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 самостійної роботи 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 самостійної роботи 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. 15 с.

Методичні вказівки містять в собі основні питання, що виносяться на самостійне опрацювання, вивчення яких є необхідним для поглиблення набутих 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».

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.

Окремим аспектом вивчення даної дисципліни є самостійна робота студентів. Самостійна робота студента – це форма організації навчального процесу, при якій заплановані завдання виконуються студентом під методичним керівництвом викладача, але без його безпосередньої участі. Самостійна робота студента є основним засобом оволодіння навчальним матеріалом у час, вільний від обов'язкових навчальних занять. Зміст самостійної роботи студента полягає в науково обґрунтованій системі дидактично та методично оформленого навчального матеріалу і визначається з урахуванням структурно-логічної схеми підготовки фахівців, яку відображено в освітньо-професійній програмі та робочому навчальному плані. Зміст самостійної роботи студента з кожної навчальної дисципліни визначається робочою програмою навчальної дисципліни, методичними матеріалами, завданнями та вказівками викладача.

Зміст самостійної роботи студента визначається навчальною програмою дисципліни, методичними матеріалами, завданнями та вказівками викладача. Самостійна робота студента забезпечується системою навчально-методичних засобів, передбачених для вивчення дисципліни: підручник, навчальні та методичні посібники, конспект лекцій викладача, практикум тощо. Методичні матеріали для самостійної роботи студентів повинні передбачати можливість проведення самоконтролю з боку студента. Для самостійної роботи студенту також рекомендується відповідна наукова та фахова монографічна і періодична література. За результатими самрстійної роборти студент може отримати 5 балів.

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

На власний вибір зробіть:

1. Складіть термінологічний словник з визначення поняття «кібербезпека».
2. Створіть схему «Напрямки кібербезпеки».
3. Зробіть у формі таблиці питання «Суб'єкти забезпечення кібербезпеки».
4. Створіть схему «Видова види кібербезпеки».

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

На власний вибір зробіть:

1. Реферативне повідомлення «Кіберзлочинність: сучасні тенденції».
2. Складіть термінологічний словник з визначення поняття «кіберзлочинність».
3. Складіть психологіний портрет кіберзлочинця.

Тема 3:
«Кібертероризм: поняття та види»

На власний вибір зробіть:

1. Хронологічну таблицю або схему «Історія кібертероризму».
3. Порівняльну таблицю «Співвідношення понять «кібертероризм» та «тероризм».
4. Зробіть підбірку з перелікорм найвідоміших кібертерористичних актів.

Тема 4:
«Система міжнародного законодавства забезпечення кібербезпеки»

На власний вибір зробіть:

1. Підбірку з переліком нормативно-правових документів що стосуються сфери кібербезпеки:
   а) Європейського Союзу;
   б) Ради Європи;
   в) ІНТЕРПОЛу;
   г) НАТО.
2. Напишіть анотацію:

а) Конвенції з кібербезпеки та захисту персональних доних Африканського Союзу від 27 червня 2014 року;

б) Регільональної стратегії щодо кібербезпеки та кіберзлочтнності Економічне співтовариство країн Західної Африки 2020 року;

в) Арабської угоди про протидію кіберзлочинам 2015 року.

Тема 5:
«Кібербезпека у Європейському Союзі»

На власний вибір зробіть:

1. Користуючись веб-порталом https://eur-lex.europa.eu/homepage.html зробіть вибірку нормативно-правових документів ЄС щодо кібербезпеки.

2. Презентацію «Нормативно-правові акти ЄС у сфері кібербезпеки (основні положення)».

3. Порівняльну таблицю «Стратегія кібербезпеки ЄС (2013 та 2021): основні положення».

Тема 6:
«Міжнародне співробітництво у боротьбі з кіберзлочинністю»

На власний вибір зробіть:

1. Реферативне повідомлення на тему: «Заходи співробітництва держав у розслідуванні кіберзлочинів».

2. Користуючись публікаціями у ЗМІ наведіть перелік прикладів співробітництва правоохоронних органів України та інших держав у розслідуванні кіберзлочинів.

3. Реферативне повідомлення на тему: «Порядок надання правової допомоги при притягненні кіберзлочинніців до відповідальності».

Тема 7: «Кібербезпека в Україні»

На власний вибір зробіть:

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

2. Реферативне повідомлення про діяльність CERT-UA.

3. Рефератине повідомлення про Центр протидії дезінформації при РНБО України.

