МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТЕФАНИКА
НАВЧАЛЬНО-НАУКОВИЙ ЮРИДИЧНИЙ ІНСТИТУТ

Кафедра політики у сфері боротьби
зі злочинністю та кримінального права

Яцина М. О.

МЕТОДИЧНІ ВКАЗІВКИ
для підготовки до семінарських (практичних) занять
з навчальної дисципліни
«КІБЕРБЕЗПЕКА ТА МІЖНАРОДНЕ ПРАВО»
для здобувачів денної форми навчання
першого (бакалаврського) рівня вищої освіти
галузі знань 08 «Право», спеціальності 081 «Право»,
ОПП «Міжнародне та європейське право»
(7 семестр)

Івано-Франківськ – 2022

Схвалено на засіданні кафедри політики у сфері боротьби зі злочинністю та кримінального права Навчально-наукового юридичного інституту (протокол № 2 від 31 серпня 2022 року).

Затверджено на засіданні Науково-методичної ради Навчально-наукового юридичного інституту (протокол № 1 від 18 жовтня 2022 року).

Яцина М. О. Методичні вказівки для підготовки до семінарських (практичних) занять з навчальної дисципліни «Кібербезпека та міжнародне право» для здобувачів денної форми навчання першого (бакалаврського) рівня вищої освіти галузі знань 081 «Право», спеціальності 081 «Право», ОПП «Міжнародне та європейське право» (7 семестр). Івано-Франківськ : Навчально-науковий юридичний інститут Прикарпатського національного університету імені Василя Стефаника. Івано-Франківськ, 2022. 18 с.

Методичні вказівки містять в собі основні питання, що виносяться на розгляд семінарських (практичних) занять, вивчення яких є необхідним для набуття знань та умінь у сфері кібербезпеки, кіберзлорчиності та нормативно-правого регулювання зазначених спеф, як національними так і міжнародними нормативними документами. До кожної теми семінарського (практичного) заняття подано питання для обговорення, додаткові завдання та список рекомендованої літератури.

Методичні вказівки призначені для викладачів та здобувачів вищої освіти Навчально-наукового юридичного інституту Прикарпатського національного університету імені Василя Стефаника при вивченні навчальної дисципліни «Кібербезпека та міжнародне право».

ЗМІСТ

ВСТУП

Дисципліна «Кібербезпека та міжнародне право» являє собою один із спецкурсів, що заснований на традиціях порівняльного правознавства, що на відміну від традиційного підходу до вивчення законодавства окремих країн, дозволяє краще засвоїти студентами навичок порівняльно-правового аналізу та критичного мислення.

Цей спецкурс покликаний надати уявлення та сформувати систему знань про сучасні підходи до розуміння таких понять як «кібербезпека», «кіберзлочинність», «кіберзлочин», «кібертероризм» та ін., визначити основні проблеми правозастосовної практики в цій сфері, а також міжнародне нормативно-праве поле забезпечення кібербезпеки у світі. Окрема увага приділена тематиці законодавства Європейського Союзу, оскільки воно виступає узагальнюючим орієнтиром для розвитку держави і права України на сучасному етапі розвитку.

Вивчення даного спецкурсу дозволить студентам набути знань про історію становлення та розвитку кібербезпеки та кіберзлочинності, стан та перспективи розвитку кримінального права щодо кримінальної відповідальності за кіберзлочини.

Метою вивчення дисципліни «Кібербезпека та міжнародне право» є оволодіння студентами теоретичними знаннями, надбання навичок порівняльно-правового аналізу та правильного застосування норм міжнародного права та права Європейського Союзу.

Цілями дисципліни є: набуття студентами знань та розуміння змісту таких як «кібербезпека», «кіберзлочинність», «кіберзлочин», «кібертероризм» та ін.; формування в них вмінь та навичок щодо вміння працювати з міжнародними нормативними актами; розвинути в них здатність до порівняльно-правового аналізу кримінально-правових норм різних європейських країн.

