

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**  
**«КІБЕРЗЛОЧИННІСТЬ»**  
для здобувачів денної форми навчання  
другого (магістерського) рівня вищої освіти  
галузі знань 08 «Право», спеціальності 081 «Право»  
(1 семестр)

*Схвалено на засіданні кафедри політики у сфері боротьби зі злочинністю та кримінального права Навчально-наукового юридичного інституту (протокол № 1 від 28 серпня 2023 року).*

*Затверджено на засіданні Науково-методичної ради Навчально-наукового юридичного інституту (протокол № 1 від 19 вересня 2023 року).*

**Яцина М. О.** Методичні вказівки для самостійної роботи з навчальної дисципліни «Кіберзлочинність» для здобувачів денної форми навчання другого (магістерського) рівня вищої освіти галузі знань 081 «Право», спеціальності 081 «Право» (5 семестр). Івано-Франківськ : Навчально-науковий юридичний інститут Прикарпатського національного університету імені Василя Стефаника. Івано-Франківськ, 2023. 25 с.

Методичні вказівки містять в собі завдання, що ввиконання яких є необхідним у межах самостійної роботи здобувачів для набуття знань та умінь у сфері кібербезпеки, кіберзлочинності та нормативно-правового регулювання зазначених сфер. 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 «Кіберзлочинність».

© Яцина М. О., 2023  
© Навчально-науковий юридичний інститут  
Прикарпатського національного університету  
імені Василя Стефаника», 2023

## ЗМІСТ

ВСТУП.....	4
СЕМІНАРСЬКІ	(ПРАКТИЧНІ)
ЗАНЯТТЯ.....	5
Семінарське заняття № 1	
<i>Тема 1. Вчення про кіберзлочинність: поняття, ознаки, види, структура та показники.....</i>	<i>5</i>
Семінарське заняття № 2	
<i>Тема 2. Зміст поняття «кіберзлочинець» та його характеристика.....</i>	<i>6</i>
Семінарське заняття № 3	
<i>Тема 3. Вчення про кібертероризм.....</i>	<i>7</i>
Семінарське заняття № 4	
<i>Тема 4. Поняття та система запобігання кіберзлочинності.....</i>	<i>8</i>
Семінарське заняття № 5	
<i>Тема 5. Вчення про кібербезпеку.....</i>	<i>9</i>
Семінарське заняття № 6	
<i>Тема 6. Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем.....</i>	<i>11</i>
Семінарське заняття № 7	
<i>Тема 7. Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з використанням комп'ютера як засобу вчинення кримінального правопорушення.....</i>	<i>12</i>
Семінарське заняття № 8	
<i>Тема 8. Кримінально правова та кримінологічна характеристика кіберзлочинів пов'язаних з контентом.....</i>	<i>13</i>
Семінарське заняття № 9	

Тема	9.	Особливості	методики	розслідування
кіберзлочинів.....				15
Особливості оцінювання.....				17
Перелік рекомендованої літератури.....				18

## ВСТУП

Навчальна дисципліна «Кіберзлочинність» покликана надати уявлення та сформуванню систему знань про сучасні підходи до розуміння таких понять як «кібербезпека», «кіберзлочинність», «кіберзлочин», «кібертероризм» та ін., надати здобувачам освітнього рівня знання з нормативно-правового регулювання та законодавчого забезпечення боротьби з кіберзлочинністю, визначити основні проблеми правозастосовної практики в цій сфері, Вивчення даної навчальної дисципліни дозволить студентам набути знань про історію становлення та розвитку кіберзлочинності, стан та перспективи розвитку кримінального права щодо кримінальної відповідальності за кіберзлочини.

Самостійна робота є важливим способом опанування матеріалу у вільний від обов'язкових навчальних занять час, але її зміст визначається робочою програмою, методичними матеріалами, завданнями та вказівками викладача. Самостійна робота забезпечується системою навчально-методичних засобів, передбаченими для вивчення конкретної навчальної дисципліни: навчальні та методичні посібники, конспекти лекцій, робочі зошити. Для самостійної роботи студентів також рекомендується відповідна наукова, спеціальна та періодична література. Самостійна робота може виконуватися у бібліотеці, навчально-методичних кабінетах, комп'ютерних класах, а також у домашніх умовах. Навчальний матеріал дисципліни, передбачений робочою програмою для засвоєння студентом у процесі самостійної роботи, виноситься на підсумковий контроль разом із навчальним матеріалом, який відпрацьовувався під час проведення навчальних занять.

На самостійну роботу студентам виділяється значна частина часу, відведеного на вивчення навчальної дисципліни. Якість засвоєння матеріалу залежить від розвинутих навичок пошуку та опрацювання отриманої інформації, поглиблення та уточнення знань, отриманих раніше. Зміст самостійної роботи визначається робочою навчальною програмою дисципліни та методичними рекомендаціями викладача.