Тема 8:
«Кримінально-правове забезпечення боротьби з кіберзлочинністю в Україні»

На власний вибір виконайте задачі з переліку:

Задача 1. Студент технічного університету Клочко з цікавості подолав систему захисту комерційного еротичного web-сайту і розповсюдив інформацію про спосіб зламу системи захисту цього сайту в комп'ютерній мережі Internet. Там же він повідомив про зареєстрованих користувачів сайту і номери їх кредитних карт. Протягом декількох годин після скоєного сайт був підданий масовим атакам мережевих хуліганів різних країн, внаслідок чого припинив функціонування на декілька днів. Крім цього, в результаті нелегального використання кредитних карток була спричинена значна шкода їх власникам. *Здійсніть юридичний аналіз ситуації.*

Задача 2. Керівник служби безпеки комерційного банку Терехов, використовуючи право доступу до захищеної комп'ютерної мережі банку, скопіював на носій інформації базу даних VIP-клієнтів банку, в якій містився

перелік номерів їх кредитних карток. Згодом Терехов за винагороду передав скопійовану інформацію відомому йому раніше програмісту Коріну, який розповсюдив дану інформацію у системі Internet. З*дійсніть юридичний аналіз ситуації.*

Задача 3. Оператор ЕОМ Зінін, посварившись з менеджером фірми, вирішив звільнитися, при цьому «насоливши» фірмі. З метою помсти він напередодні свого звільнення встановив на комп'ютер пароль, відомий тільки йому, і заблокував його роботу. При включенні комп'ютера новим оператором, прийнятим на роботу, він зажадав ввести пароль, оператор розгубився, і при спробі примусити працювати систему, знищив інформацію. *Здійсніть юридичний аналіз ситуації.*

Задача 4. Рибак, з метою безоплатного перегляду телепередач, здійснив приєднання телевізійного кабелю до телекомунікаційної мережі через розподільчу коробку, яка знаходилась на сходовій площадці біля його квартири. Після цього він користувався мережею ПП «Терра», отримавши можливість перегляду телепередач, чим спричинив підприємству матеріальну шкоду на суму 1 534 грн. Продовжуючи свої дії, Рибак здійснив ще одне приєднання до телекомунікаційної мережі ПП «Терра», внаслідок чого безпідставно користувався інформацією, чим спричинив підприємству матеріальну шкоду на суму 2 534 грн. *Здійсніть юридичний аналіз ситуації.*

Задача 5. Полохало та Вишневський за допомогою мережі «Інтернет» зареєструвалися на сайті, через котрий повинні були отримувати грошові кошти за здійснення телефонних дзвінків за кордон України. Після цього вони придбали на радіотехнічному ринку м. Полтави чотири стаціонарні телефони, котрі в подальшому переробили, зробивши їх меншого розміру та модернізувавши для зручного використання. Полохало та Вишневський за допомогою придбаних електронно-магнітних ключів, таємно проникли до під'їзду багатоквартирного будинку, де відкрили електрощитову та приєдналися до телефонних ліній ПАТ «Укртелеком», якими користувалися громадяни, що проживали у будинку. Після цього вони здійснили ряд дзвінків за кордон України, а саме: в Гвінею, Аввстралію, США, чим завдали матеріальної шкоди ПАТ «Укртелеком» на загальну суму 2 800 грн. *Здійсніть юридичний аналіз ситуації.*

Задача 6. Винник працював державним виконавцем відділу ДВС Нетішинського міського управління юстиції. До нього звернувся працівник КБ «Приватбанк» Мазурик з проханням посприяти у стягненні з боржників кредитної заборгованості, заарештувавши їх рухоме та нерухоме майна. У протилежному випадку Мазурик пообіцяв звернутися із скаргою на бездіяльність державного виконавця. У зв'язку із браком часу, Винник, не винісши постанови про опис та арешт майна боржників та не затвердивши у начальника ВДВС, маючи відповідний доступ, увійшов до електронних систем Державного реєстру обтяжень рухомого майна та Єдиного реєстру заборон відчуження об'єктів нерухомого майна і заповнив поля електронних заяв про удаване накладення арешту на рухоме майно фізичних осіб – боржників. Заповнені електроні заяви він скріпив власним електронним підписом і направив до сервера ДП

«Інформаційний центр», у результаті чого в автоматичному режимі було зареєстровано обтяження рухомого і нерухомого майна Іваницького, Філімонова та Патригури. *Здійсніть юридичний аналіз ситуації.*

Задача 7. Мельниченко зателефонував своєму знайомому – Абдулову, співробітнику Державної податкової інспекції з проханням надати інформацію з приводу конкретних суб'єктів господарської діяльності. Погодившись з проханням Мельниченко, Абдулов зі своєї особистої електронної поштової скрині відправив електронний лист з відповідною інформацією, яка оброблялась і зберігалась в автоматизованій інформаційній системі (АІС) «Податки». У подальшому Мельниченко передав отриману інформацію Зубкову, скопіювавши її зі свого ноутбука на флеш-накопичувач, а останній, у якості оплати, передав йому грошові кошти у розмірі 6 500 грн. Посадові особи юридичних осіб, а також органи ДПС дозволу на отримання, розповсюдження або збут інформації про вищевказаних суб'єктів господарської діяльності не давали. *Здійсніть юридичний аналіз ситуації.*