СЕМІНАРСЬКІ (ПРАКТИЧНІ) ЗАНЯТТЯ

Семінарське заняття 1, Тема 1:
«Кібербезпека: історія, поняття, види»

Методичні рекомендації: при вивченні даної теми студенти повинні з'ясувати історію зародження кібербезпеки. Знати зміст поняття «кібербезпеки», її види та напрямки, знати суб'єктів забезпечення кібербезпеки. Знати основні понятійний апарат кібербезпеки (напр., кіберпростір, кібертероризм, кіберзлочинність тощо). Знати співвідношення кібербезпеки із суміжними поняттями (напр., інформаційна безпека).

Питання для обговорення:

1. Сутність та підходи до визначення поняття «кібербезпека» та її ознаки.
2. Напрямки кібербезпеки.
3. Суб'єкти забезпечення кібербезпеки.
4. Видова характеристика кібербезпеки (види кібербезпеки).

Список рекомендованої літератури:

1. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. — К.: Видавничий дім «Кондор», 2019. — 272 с. URL: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf

2. Про основні засади гарантування кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

3. Бакалінська О.О, Бакалинський О.О. Правове гарантування кібербезпеки в Україні. Підприємство, господарство 1 право. 2019. № 9. С. 100-108. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf

4. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016

5. Ю. Хоббі Право людини на кібербезпеку: проблеми визначення та гарантування. Юридичний вісник. 2020. № 2. С. 37-43. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/1701/1811

Семінарське заняття 2, Тема 2:
«Кіберзлочинність: поняття, види та запобігання»

Методичні рекомендації: при вивченні даної теми студенти повинні зміст поняття «кіберзлочиність» та її відмінність від інших («традиційних») видів злочинності. Види кіберзлочинності. Знати основні понятійний апарат кіберзлочинності (напр., кіберпростір, кібертероризм, кіберправопорушення тощо). З'ясувати місце кіберзлочинності у структурі злочинності.

Питання для обговорення:

1. Кіберзлочинність як глобальна загроза у сучасному світі.
2. Сутність та підходи до визначення поняття «кіберзлочинність» та її ознаки.
3. Види та класифікації кіберзлочинності.
4. Заходи запобігання кіберзлочинності.

Додаткове завдання:

Користуючись публікаціями у засобах масової інформації знайдіть реальні приклади кіберзлочинів. Проаналізуйте їх з точни зору кримінально-правової кваліфікації.

Список рекомендованої літератури:

1. Бабанін С. В. Кіберзлочинність. *Вісник Асоціації кримінального права України*. 2016. Т. 1, № 5. С. 468–470. URL: http://vakp.nlu.edu.ua/article/view/173523
2. Русецький А. А., Куцолабський Д. А. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78. URL:http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pib_2017_1_15.pdf
3. Пивоваров В. В., Лисенко С. Ю. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3 ч. 2. С. 177–182.
URL:http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pis_2016_3(2)__32.pdf
4. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»:стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2 (10–11). С. 276–282.
5. Бондаренко О. С., Рєпін А. Д. Кіберзлочинність в україні: причини, ознаки та заходи протидії. *Порівняльно-аналітичне право*. 2018. № 1. С. 246–248. URL:
https://essuir.sumdu.edu.ua/bitstream/123456789/67982/1/Bondarenko_Repin_KIberzlochinist.pdf
6. Нашинець-Наумова А. Ю. Кіберзлочинність. нова кримінальна загроза. *Наукові розвідки з актуальних проблем публічного та приватного права : Матеріали IV Всеукр. науково-практ. конф*., м. Київ, 24 квіт. 2021 р. Київ, 2021. С. 111–114. URL:

https://fpmv.kubg.edu.ua/images/stories/Departaments/Ogoloshenia/00_2021/kpp/Zbirnyk_tez_2021_konferentsiya_z_prav_24.04.21.pdf#page=111

7. Уткіна Г. А., Лопушенко Г. М. Кіберзлочинність та перспективи її протидії. *Регіональні особливості злочинності: сучасні тенденції та стратегії протидії: збірник. матеріалів Всеукраїнської науково-практичної конференції.* Кривий Ріг - 14 травня 2021 р. С. 379-380. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/41082/1/%D0%A0%D0%95%D0%93%D0%86%D0%9E%D0%9D%D0%90%D0%9B%D0%AC%D0%9D%D0%86%20%D0%9E%D0%A1%D0%9E%D0%91%D0%9B%D0%98%D0%92%D0%9E%D0%A1%D0%A2%D0%86.pdf#page=379

