне право. Його норми спрямовані на боротьбу із міжнародною злочинністю та на забезпечення притягнення до відповідальності за скоєння злочинів міжнародного характеру (інакше: транснаціональних або конвенційних). Важливо не плутати їх із міжнародним злочинами. Ці дві категорії відрізняються за низкою ознак, серед яких однією з головних є неможливість притягнення до відповідальності за скоєння транснаціональних злочинів у міжнародних судах. Як наслідок, за них засуджують за національним правом держав та притягають до відповідальності у національних судових інституціях. Саме до цієї групи відносяться кіберзлочини.

Здобувачі повинні знати ключові ознаки складу кіберзлочинів та їх основні види. Потрібно звернути увагу на те, що існують вузький та широкий підходи до визначення кіберзлочинів. Відповідно до них, до цього поняття можуть потрапляти або виключно злочини проти конфіденційності, цілісності та доступності комп'ютерних систем та даних (вузький підхід), або ж й інші злочини, які пов'язані із застосуванням комп'ютерів та Інтернету, змістом інформації, розміщеної у кіберпросторі, з порушенням прав інтелектуальної власності (широкий підхід). Цікаво дослідити та визначитись із кримінально-правовою кваліфікацією таких нових видів кіберзлочинів, як кардинг, фішинг, вішинг, скімінг, шимінг, рефайлінг, грумінг тощо

Зважаючи на необхідність притягнення кіберзлочинців до відповідальності у національних судах, особливо гостро постає питання

визначення юрисдикції певної держави, адже інколи злочин може бути скоєно громадянином однієї держави на території іншої, завдавши шкоди інтересам громадян третьої держави. У таких ситуаціях можливий як позитивний, так і негативний конфлікт юрисдикцій. Студенти мають встановити, які підходи до визначення юрисдикції відображено у Конвенції про кіберзлочинність 2001 р., та відповісти на питання щодо їх ефективності у сучасних умовах.

Рекомендована література та нормативні матеріали

1. Ануфрієв М.І., Кісілевич-Чорнойван О. М. Міжнародно-правові засади співробітництва у боротьбі з кіберзлочинами. *Наше право.* 2017. №3. С. 45−50.
2. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і безпека.* 2011. № 4 (41). С. 107−112.
3. Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104−110.
4. Трофименко В. А., Мішанчук А. В. Кібертероризм: спроба філософсько-правового осмислення. *Вісник НЮУ імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2021. № 2(49). С. 93−104.
5. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права.* 2009. № 2. С. 434–441.
6. Конвенція Ради Європи про кіберзлочинність 2001 р. (ратифікація Україною: 07.09.2005; набрання чинності: 01.07.2006). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text

Тема 6. Міжнародно-правові аспекти регулювання обігу криптоактивів

Лекція

Засади функціонування технології блокчейну та криптовалют. Історія виникнення. Поняття, види та правовий статус криптоактивів. Особливості обігу глобальних стейблкойнов. Первинні засоби придбання криптоактивів: майнінг, форжинг (мінтінг), ICO як вид краудфандінгу. Вторинні засоби придбання криптоактивів. Основи міжнародно-правового регулювання криптоекономіки. Міжнародно-правове регулювання боротьби із фінансування злочинної діяльності та відмиванням грошей за допомогою крипто активів. Рекомендації ФАТФ. Діяльність постачальників послуг,

пов’язаних з оборотом криптоактивів (криптобірж та криптообмінників). Міжнародна кіберзлочинність у сфері обігу криптовалют. Практика органів міжнародного та національного правосуддя стосовно криптовалют. Вирішення спорів онлайн через блокчейн інституції та децентралізоване правосуддя. Особливості правового регулювання обігу криптовалют в Україні та інших країнах. Проект Закону України про віртуальні активи 2021 р.

Семінарське заняття

1. Історія виникнення криптоактивів.
2. Поняття, правовий статус криптоактивів та способи їх придбання.
3. Міжнародно-правове регулювання боротьби із фінансування злочинної діяльності та відмиванням грошей за допомогою криптоактивів, рекомендації ФАТФ.
4. Міжнародна кіберзлочинність у сфері обігу криптоактивів.
5. Особливості правового регулювання обігу криптоактивів в Україні та інших країнах.