Формами самостійної роботи можуть виступати наступні: доопрацювання отриманого лекційного матеріалу; виконання домашніх завдань; робота у інформаційних мережах, спрямована на поглиблене вивчення додаткових питань по відповідній темі; опрацювання додаткової літератури; підготовка до виступу на семінарських заняттях та підготовка до практичних (лабораторних) занять; складання конспектів тем, що виносяться на самостійне опрацювання студентами.

До самостійної роботи можуть відноситися індивідуальні завдання: підготовка реферативних матеріалів на актуальні теми; написання тез наукових доповідей; анотація прочитаної додаткової літератури із курсу; складання бібліографії за відповідної тематикою.

## ЗАВДАННЯ ДЛЯ СОМОСТІЙНОЇ РОБОТИ

### Тема 1:

#### «Вчення про кіберзлочинність: поняття, ознаки, види, структура та показники»

**Методичні рекомендації:** при вивченні даної теми студенти повинні засвоїти зміст поняття «кіберзлочинності», її види та структуру та показники. Знати основні понятійний апарат кіберзлочинності (напр., кіберпростір, кібертероризм, кібератака тощо). Знати місце кіберзлочинності у структурі злочинності.

#### **Питання:**

1. Кіберзлочинність як соціально-правове явище сучасного світу, її поняття та ознаки.
2. Детермінанти кіберзлочинності.
3. Видова характеристика кіберзлочинності та її структура.
4. Місце кіберзлочинності у структурі системі злочинності, її показники.

#### **Завдання:**

1. Складіть хронологічну таблицю розвитку кіберзлочинності.
2. Користуючись статистичними даними Офісу Генерального прокурора про стан злочинності в Україні складіть діаграму яка відображає структуру кіберзлочинності в Україні.
3. Користуючись статистичними даними Офісу Генерального прокурора про стан злочинності в Україні складіть схему, яка відобразатиме динаміру кіберзлочинності в Україні за період від 2010 року.

#### **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](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](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., Репін 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\\_Kiber\\_zlochinst.pdf](https://essuir.sumdu.edu.ua/bitstream/123456789/67982/1/Bondarenko_Repin_Kiber_zlochinst.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/Zbinyk\\_tez\\_2021\\_konferentsiya\\_z\\_prav\\_24.04.21.pdf#page=111](https://fpmv.kubg.edu.ua/images/stories/Departaments/Ogoloshenia/00_2021/kpp/Zbinyk_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>

## Тема 2:

### «Зміст поняття «кіберзлочинець» та його характеристика»

**Методичні рекомендації:** при вивченні даної теми студенти повинні зміст поняття «кіберзлочинність» 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:**

1. Поняття особи кіберзлочинця.
2. Структура особистості кіберзлочинця (соціально-демографічні ознаки та морально-психологічні якості).
3. Типологія кіберзлочинності.
4. Наукове і практичне значення вивчення особистості кіберзлочинців.

### **Завдання:**

1. Користуючись публікаціями у засобах масової інформації знайдіть реальні приклади кіберзлочинців. Проаналізуйте їх з точни зору соціально-демографічних та морально-психологічних ознак осіб, які їх вчинили.
2. Складіть таблицю «Морально-психологічні якості особи-кіберзлочинця».

### **Список рекомендованої літератури:**

1. Бабенко О.О., Мокляк А.С. Теоретичний аналіз дослідження психологічного портрета кіберзлочинця. *Теорія і практика сучасної психології*. 2018. №2. С. 89-93. URL: [http://www.tpsp-journal.kpu.zp.ua/archive/2\\_2018/19.pdf](http://www.tpsp-journal.kpu.zp.ua/archive/2_2018/19.pdf)
2. Лугіна Н.А. та ін. Кримінологічна характеристика сучасного кіберзлочинця. *Порівняльно-аналітичне право*. 2019. №6. С. 400-402. URL: [http://pap-journal.in.ua/wp-content/uploads/2020/08/PAP\\_6\\_2019-sai-t.pdf#page=400](http://pap-journal.in.ua/wp-content/uploads/2020/08/PAP_6_2019-sai-t.pdf#page=400)
3. Неділько Я.В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*. 2020. Вип. 88. С. 202-211. URL: [URL:doi.org//10.33663/1563-3349-2020-88-202](https://doi.org/10.33663/1563-3349-2020-88-202)
4. Guoqiang Fu, Криволап Є.В. Особливості термінології в англomовній літературі у сфері кібербезпеки. *Юридичний вісник*. №1 (66). Ст. 63-71. URL: [URL:doi.org//0.18372/2307-9061.66.17419](https://doi.org/0.18372/2307-9061.66.17419)

### **Семінарське заняття 3, Тема 3: «Вчення про кібертероризм»**

**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:**

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.

### **Завдання:**

1. Користуючись публікаціями у засобах масової інформації знайдіть реальні приклади терористичних актів вчинених з використанням цифрових технологій. Проаналізуйте їх з позицій кримінології.
2. Підготуйте реферативне повідомлення на тему «Кібертероризм та гібридна війна».

### **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](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. Issue 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>



## Тема 4: «Поняття та система запобігання кіберзлочинності»

**Методичні рекомендації:** при вивченні даної теми студенти повинні з'ясувати систему запобігання кіберзлочинності. Необхідно звернути та нормативно-правові та організаційні методи забезпечення запобігання кіберзлочинам.