Семінарське заняття 3, Тема 3: «Кібертероризм: поняття та види»

***Методичні рекомендації**:* при вивченні даної теми студенти повинні з'ясувати історію зародження кібертероризму. Знати зміст поняття «кібертероризм», його види та співвідношення з тероризмом. Знати основні понятійний апарат кібертероризму (напр., кібератака, кібер-тетористичний акт тощо). Знати методи та заходи запобігання та боротьби з кібертероризмом.

Питання для обговорення:

1. Феномен «кібертероризму» та історія його виникнення.
2. Кібертероризм: поняття та ознаки, види.
3. Співвідношення понять «кібертероризм» та «тероризм» (спільне та відмінне).
4. Кібер-терористичний акт: поняття та види.
5. Запобігання кібертероризму.

Додаткове завдання:

Користуючись публікаціями у засобах масової інформації знайдіть реальні приклади терористичних актів вчинених з використанням цифрових технологій. Проаналізуйте їх.

Список рекомендованої літератури:

1. Зінченко О. І. Європейська регіональна система протидії кібертероризму: політичні, інституційні та правові механізми. *Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Питання політології*». Вип. 39. 2021. С.118-122. URL: https://periodicals.karazin.ua/politology/article/view/17813

2. Кібербезпека та інтелектуальна власність: проблеми правового забезпечення: Матеріали міжнародної науково-практичної конференції. 21 квітня 2017 р., м. Київ, в 2-х частинах. Частина друга. / Упоряд. : В. М. Фурашев, С. Ю.

Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2017. – 124 с. URL: http://ippi.org.ua/sites/default/files/ch-2_.pdf

3. Рульов І. Співвідношення кібертероризму та кіберзлочину. *Юридичний вісник*. 2021. № 3. С. 178–185. URL: http://yuv.onua.edu.ua/index.php/yuv/article/view/2202

4. Conway Maura. Cyberterrorism: the story so far. *Journal of Information Warfare*. 2003. Vol. 2. No. 2. P. 33-42. URL: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.579.6777&rep=rep1&type=pdf

5. Lee Jarvis, Stuart Macdonald. What Is Cyberterrorism? Findings From a Survey of Researchers. *Terrorism and Political Violence*. 2015. Volume 27. Isuue 4. P. 657-678. URL: https://sci-hub.se/10.1080/09546553.2013.847827

6. Marco Marsili. The War on Cyberterrorism. *Democracy and Security*. Volume 15. Issue 2. P. 172-199. URL: https://sci-hub.se/10.1080/17419166.2018.1496826

7. Stuart Macdonald, Lee Jarvis, Simon M. Lavis. Cyberterrorism Today? Findings From a Follow-on Survey of Researchers. *Studies in Conflict & Terrorism*. 2019. Volume 5. Issue 8. P. 727-752. URL: https://sci-hub.se/10.1080/1057610X.2019.1696444

Семінарське заняття 4, Тема 4: «Система міжнародного законодавства забезпечення кібербезпеки».

Методичні рекомендації: при вивченні даної теми студенти повинні з'ясувати систему міжнародного законодавства забезпечення кібербезпеки (конвенції, декларації, договори тощо) та боротьби з кіберзагрозами. Знати перелік основних міжнародних нормативно-правових актів з галузі та їх основні положення.

Питання для обговорення:

1. Нормативно-правові документи світового масштабу.
2. Регіональні нормативно-правові документи (ЄС, Рада Європи, ІНТЕРПОЛ, НАТО).
3. Нормативно-правове регулювання кібербезпеки країн Африканського континенту, Латинської Америки та держав Арабського регіону.

Додаткове завдання:

Проаналізуйте положення Конвенції з кібербезпеки та захисту персональних доних Африканського Союзу від 27 червня 2014 року.

Проаналізуйте положення Регільональної стратегії щодо кібербезпеки та кіберзлочтнності Економічне співтовариство країн Західної Африки 2020 року.