Контрольні запитання до семінарського заняття

1. Що таке блокчейн та де він застосовується?
2. Які первинні засоби придбання криптовалюти Вам відомі? Що таке майнінг, форджинг (мінтінг), ICO як вид краудфандінгу?
3. Що таке віртуальні активи?
4. Які моделі правового регулювання криптовалюти Вам відомі? Яка з них, на Вашу думку, є оптимальною?
5. Надайте характеристику смарт-контрактам, їхнім умовам, принципу дії та засобам забезпечення.

Методичні вказівки до вивчення питань теми

Стрімке поширення біткойну, починаючи з 2009 р., та поява інших криптовалют обумовлює необхідність ефективного правового регулювання цього виду активів не тільки на національному, але на міжнародному рівні. Наразі у цій справі переважає національне законодавство, яке, однак, демонструє дуже різні підходи до регулювання криптоактивів: від повного невизнання та заборони до майже неврегульованого та необмеженого обігу.

Така ситуація не може не створювати проблеми, які вимагають міжнародно-правового вирішення, адже відносини, які виникають у зв’язку з обігом криптовалют, як правило, обтяжені іноземним елементом. Як

наслідок, вони не тільки потребують механізмів вибору юрисдикції, але часто породжують проблеми застосування матеріального права. Зокрема, це пов'язано з вирішенням інвестиційних та торговельних спорів, які, можна припустити, почнуть виникати у великій кількості.

Інший аспект, який потребує регулювання саме у міжнародному праві, − боротьба із злочинністю та відмиванням грошей. У цьому аспекті студенти мають звернути особливу увагу на Рекомендації ФАТФ (Групи з розроблення фінансових заходів боротьби з відмиванням грошей). Крім того, на цей момент зростає кількість кіберзлочинів, чиїм об'єктом або предметом є власне криптоактиви.

Для глибокого вивчення теми слід розпочати з визначення криптоактивів та розуміння технології блокчейну, який наразі стає усе ширше застосованим не тільки стосовно криптовалют, але й у інших сферах, як-то: перевезення вантажів, вирішення спорів онлайн, збереження речових доказів при розгляді спорів у судах, смарт-контракти тощо.

Важливо розуміти, що криптоактиви не одноманітні. Їх можна поділяти на децентралізовані та централізовані, на незабезпечені та забезпечені, на такі, що базуються на публічному та непублічному реєстрах, тощо. Усі вони потребують різного правового регулювання. На особливу увагу з точки зору міжнародного права заслуговують так звані глобальні стейблкойни (зокрема, Libra).

Студенти мають знати первинні та вторинні способи придбання криптовалют, розуміти, у чому полягають особливості майнінгу, форжингу (мінтінгу), ICO як виду краудфандінгу. Цікавим питанням є укладання договорів стосовно криптоактивів та їх спадкування.

У контексті функціонування вторинних засобів придбання криптоактивів та їх переведення у готівку необхідно розуміти особливості правового статусу та діяльності провайдерів послуг з їх адміністрування та обміну − так званих криптобірж та криптообмінників. Зважаючи на важливу роль, які вони можуть відігравати у процесі контролю за відповідними транзакціями та ідентифікації власників криптоактивів, рекомендації ФАТФ (див. рекомендацію № 15) містять на зобов'язання держав щодо встановлення процедур їх реєстрації та ліцензування діяльності, а також здійснення подальшого надзору та моніторингу.

Слід відмітити, що відповідні рекомендації були враховані при розробці проекту закону України «Про віртуальні активи» (2021), із яким студентам також варто ознайомитися. Окрему увагу слід приділити правову статусу криптоактивів, який запропоновано цим документом, та зазначеним вище вимогам щодо постачальників послуг з адміністрування та обміну віртуальних активів. За можливості корисним буде також звернутися до правового регулювання обігу криптоактивів у інших країнах.