Задача 8. Гринів отримав абонентський номер мобільного зв'язку оператора «МТС», що використовувався незнайомим йому директором ПП «Клеопатра – центр краси та здоров'я». Після цього, перебуваючи за місцем свого проживання, з використанням належного йому комп'ютера та інстальованих на ньому комп'ютерної програми «skype», направив на вказаний абонентський номер 495 дзвінків та 990 повідомлень без звукового та текстового змісту. Протягом наступних двох тижнів Гринів направив на абонентський номер директора ПП «Клеопатра – центр краси та здоров'я» загалом 9940 дзвінків та повідомлень, що призвело до створення перешкод для використання за призначенням номера мобільного зв'язку. *Здійсніть юридичний аналіз ситуації.*

Тема 9: «Особливості методики розслідування кіберзлочинів».

На власний вибір зробіть:

1. Особливості проведення слідчих (розшукових) дій при розслідуванні кіберзлочинів.

2. Охарактеризуйте види експертих, які можуть використовуватися при розслдуванні кіберзлочинів.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ:

1. A Geneva Convention or Declaration for Cyberspace. Presentation at the WSIS Forum 2018. URL: http://www.cybercrimelaw.net/documents/Presentation1.pdf
2. 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
3. Arab Treaty on Combating Cybercrime. Riyadh Al-Balushi. 2015. URL: http://www.riyadh.om/2015/arab-treaty-on-combating-cybercrime/
4. Computer Emergency Response Team of Ukraine – CERT-UA. cert.gov.ua. URL: https://cert.gov.ua/
5. 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
6. 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/
7. 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
8. 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
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. 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. 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. 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
13. Inter-American Cooperation Portal on Cyber-Crime. Department of Legal Cooperation. OAS. URL: http://www.oas.org/juridico/english/cyber.htm

14. 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

15. 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

16. 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

17. 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.

18. 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.

19. 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

20. 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

21. 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

22. 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

23. 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

24. 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

25. 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

26. 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

27. 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

28. 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

29. 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.

30. Навчальний курс з виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій : навч. посіб. Київ : Посольство Велик. Британії в Україні, МВС України, Координатор проектів ОБСЄ, Global Affairs, Canada, Affaires mondiales Canada, 2017. 148 с. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/1225.

31. 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

32. 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

33. 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

34. 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

35. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.2017 р. № 47/2017. Офіційний вісник Президента України. 2017. № 5. С.15. Ст.102.

36. Звоздецька О. О. Кібербезпека ЄС в умовах посилення кіберзагроз в сучасному глобалізованому світі. *Медіафорум : аналітика, прогнози,*

менеджмент. 2019. № 7. С. 27–46. URL: https://doi.org/10.31861/mediaforum.2019.7.27-46

37. 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

38. 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

39. *Кібербезпека та інтелектуальна власність: проблеми правового забезпечення* : Матеріали міжнар. науково-практ. конф., м. Київ, 17 квіт. 2017 р. / упоряд.: В. М. Фурашев, С. Ю. Петряєв. Київ, 2017. С. 124. URL: http://ippi.org.ua/sites/default/files/ch-2_.pdf.

40. 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.

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

42. 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

43. 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.

44. Тютюгін В. І., Рубащенко М. А. Кримінальне право України (Загальна та Особлива частини) : посіб. для підгот. до зовніш. незалеж. оцінювання. Харків : Право, 2021. 336 с.

45. 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

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

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

48. 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

49. 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

50. 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

51. Лісовська Ю. П. Кібербезпека: ризики та заходи : навч. посіб. Київ : Вид. дім «Кондор», 2019. 272 с. URL: http://dcmaup.com.ua/assets/files/kiberbezpeka.pdf.

52. 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.

53. 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

54. 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

55. 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

56. 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

57. Леган І. М. Міжнародне співробітництво у сфері запобігання та протидії транснаціональній злочинності : монографія. Чернігів : НУ «Черніг. політехніка», 2021. 327 с. 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

58. 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

59. 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

60. 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.

61. Піцик Ю. М. Класифікація кіберзлочинів проти власності. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція*. 2017. № 30(2). С. 65-68. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_30(2)__18

62. 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

63. 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

64. 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

65. 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

66. 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

67. 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

68. 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

69. 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

70. 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

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

72. Самойленко О. А. Виявлення та розслідування кіберзлочинів : 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

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

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

75. 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

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

77. Сухонос В. В. Кримінальне право України. Особлива частина. Суми : Вид-во "Унів. кн.", 2020. 672 с. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/76320/1/Sukhonos_KrumGpravo.pdf

78. 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

79. 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

80. 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

81. 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

82. 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

83. 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