Проаналізуйте положення Арабської угоди про протидію кіберзлочинам 2015 року.

Список рекомендованої літератури:

1. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері : навч. посіб. Київ : Центр глобалістики «Стратегія XXI», 2019. 30 с. URL: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf/c970b17f-d9db-aba3-7990-bb4441a3e041?version=1.0&t=1554283399244

2. Шемчук В. В. Основні напрями міжнародного співробітництва у сфері кібербезпеки. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2018. Т. 29 (68), № 2. URL: https://www.juris.vernadskyjournals.in.ua/journals/2018/2_2018/24.pdf

3. Конвенція про кіберзлочинність URL: http://zakon5.rada.gov.ua/laws/show/994_575

4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи URL: http://zakon5.rada.gov.ua/laws/show/994_687

5. Developments in the field of information and telecommunications in the context of international security UN General Assembly A/RES53/70.: URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement

6. Developments in the field of information and telecommunications in the context of international security UN General Assembly A/RES/54/49. URL: https://documents-ddsny.un.org/doc/UNDOC/GEN/N99/777/13/PDF/N9977713.pdf?OpenElement

7. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.2019

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.

9. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30.

10. African Union Convention on Cyber Security and Personal Data Protection, adopted on June 27, 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

11. ECOWAS Regional Cybersecurity and Cybercrime Strategy – 2020, URL: https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-

Cybersecurity-Cybercrime-Strategy-EN.pdf
12. A Geneva Convention or Declaration for Cyberspace. Presentation at the WSIS Forum 2018. URL: http://www.cybercrimelaw.net/documents/Presentation1.pdf
13. Inter-American Cooperation Portal on Cyber-Crime. Department of Legal Cooperation. OAS. URL: http://www.oas.org/juridico/english/cyber.htm
14. Arab Treaty on Combating Cybercrime. Riyadh Al-Balushi. 2015. URL: http://www.riyadh.om/2015/arab-treaty-on-combating-cybercrime/

Семінарське заняття 5, Тема 5:
«Кібербезпека у Європейському Союзі».

Методичні рекомендації: при вивченні даної теми студенти повинні з'ясувати історію становлення та розвитки політики Європейського Союзу (ЄС) у сфері забезпечення кібербезпеки. Знати перелік та положення основних нормативно-правових актів ЄС у сфері кібербезпеки.

Питання для обговорення:

1. Історія становлення та формування кібербезпеки ЄС.
2. Нормативно-правові акти ЄС у сфері кібербезпеки (основні положення).
3. Стратегія кібербезпеки ЄС (2013 та 2021): основні положення.
4. Співробітництво у сфері кібербезпеки ЄС-НАТО.

Список рекомендованої літератури:

1. Грубінко А. Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. Актуальні проблеми правознавства. 2021. № 1 (25). С. 5–10. URL: http://appj.wunu.edu.ua/index.php/appj/article/view/1142/1186
2. Кузнєцов О. М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. Інформація і право. 2021. № 1(36). С. 106–113. URL: http://ippi.org.ua/sites/default/files/14_18.pdf
3. Рижков М., Рубан А. Стратегія інформаційної і кібербезпеки ЄС: сучасний вимір. *International relations, part "Political sciences"*. 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3866/3526
4. Звоздецька О.Кібербезпека ЄС в умовах посилення кіберзагроз в сучасному глобалізованому світі // Медіафорум : аналітика, прогнози, Mediarorum: Analytics, Forecasts, інформаційний менеджмент : Information Management: зб. наук. праць. – Чернівці : Collection of Research Articles. – Chernivtsi: Чернівецький нац. ун-т, 2019. – Chernivtsi National University, 2019. – Том 7. – С. 27-46. URL: https://journals.chnu.edu.ua/index.php/mediaforum/article/view/70/38
5. Кавин С. Я. Правові засади забезпечення кібербезпеки в державах - членах Європейського Союзу. *Актуальні проблеми держави і права*. 2020. № 87. С. 51–

58. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/14107/Kavin%20S.%20Y.%20Legal%20framework%20for%20cybersecurity%20in%20European%20Union%20member%20states.pdf?sequence=1&isAllowed=y