Рекомендована література та нормативні матеріали

1. Казначеєва Д. В. Дорош А. О. Кримінальні правопорушення у сфері обігу криптовалюти. *Вісник Кримінологічної асоціації України*. 2021. №2 (25). С. 149−157.
2. Казначеєва Д. В., Дорош А. О. Криптовалюта: проблеми правового регулювання. *Вісник Кримінологічної асоціації України.* № 2 (23). 2020. С. 171−176.
3. Нігреєва О. О. Криптоактиви як інвестиція крізь призму тесту Саліні. *Актуальні шляхи вдосконалення українського законодавства: збірник тез допов. XIV Всеукр. наук.-практ. конф.* Харків, 2021. С. 136−139.
4. Розвінчуємо міфи про законопроект «Про віртуальні активи»: Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/news/rozvinchuemo-mifi-pro-zakonoproekt-pro-virtualni-aktivi
5. Про віртуальні активи: Проект Закону України від 08.09.2021 (прийнято та відправлено на доопрацювання). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110
6. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012-2020, FATF. URL: www.fatf-gafi.org/recommendations.html

4. КОНТРОЛЬНІ ПИТАННЯ З НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Поняття кіберпростору та мережі Інтернет.
2. Поняття міжнародного права Інтернету.
3. Місце міжнародного права Інтернету у системі міжнародного та національного права.
4. Кіберправо як комплексне транснаціональне право.
5. Предмет міжнародного права Інтернету.
6. Об'єкти міжнародного права Інтернету.
7. Суб'єкти міжнародного права Інтернету.
8. Джерела міжнародного права Інтернету.
9. Історія виникнення Інтернету та формування регулювання у цій сфері.
10. Суб'єкти управління Інтернетом.
11. Моделі управління Інтернетом.
12. Особливості зміни моделі саморегулювання Інтернету на модель національно- та міжнародно-правового регулювання.
13. Особливості здійснення національної юрисдикції в кіберпросторі, екстериторіальна юрисдикція.
14. Роль США в управлінні кореневими серверами.
15. Статус ІКАНН як основної організації з управління Інтернетом.
16. «Цифрове» покоління прав людини.
17. Право на доступ до Інтернету як фундаментальне право людини.
18. Інтернет як засіб для реалізації прав та свобод людини.
19. Особливості здійснення основних прав та свобод людини в Інтернеті.
20. Специфіка реалізації прав інтелектуальної власності в Інтернеті.
21. Правові механізми захисту прав і свобод людини в Інтернеті.
22. Відповідальність власників сайтів та провайдерів.
23. Практика ЄСПЛ щодо захисту прав людини у Інтернеті.
24. Кібербезпека як складова міжнародної та національної безпеки.
25. Загрози міжнародній безпеці у кіберпросторі.
26. Особливості застосування сили (як правомірного, так і неправомірного) у кіберпросторі.
27. Поняття гібридної війни, інформаційної війни та кібервійни.
28. Розрізнення кібервійни та кібезтероризма.
29. Особливості застосування міжнародного гуманітарного права до Інтернет-відносин.
30. Перспективи притягнення до міжнародно-правової відповідальності за міжнародні злочини, зокрема, агресію, із застосуванням Інтернету.
31. Транснаціональне кримінальне право у кіберпросторі.
32. Поняття кіберзлочинів.
33. Класифікація кіберзлочинів.
34. Нові види кіберзлочинів
35. Юрисдикція щодо притягнення до відповідальності за кіберзлочини.

36. Особливості здійснення міжнародного співробітництва в боротьбі із кіберзлочинністю
37. Міжнародне співробітництво в боротьбі із кіберзлочинністю у рамках міжнародних організацій.
38. Форми взаємної правової допомоги держав у боротьбі із кіберзлочинністю.
39. Особливості притягнення до відповідальності за кібертероризм.
40. Засади функціонування технології блокчейну та криптоактивів.
41. Поняття та правовий статус крипто активів.
42. Різновиди криптоактивів.
43. Особливості обігу та правого регулювання глобальних стейблкойнів.
44. Первинні способи придбання криптоактивів.
45. Вторинні способи придбання криптоактивів.
46. Міжнародно-правове регулювання боротьби із фінансування злочинної діяльності та відмиванням грошей за допомогою криптоактивів.
47. Особливості правового статусу та діяльності провайдерів послуг з адміністрування та обміну криптоактивів.
48. Розгляд спорів стосовно криптоактивів у міжнародних судових органах.
49. Особливості правового регулювання обігу криптоактивів в Україні та інших країнах.
50. Загальна характеристика проекту закону України «Про віртуальні активи» (2021).