6. Марущак А.І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. *Безпека інформації*. 2019. Т. 25. № 1. С. 13-17. URL: https://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/13665

7. Петров С. Г. Організаційні і правові основи вирішення проблем протидії кіберпосяганням у Європейському Союзі. *Інформація і право*. 2020. № 1(32). С. 99–105. URL: http://il.ippi.org.ua/article/view/200386

8. Сайт ENISA – (Агентство ЄС з кібербезпеки). URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies

9. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері : навч. посіб. Київ : Центр глобалістики «Стратегія XXI», 2019. 30 с. URL: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf/c970b17f-d9db-aba3-7990-bb4441a3e041?version=1.0&t=1554283399244

10. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, p. 1–30.

11. EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions. *Security and Defense Policy. Policy Brief*. 2017. № 8. С. 1–9. URL: https://www.gmfus.org/sites/default/files/EU-NATO%20Cybersecurity%20and%20Defense%20Cooperation%20edit.pdf

12. Poptchev Peter. "NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages." *Information & Security: An International Journal*. Isuue 45 (2020) P. 35-55. URL: https://infosec-journal.com/article/nato-eu-cooperation-cybersecurity-and-cyber-defence-offers-unrivalled-advantages

13. Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.2019

14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88.

Семінарське заняття 6, Тема 6:
«Міжнародне співробітництво у боротьбі з кіберзлочинністю».

Методичні рекомендації: при вивченні даної теми студенти повинні засвоїти інформацію про порядок, види та заходи міжнародного співробітництва у боротьбі з кіберзлочинністю.

Питання для обговорення:

1. Загальна характеристика міжнародно-правової боротьби з кіберзлочинністю.
2. Становлення та розвиток міжнародно-правового регулювання боротьби з кіберзлочинністю.
3. Міжнародно-правовий механізм боротьби з кіберзлочинністю на універсальному рівні.
4. Міжнародно-правовий механізм боротьби з кіберзлочинністю на регіональному рівні.
5. Заходи міжнародного співробітництва боротьби з кіберзлочинністю.

Додаткове завдання:

Користуючись публікаціями у засобах масової інформації знайдіть реальні приклади міжнародного співробітництва боротьби з кіберзлочинністю. Проаналізуйте їх.

Список рекомендованої літератури:

1. Войціховський, А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. *Право і Безпека*. 2011. № 4 (41). С. 107-112 URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/1225
2. Горощак К. О. Міжнародно-правове співробітництво держав у боротьбі з кіберзлочинністю / К. О. Горощак. – Львів, 2019. – 40 с. URL: http://dspace.onua.edu.ua/handle/11300/14991
3. Косаревська О. В., Шутило С. В. Деякі аспекти міжнародного співробітництва правоохоронних органів у сфері боротьби з кіберзлочинністю. *Кібербезпека в Україні: правові та організаційні питання* : Матеріали міжнар. наук. конф., м. Одеса. С. 156–158. URL: https://oduvs.edu.ua/wp-content/uploads/2017/01/Kiberbezpeka-v-Ukrayini-final.pdf
4. Кузнєцов О. М. Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. Інформація і право. 2021. № 1(36). С. 106–113. URL: http://ippi.org.ua/sites/default/files/14_18.pdf
5. Леган І. М. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2021. № 50. С. 118–121. URL: https://vestnik-pravo.mgu.od.ua/archive/juspradenc50/27.pdf
6. Марущак А. І. Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю. *Інформація і право.* 2018. Т. 3 (26). С. 104–110 URL: http://ippi.org.ua/sites/default/files/12_9.pdf
7. Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності [Текст] : монографія / І. М. Леган. – Чернігів : НУ

«Чернігівська політехніка», 2021. – 328 с. (с. 248-262) URL: http://ir.stu.cn.ua/bitstream/handle/123456789/23756/%D0%9C%D1%96%D0%B6%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%B5%20%D1%81%D0%BF%D1%96%D0%B2%D1%80%D0%BE%D0%B1%D1%96%D1%82%D0%BD%D0%B8%D1%86%D1%82%D0%B2%D0%BE%20%D1%83%20%D1%81%D1%84%D0%B5%D1%80%D1%96%20%D0%B7%D0%B0%D0%BF%D0%BE%D0%B1%D1%96%D0%B3%D0%B0%D0%BD%D0%BD%D1%8F%20%D1%82%D0%B0%20%D0%BF%D1%80%D0%BE%D1%82%D0%B8%D0%B4%D1%96%D1%97%20%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%D0%B9%20%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D1%96.pdf?sequence=1&isAllowed=y