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

І. Нормативні джерела

1. Міжнародні акти

1. Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20.12.1996, та положення Бернської конвенції (1971 р.), на які містяться посилання у Договорі (Договір ВОІВ про авторське право) (1996). URL: https://zakon.rada.gov.ua/laws/show/995_770#Text
2. Конвенція про захист прав людини і основоположних свобод 1950 р. (ратифікація Україною: 17.07.1997) URL: http://zakon1.rada.gov.ua/laws/show/995_004 .
3. Конвенція Ради Європи про кіберзлочинність 2001 р. (ратифікація Україною: 07.09.2005; набрання чинності: 01.07.2006). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
4. Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р. (ратифікація Україною: 06.07.2010). URL: https://zakon.rada.gov.ua/laws/show/994_326#Text
5. Міжнародна конвенція про боротьбу з актами ядерного тероризму 2005 р. (ратифікація Україною: 15.03.2006). URL: http://zakon2.rada.gov.ua/laws/show/995_d68
6. Міжнародна конвенція про боротьбу з бомбовим тероризмом 1997 р. (ратифікація Україною: 29.11.2001). URL: http://zakon2.rada.gov.ua/laws/show/995_374
7. Міжнародна конвенція про боротьбу з фінансуванням тероризму 1997 р. (ратифікація Україною: 12.09.2002). URL: http://zakon3.rada.gov.ua/laws/show/995_518
8. Римський статут Міжнародного кримінального суду 1998 р. URL: https://zakon.rada.gov.ua/laws/show/995_588#Text
9. Статут Організації Об’єднаних Націй та Статут Міжнародного Суду 1945 р. (ратифікований Указом Президії Верховної Ради СРСР 20.08.1945) URL: http://zakon2.rada.gov.ua/laws/show/995_010
10. Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту ООН 1970 р.: Прийнята 24.10.1970 Резолюцією № 2625 (XXV) Генеральної Асамблеї ООН. URL: http://zakon1.rada.gov.ua/laws/show/995_569

11. Декларація про право на розвиток: Резолюція № 41/128 Генеральної Асамблеї від 04.12.1986. URL: https://zakon.rada.gov.ua/laws/show/995_301#Text

12. Декларація про свободу комунікацій в Інтернеті: Затверджена Комітетом Міністрів Ради Європи 28.05.2003. URL: https://cedem.org.ua/library/deklaratsiya-pro-svobodu-komunikatsij-v-internet/

13. Заключний акт Наради з безпеки та співробітництва в Європі 1975 р. URL: http://zakon1.rada.gov.ua/laws/show/994_055/page1

14. Заохочення, захист та здійснення прав людини в Інтернеті від 14.07.2014: Резолюція № 26/13, Рада з прав людини. URL: https://digitallibrary.un.org/record/775322?ln=ru

15. Резолюція Генеральної Асамблеї ООН про право на розвиток № A/ RES/67/171 від 20.12.2012. URL: http://daccess-dds-ny.un.org/ doc /UNDOC/GEN/N12/488/88/PDF/N1248888.pdf?OpenElement

16. Рекомендації про розвиток та використання багатомовності та загальний доступ до кіберпростору 2003 р.: Рекомендації, прийняті Генеральною конференцією ЮНЕСКО на 32-й сесії. URL: https://en.unesco.org/sites/default/files/rus_-_recommendation_concerning_ the_ promotion_and_use_of_multilingualism_and_universal_access_to_cyberspace.pdf

17. Agreement between the Governments of State Members of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring the International Information Security of June 16, 2009. URL: https://cis-legislation.com/document.fwx?rgn=28340

18. Declaration by the Committee of Ministers on Internet governance principles: Adopted by the Committee of Ministers of the Council of Europe on 21 September 2011. URL: https://search.coe.int/cm/Pages/ result_details. aspx?ObjectID=09000016805cc2f6

19. European Parliament resolution of 15 June 2010 on internet governance: the next steps. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010IP0208

20. NETmundial Multistakeholder Statement: April, 24th 2014. URL: https://netmundial.br/netmundial-multistakeholder-statement/

21. Recommendation of the Committee of Ministers of the Council of Europe to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality: Adopted by the Committee of Ministers on 13 January 2016. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1e59\

22. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, 2012-2020, FATF. URL: www.fatf-gafi.org/recommendations.html

2. Національне законодавство

1. Конституція України від 28.06.1996 (дата оновлення: 01.01.2020). URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text
2. Кримінальний кодекс України : Закон України від 05.04.2001 (дата оновлення: 05.01..2022). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
3. Про боротьбу із тероризмом: Закон України від 20.03.2003 (дата оновлення: 01.01.2022). URL: http://zakon3.rada.gov.ua/laws/show/638-15
4. Про віртуальні активи: Проект Закону України від 08.09.2021 (прийнято та відправлено на доопрацювання). URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69110
5. Про виконання рішень та застосування практики Європейського суду з прав людини: Закон України від 23.02.2006 (дата оновлення: 02.12.2012). URL: https://zakon.rada.gov.ua/laws/show/3477-15#Text
6. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон Україна від 06.12.2019 (дата оновлення: 01.01.2022). URL: https://zakon.rada.gov.ua/laws/show/361-20#Text
7. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 (дата оновлення: 15.12.2021). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
8. Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.2007. URL:. https://zakon.rada.gov.ua/laws/show/537-16#Text
9. Про електронні комунікації: Закон України від 16.12.2020. URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text .
10. Порядок інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади: Наказ Державного комітету інформаційної політики, телебачення та радіомовлення України та Державного комітету зв'язку та інформатизації України № 327/225 від 25.11.2002. URL: https://zakon.rada.gov.ua/laws/show/z1021-02#Text
11. U.S. Principles on the Internet's Domain Name and Addressing System Domain Name System of June 30, 2005 : National Telecommunications and Information Administration of the United States Department of Commerce. URL: https://www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system

2. Основна література

1. Антонович М. М. Міжнародне право: навчальний посібник. Київ: Юрінком Інтер, 2011. 384 с.
2. Баймуратов М. О. Міжнародне публічне право: підручник. Київ : Фенікс, 2018. 762 с.
3. Гердеген М. Міжнародне право. Перек. з нім. 9-го вид., перероб. і доп. Київ : К.І.С., 2011. 516 с.
4. Грушко М. В. Атрибуція кібератак як передумова забезпечення відповідальної поведінки в кібепросторі. *Правова держава*. 2021. № 43. С. 195−201.
5. Кирилюк О. В. Міжнародно-правове забезпечення розвитку глобального інформаційного суспільства: дис. … канд. юрид. наук: 12.00.11. Київ, 2016. 247 с.
6. Казначеєва Д. В. Дорош А. О. Кримінальні правопорушення у сфері обігу криптовалюти. *Вісник Кримінологічної асоціації України*. 2021. №2 (25). С. 149−157.
7. Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право*. 2018. № 3. С. 104-110. URL: http://nbuv.gov.ua/UJRN/Infpr_2018_3_12.
8. Міжнародне кримінальне право (співробітництво держав у протидії злочинності) : підручник / В. А. Гринчак та ін.. Харків: Право, 2019. 440 с.
9. Мицик В. В., Бурменський М. В., Гнатовський М. М. Міжнародне публічне право: підручник. Харків: Право. Т. 2. Основні галузі. 2018. 624 с.
10. Мічурін Є.О., Мічурін І.Є. Криптовалюта в Україні: проблеми визнання, визначення правової природи та обмежень. *Форум права*. 2021. № 67(2). С. 46–53.
11. Нігреєва О. О. Криптоактиви як інвестиція крізь призму тесту Саліні. *Актуальні шляхи вдосконалення українського законодавства: збірник тез допов. XIV Всеукр. наук.-практ. конф.* Харків, 2021. С. 136−139.
12. Нігреєва О. Щодо питання про міжнародно-правовий режим кіберпростору. *Матер. Міжн. наук.-практ. конф. «IT право: проблеми і перспективи розвитку в Україні*» (Львів, 27 лист. 2020). URL: http://aphd.ua/publication-785/
13. Пазюк А. В. Міжнародне інформаційне право: теорія та практика: монографія. Дніпропетровськ: Середняк Т. К., 2015. 447 с.
14. Петришина М.О., Правник С.О. Право на доступ до Інтернету та його конституційно-правове регулювання у зарубіжних країнах та в Україні. *Юридичний науковий електронний журнал*. 2021. № 3. С. 62−66.
15. Посібник з прав людини для Інтернет-користувачів та пояснювальний меморандум: Рекомендація CM/Rec (2014) Комітету міністрів Ради Європи державам-членам щодо посібника з прав людини для Інтернет-користувачів та пояснювальний меморандум. Київ : Інжиніринг,