8. Саєнко М., Савела Є., Тополянський Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. Науковий вісник Ужгородського національного університету. Серія: Право. 2021. Т. 64. С. 386–391. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/238897/237481

9. Співробітництво Україна – ЄС – НАТО з протидії гібридним загрозам у кіберсфері : навч. посіб. Київ : Центр глобалістики «Стратегія XXI», 2019. 30 с. URL: https://www.kas.de/documents/270026/4625039/UA+Ukraine+-+EU+-+NATO+cooperation+to+counter+hybrid+threats+in+cyber+sphere.pdf/c970b17f-d9db-aba3-7990-bb4441a3e041?version=1.0&t=1554283399244

10. CyberEast - Дія щодо боротьби з кіберзлочинністю для кіберстійкості в регіоні Східного партнерства - EU4Digital. EU4Digital. URL: https://eufordigital.eu/uk/discover-eu/cybereast-action-on-cybercrime-for-cyber-resilience-in-the-eastern-partnership-region/

Семінарське заняття 7, Тема 7: «Кібербезпека в Україні».

Методичні рекомендації: при вивченні даної теми студенти повинні засвоїти інформацію про порядок, види та заходи міжнародного співробітництва у боротьбі з кіберзлочинністю.

Питання для обговорення:

1. Сучасна кібербезпека України: поняття, зміст, ознаки.
2. Нормативно-правова основа кібербезпеки в Україні.
3. Напрями кібербезпеки України.
4. Суб’єкти забезпечення кібербезпеки в Україні: види, повноваження.
5. Співробітництво України х міжнародними партнерами у сфері забезпечення кібербезпеки.

Додаткове завдання:

Схематично зобразіть перелік нормативно-правових документів, що регулюють сферу кібербезпеки України.

Список рекомендованої літератури:

1. Computer Emergency Response Team of Ukraine – CERT-UA. *cert.gov.ua*. URL: https://cert.gov.ua/
2. Бакалинський О., Бакалинська О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2017. № 9. С. 100–108. URL: http://pgp-journal.kiev.ua/archive/2019/9/18.pdf
3. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник НТУУ "КПІ" Політологія. Соціологія. Право.* 2016. № 3/4 (31/32). С. 117–124. URL: http://visnyk-psp.kpi.ua/article/view/140496/137578
4. Діордіца І. В. Суб'єкти забезпечення кібербезпеки. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2017. Т. 1, № 45. С. 160–165.
URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/34119/1/СУБ'ЄКТИ%20ЗАБЕЗПЕЧЕННЯ%20КІБЕРБЕЗПЕКИ.pdf
5. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. Офіційний вісник Президента України. 2017. № 5. С.15. Ст.102.
6. Колб О. Г., Колб Р. О. Нормативно-правові неузгодженості та суперечності інформаційної діяльності – одна із загроз національної безпеки України. Вісник Пенітенціарної асоціації України. Пенітенціарна асоціація України; Науково-дослідний інститут публічного права. Київ: ФОП Кандиба Т. П., 2020. № 3 (13). С. 90-97.
7. Лук'янчук Р. В. Державне управління у сфері забезпечення кібербезпеки України : автореф. дис. ... канд. наук з держ. упр. : 25.00.01. Київ, 2017. 19 с.
8. Мамедова Е. Категоріальні та історико-правові аспекти державної політики кібербезпеки в Україні. *Юридичний вісник*. 2022. № 6. С. 272–281. URL: https://doi.org/10.32837/yuv.v0i6.2293
9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
10. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р. : станом на 3 лют. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
11. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. 2020. Т. 31 (70) Ч. 2, № 2. С. 119–124. URL: https://juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf
12. Трофименко О. Кібербезпека України: аналіз сучасного стану. *Захист інформації*. 2019. Т. 21, № 3. С. 150–157. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y

Семінарське заняття 8, Тема 8: «Кримінально-правове забезпечення боротьби з кіберзлочинністю в Україні».