2015. 56 с. URL: https://rm.coe.int/16802e3e96

16. Правове регулювання відносин у мережі Інтернет : монографія / за ред. С. В. Глібка, К. В. Єфремової. Харків: Право, 2016. 360 с.

17. Сироїд Т. Л. Міжнародне публічне право: підручник. Одеса: Фенікс, 2018. 744 с.

18. Спасибо І. А. Щодо історії виникнення глобальної мережі Інтернет. *Право та інновації*. 2014. № 3 (7). С. 15−25.

19. Трофименко В. А., Мішанчук А. В. Кібертероризм: спроба філософсько-правового осмислення. *Вісник НЮУ імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2021. № 2(49). С. 93−104.

20. Ruotolo G. M. Internet-ional law: profile di diritto internazionale pubblico della Rete. Bari: Cacucci Editore, 2012. 168 p.

21. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет: автореф. дис…. канд. юрид. наук: 12.00.11. Київ, 2009. 21 с.

22. Юртаєва К. В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права.* 2009. № 2. С. 434–441. URL: http://www.nbuv.gov.ua/e-journals/FP/2009-2/09ykvvkt.pdf

3. Додаткова література

1. Ануфрієв М.І., Кісілевич-Чорнойван О. М. Міжнародно-правові засади співробітництва у боротьбі з кіберзлочинами. *Наше право.* 2017. №3. С. 45−50.

2. Базов О.В. Юрисдикція Європейського суду з прав людини: дис.. … канд. юрид.наук: 12.00.11. Київ, 2016. 230 с.

3. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика*, 2014, № 2(42). С. 54−62

4. Бортник Н., Єсімов С. Відносини в мережі Інтернет як об'єкт правового регулювання. *Вісник Національного університету "Львівська політехніка".* Серія: Юридичні науки, 2019, Вип. 22. С. 147–153.

5. Бурменський М. Деякі судження про поняття міжнародного кримінального права. *Вісник Академії правових наук України*. 2003. № 2(33)−3 (34). С. 359 −370.

6. Войціховський А.В. Кібербезпека як важлива складова системи захисту національної безпеки європейських країн. *The Journal of Eastern European Law*. 2018. № 53. С.26-37. URL: http://easternlaw.com.ua/wp-content/uploads/2018/07/voytsikhovskyy_53.pdf

7. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і безпека.* 2011. № 4 (41). С. 107−112.

8. Герасимчук Н. В. Функції міжнародних інституцій у підвищенні ефективності міжнародно-правового регулювання: дис.. … канд. юрид. наук: 12.00.11. Київ, 2016. 228 с.

9. Гончаренко О. А. Право доступу до Інтернету як складова прав дитини. *Право та інновації.* 2016. № 4 (16). С. 23−29.

10. Грицун О. О. Правовий аналіз використання кіберпростору у воєнних цілях. *Актуальні проблеми міжнародних відносин*. 2015. Вип. 124 (Ч. І). С. 112−121.

11. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ : НІСД, 2014. 328 с.

12. Єннан Р. Є. Правове регулювання відносин у мережі Інтернет. *IT право: проблеми і перспективи розвитку в Україні : зб. матеріалів наук.-практ. конф.* Львів : НУ «Львів. політехніка», 2016. С. 172–181. URL: http://aphd.ua/publication-173/

13. Задорожний А.В., Пазюк А. В. Международное информационное право: учебное пособие. Т. 1. Одесса: Феникс, 2013. 854 с.

14. Іванов Ю. А. Міжнародно-правове регулювання боротьби з тероризмом у сучасних умовах: дис. на здобуття ступеня канд. юрид. наук: 12.00.11. Київ, 2000. 173 с.

15. Казначєєва Д. В., Дорош А. О. Криптовалюта: проблеми правового регулювання. *Вісник Кримінологічної асоціації України*. № 2 (23). 2020. С. 171−176.

16. Логойда В.М. Правовий статус криптовалюти в країнах Азії. *Науковий вісник Ужгородського національного університету*. 2021. № 66. С. 96−102.

17. Нігреєва О.О. International Law-making Subjects in a Changing World. Legea si Viata, 2014, № 8/3. Pp. 104−106.

18. Нігреєва О.О. «М'яке право» у міжнародній системі: до питання про зміст та функції. Правова держава, 2018, № 30. С.147−153

19. Нігреєва О.О. Правотворчість у міжнародному праві: окремі питання: *Формування і розвиток правотворчості в умовах трансформації суспільства*: колект. монографія; за ред. В. П. Плавича. Одеса: Фенікс, 2018. С. 267−293.

20. Стець В. Теоретико-правові проблеми визначення сутності кібербезпеки як складової інформаційної безпеки. *Актуальні проблеми державного управління*, 2019, № 4(80)- 24−28

21. Скулиш Є.Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право*. 2014. № 1(10). С. 93−100.

22. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2(5). С.162−175.

23. Швидка Т., Ніколенко А. Законодавче закріплення права на доступ до Інтернету. *Підприємництво, господарство і право*. 2021. № 5. С. 145−150.

24. Яцишин М.Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право,* 2018. № 4(27). С. 22−31

25. Яцишин М. Ю. Сучасні тенденції у сфері міжнародно-правового регулювання кіберпростору. *Матеріали конференцій кафедри міжнародного права і порівняльного правознавства* НАУ (2013). URL: http://er.nau.edu.ua/handle/NAU/31205

26. Buttigieg, Jean. The Common Heritage of Mankind: From the Law of the Sea to the Human Genome and Cyberspace. *Symposia Melitensia*, 2012, Vol. 8. P. 81−92;

27. Eichensehr, Kristen. The Cyber-Law of Nations. *Georgetown Law Journal*. 2015. Vol. 103. P. 317−380.

28. Nihreieva O. O. The Common Heritage of Humankind and Global Commons: Interrelation between Concepts. *Правова держава*, 2020, Т. 39. С. 86−93.

29. Segura-Serrano, Antonio. Internet Regulation and the Role of International Law. *Max Planck Yearbook of United Nations Law,* Volume 10, 2006. P. 191−272.

6. МЕТОДИ НАВЧАННЯ ТА СИСТЕМА КОНТРОЛЮ ЗНАНЬ

При вивченні курсу застосовуються такі методи навчання: словесний, наочний, практичний, що передбачають лекції, роботу з учбовою та спеціальною літературою, нормативними актами, індивідуальні бесіди. З найбільш важливих тем курсу проводяться семінарські заняття. На них можуть використовуватись різні форми та методи навчання і контролю знань студентів: доповіді, експрес-опитування, доповнення відповіді, співбесіда, вільна дискусія, обговорення реферативних повідомлень, розв'язання казусів, виконання самостійних і контрольних робіт, індивідуальні завдання та інші. Рівень знань, підготовленості, ерудиції, активності студентів на семінарах викладач оцінює самостійно.