Методичні рекомендації: при вивченні даної теми студенти повинні набути знання про сучасні методологічні основи кримінально-правової кваліфікації кіберзлочинів, визначити основні проблеми правозастосовної практики в цій сфері, а також шляхи їх подолання.

Питання для обговорення:

1. Сучасний стан кіберзлочинності в Україні.
2. Загальна характеристика кримінальних правопорушень передбачених Розділом XVI Особливої частини Кримінального кодексу України.
3. Кваліфікаця кримінальних правопорушенння проти конфіденційності, цілісності і доступності комп'ютерних даних і систем.
4. Кваліфікаця кримінальних правопорушенння пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів.
5. Кваліфікаця кримінальних правопорушенння пов'язаних зі змістом інформації (зокрема, дитяча порнографія, расизм і ксенофобія).
6. Кваліфікаця кримінальних правопорушенння пов'язаних з порушенням авторських та суміжних прав, наприклад незаконне відтворення і використання комп'ютерних програм, аудіо/відео та інших видів цифрової продукції, а також баз даних і книг.

Список рекомендованої літератури:

1. Бєльський Ю. А. Особливості визначення родового об'єкта Розділу XVI Кримінального кодексу України "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку". *Науковий вісник публічного та приватного права*. 2016. № 4. С. 222–225. URL: http://www.nvppp.in.ua/vip/2016/4/53.pdf
2. Васильєв А. А., Пашнєв Д. В. Особливості кваліфікації злочинів у сфері використання еом (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. *Вісник Кримінологічної асоціації України*. 2013. № 5. С. 34–42. URL: https://core.ac.uk/download/pdf/187222923.pdf
3. Кримінальне право України (Загальна та Особлива частини) : посіб. для підгот. до зовніш. незалеж. оцінювання / В. І. Тютюгін, М. А. Рубащенко ; відп. ред. В. І. Тютюгін. – 2-ге вид., перероб. і допов. – Харків : Право, 2021. – 336 с.
4. Кримінальне право України. Особлива частина : навчальний посібник / Попович О.В., Томаш Л.В., Латковський П.П., Бабій А.Ю. Чернівці, 2022. 319 с. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/18921/%D0%9A%D1%80%D0%

B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B5%20%D0%BF%D1%80%D0%B0%D0%B2%D0%BE%20%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8.%20%D0%9E%D1%81%D0%BE%D0%B1%D0%BB%D0%B8%D0%B2%D0%B0%20%D1%87%D0%B0%D1%81%D1%82%D0%B8%D0%BD%D0%B0.pdf?sequence=1&isAllowed=y

5. Луцький Т. М., Пасєка О. Ф. Окремі проблемні аспекти кримінальної відповідальності та покарання за правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2022. № 5. С. 270–275. URL: http://app-journal.in.ua/wp-content/uploads/2022/05/52.pdf

6. Піцик Ю. М. Класифікація кіберзлочинів проти власності. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція.* 2017. Вип. 30(2). С. 65-68. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_30(2)__18

7. Сухонос, В.В. Кримінальне право України. Особлива частина: підручник / В.В. Сухонос, Р.М. Білоконь, В.В.Сухонос (мол.) / за заг. ред. доктора юрид. наук, проф. В.В. Сухоноса. Суми : ПФ "Видавництво "Університетська книга", 2020. - 672 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/76320/1/Sukhonos_KrumGpravo.pdf

8. Хахановський В. Г., Гавловський В. Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право*. 2020. № 2 (33). С. 99–109. URL: http://il.ippi.org.ua/article/view/20810

Семінарське заняття 9, Тема 9: «Особливості методики розслідування кіберзлочинів».

Методичні рекомендації: при вивченні даної теми студенти повинні засвоїти основи виявлення та розслідування кіберзлочинів, знати особливості кримінального провадження щодо кіберзлочинів, специфіку використання спеціальних знань підчас розслідування кіберзлочинів.