Навчальна дисципліна «Міжнародне право Інтернету» викладається за кредитно-модульною системою організації навчального процесу. Оцінювання знань студентів повинно сприяти реалізації низки завдань, зокрема: підвищенню мотивації студентів; забезпеченню відкритості контролю; подоланню суб'єктивізму при оцінюванні знань; розвитку творчого мислення студентів та підвищенню ефективності навчання. Ця дисципліна вивчається протягом одного семестру та складається з 3х змістовних модулів (ЗМ). Оцінювання знань студентів здійснюється шляхом виконання індивідуальних завдань, які включають *поточний* та *підсумковий* контроль.

Під час вивчення дисципліни здобувачі за бажанням виконують творчу роботу у вигляді наукової доповіді. Метою проведення цієї роботи є: закріплення, поглиблення і узагальнення знань, отриманих студентами під час набуття теоретичних і практичних навичок та їхнього використання при розв'язанні теоретичних і практичних завдань, пов'язаних із правовим врегулюванням міжнародних та національних відносин.

При виконанні роботи студент повинен продемонструвати вміння роботи в сфері науково-дослідної діяльності, здатність опрацювання нормативних матеріалів, вміння творчого й оригінального вирішення складних завдань. Завдання студенти виконують самостійно протягом вивчення дисципліни на тлі проведення консультацій із викладачем дисципліни відповідно до графіка навчального процесу.

Робота повинна містити такі елементи наукового дослідження, як: практична значущість; комплексний і системний підходи до вирішення поставленого завдання; використання сучасної методології та наукових розробок та досліджень за обраною темою; застосування оригінального підходу до вирішення поставленого завдання.

Викладення матеріалу має починатися із вступної частини, де студент повинен продемонструвати теоретичну та практичну значущість обраної теми, довести її актуальність. Основна частина має містити викладення необхідного матеріалу за темою. На завершення студент повинен дійти

власних висновків та надати рекомендації щодо вирішення окреслених у вступі проблем.

Оформлення доповіді має відповідати наступним вимогам.

Обсяг роботи не повинен перевищувати 7000 знаків та пробілів. Список використаної літератури має містити опрацьовані під час виконання роботи нормативні акти, теоретичні джерела із зазначенням автору чи авторів, назви роботи, року і місця видання, оформлені відповідно до вимог державного стандарту з бібліографічного опису ДСТУ 8302:2015.

Орієнтовні теми для написання наукової доповіді:

1. Статус ІКАНН як основної організації з управління Інтернетом.
2. Поняття кібервійни, її розрізнення із суміжними концептами.
3. Поняття та види кіберзлочинів.

Студенти мають право обрати тему на власний розсуд відповідно до програми курсу, попередньо узгодивши її з викладачем. Бали, отримані за виконання роботи (максимально − 20), враховуються при проведенні підсумкового контролю.

Результати роботи студентів протягом семестру оцінюються за 100-бальною системою. За результатами оцінювання змістового модуля студентам виставляються бали. Максимальна кількість балів, що може набрати студент за ЗМ дорівнює 20-ти, 30-ти та 10-ти балам. 40 балів надаються студентові у випадку успішного проходження підсумкового контролю. Під час викладання матеріалу лекцій лектор може здійснювати контрольні опитування студентів.

У випадку відсутності студента на лекції або семінарському занятті він зобов'язаний відпрацювати пропущене заняття через усне опитування в позааудиторний час (час консультацій викладача). Невідпрацьовані заняття вважаються незданими, і за них не нараховується оцінка в балах.

Таким чином, за цю дисципліну студентом може бути отримано максимально 100 балів.

РОЗПОДІЛ БАЛІВ, ЯКІ ОТРИМУЮТЬ СТУДЕНТИ

Поточне тестування та самостійна робота						Підсумковий контроль (залік)	Сума
Змістовий модуль 1		Змістовий модуль 2			Змістовий модуль 3		
Т1	Т2	Т3	Т4	Т5	Т6	40	100
10	10	10	10	10	10		
Разом: 60 балів							