Питання для обговорення:

1. Методичні основи розслідування кіберзлочинів.
2. Організаційні засади виявлення та початку кримінального провадження щодо кіберзлочинів.
3. Організаційно-тактичні основи розслідування кіберзлочинів.
4. Використання спеціальних знань під час розслідування кіберзлочинів.

Список рекомендованої літератури:

1. Виявлення, попередження та розслідування злочинів торгівлі людьми,

вчинених із застосуванням інформаційних технологій: навчальний курс / [А. Вінаков, В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков, В. Носов, О. Соловйов]. – К., 2017. – 148 с. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/9028

2. Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка, О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.

3. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14

4. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/ laws/show/4651-17

5. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17

6. Радутний О. Е. Інформація, яка надходить у режимі реального часу через веб-камеру, як предмет злочину, що передбачений ст. 301 КК України. *Інформація і право*. 2014. № 1. С. 115-119. URL: http://nbuv.gov.ua/UJRN/Infpr_2014_1_16

7. Самойленко О. А. Виявлення та розслідування кіберзлочинів [Текст] : навчально-методичний посібник. Одеса. 2020. 112 с. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12612/%D0%9D%D0%9C%D0%9F%20%D0%A1%D0%BF%D0%B5%D1%86%D0%BA%D1%83%D1%80%D1%81%20%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B7%D0%BB%D0%BE%D1%87%D0%B8%D0%BD%D0%B8.pdf?sequence=1&isAllowed=y

8. Самойленко О. А. Відкриття кримінального провадження щодо злочинів, вчинених у кіберпросторі. Підприємство, господарство і право. 2019. №8. С. 222-225

9. Самойленко О.А. Основи методики розслідування злочинів, вчиненихуу кіберпросторі: монографія / О. А. Самойленко ; за заг. ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

ОСОБЛИВОСТІ ОЦІНЮВАННЯ

Загальна система оцінювання навчальної дисципліни є уніфікованою в межах навчально-наукового юридичного інституту і визначається п. 4.4 Положення про порядок організації навчального процесу та оцінювання успішності студентів у навчально-науковому юридичному інституті Прикарпатського національного університету імені Василя Стефаника, затвердженим Вченою радою Юридичного інституту Прикарпатського національного університету імені Василя Стефаника, протокол № 2 від 12.10.2010 р. (з наступними змінами) – текст розміщений на інформаційному стенді та сайті Інституту https://law.pnu.edu.ua/організація-навчального-процесу/.

Вивчення дисципліни передбачає обов'язкове виконання всіма студентами двох письмових модульних контрольних робіт. Роботи виконуються на 5-му та 9-му практичному занятті. На контрольну виноситься 1 описове завдання, яке оцінюється в 6 балів, 1 коротке завдання нормативного змісту, яке оцінюється в 6 балів та 8 тестових запитань, кожне з яких оцінюється в 1 бал. Максимальний бал за контрольну становить 20. За бажанням (для отримання додаткових до 5 балів) студенти можуть виконувати індивідуальні завдання за темою відповідного практичного заняття. Види індивідуальних завдань знаходяться на кафедрі та розміщені на сайті кафедри https://kkp.pnu.edu.ua/.

Система оцінювання семінарських занять визначена п.п. 4.4.3.2, 4.4.3.3 Положення про порядок організації навчального процесу та оцінювання успішності студентів у навчально-науковому юридичному інституті Прикарпатського національного університету імені Василя Стефаника.

Шкала оцінювання

<table>
<tr><th rowspan="2">Сума балів
за всі види навчальної
діяльності</th><th rowspan="2">Оцінка
ECTS</th><th colspan="2">Оцінка за національною шкалою</th></tr>
<tr><th>для екзамену, курсової
роботи (проекту), практики</th><th>для заліку</th></tr>
<tr><td>90 – 100</td><td>A</td><td>Відмінно</td><td rowspan="5">Зараховано</td></tr>
<tr><td>82 – 89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>75 - 81</td><td>C</td></tr>
<tr><td>67 -74</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60 - 66</td><td>E</td></tr>
<tr><td>1 – 59</td><td>Fx</td><td>Незадовільно</td><td>Незараховано</td></tr>
</table>