### **Питання:**

1. Поняття і система запобігання кіберзлочинності.
2. Суб'єкти запобігання кіберзлочинності (їх система та функції).  
кти запобігання Кібер злочинності.
3. Види запобігання кіберзлочинності:
  - 3.1. Загально-соціальне запобігання.
  - 3.2. Спеціально-кримінологічне запобігання.
  - 3.3. Індивідуальне запобігання.
4. Міжнародне співробітництво у запобіганні кіберзлочинності.

### **Завдання:**

1. Підготуйте реферативне повідомлення на тему «Цифрові технології запобігання кіберзлочинам».
2. Користуючись статистичними даними Інтерполу складіть підбірку інформації про заходи із запобігання кіберзлочинності на міжнародному рівні.

### **Список рекомендованої літератури:**

1. Бодунова О. М. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського університету: серія: Право*. 2023. Т.2. Вип. 75. С. 83-87. URL: <https://doi.org/10.24144/2307-3322.2022.75.2.13>
2. Болгов В. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. Київ : Національна академія прокуратури України, 2015. 202 с.
3. Леган І.М. Особливості міжнародного співробітництва щодо запобігання і протидії кіберзлочинності та кібертероризму. *Науковий вісник Міжнародного гуманітарного університету. Серія: Юриспруденція*. 2021. № 50. С. 118-121. URL: <https://doi.org/10.32841/2307-1745.2021.50.25>
4. Сащенко М. Проблемні аспекти запобігання кіберзлочинності в Україні. *Молодий вчений*. 2022. Вип. 1 (101). С. 17-20. <https://doi.org/10.32839/2304-5809/2022-1-101-4>

5. Таволжанський О.В. Особливості забезпечення кібербезпеки у сучасному світі: огляд суб'єктів запобігання кіберзлочинності. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Серія Право. 2018. Вип. 6 (18). С. 154–163.

### **Тема 5: «Вчення про кібербезпеку»**

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

#### **Питання:**

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 з міжнародними партнерами у сфері забезпечення кібербезпеки.
6. Кібербезпека України в умовах дії правового режиму воєнного часу.

#### **Завдання:**

1. Схематично зобразіть перелік нормативно-правових документів, що регулюють сферу кібербезпеки України.
2. Проаналізуйте основні ідеї положення Конвенції про кіберзлочинність.
3. Підготуйте реферативний повідомлення на тему «Державна політика у сфері забезпечення кібербезпеки».

#### **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](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\\_P\\_ropok\\_Loginova\\_Zadereyko\\_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y](http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_P_ropok_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y)

### Семінарське заняття 6, Тема 6:

**«Кримінально-правова та кримінологічна характеристика кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем»**

**Методичні рекомендації:** при вивченні даної теми студенти повинні набути знань з основ кримінально-правової кваліфікації кіберзлочинів проти конфіденційності, цілісності та доступності інформації, даних і систем, а також їх кримінологічну характеристику.

**Питання:**

1. Загальна характеристика кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.

2. Види кримінальних правопорушень, які посягають на конфіденційність, цілісність та доступність інформації, даних і систем.

3. Причини та умови кримінальних правопорушень проти конфіденційності цілісності та доступності інформації, даних і систем.

### **Завдання:**

1. Складіть задачу про кримінальне правопорушення яке посягає на конфіденційність тільки цілісність або доступність інформації.

2. Проаналізуйте положення Особливої частини Кримінального кодексу України та знайдіть приклади кримінальних правопорушень які посягають на конфіденційність цілісність та доступність інформації яких немає у розділі 16-му Розділі Особливої частини Кримінального кодексу України.

### **Список рекомендованої літератури:**

1. Аніщук В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2023. Т. 2 № 77. С. 139-143. URL: <https://doi.org/10.24144/2307-3322.2023.77.2.23>

2. Батиргареева В.С. Правова платформа для забезпечення в Україні ефективного захисту цифрових трансформації суспільства. *Інформація і право.* №1(40). С. 21-34. URL: [https://doi.org/10.37750/2616-6798.2022.1\(40\).254339](https://doi.org/10.37750/2616-6798.2022.1(40).254339)

3. Кримінально-правова охорона інформаційної безпеки України : монограф. / М.В. Карчевський ; МВС України, Луган. держ. ун-т внутр. справ ім. Е.О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. – 528 с. URL: <https://karchevskiy.files.wordpress.com/2020/04/karchevskiy-m.pdf>

4. Прокопчук Т. Міжнародні стандарти кримінально-правової охорони інформації з обмеженим доступом. *Підприємництво, господарство і право.* 2021. № 3. С. 232-239. URL: <https://doi.org/10.32849/2663-5313/2021.3.38>

5. Форос Г.В. Кримінально правова охорона з обмеженим доступом. *Південноукраїнський правничий часопис.* 2016. № 3-4. С. 64-66. URL: <http://www.sulj.oduvs.od.ua/archive/2016/3-4/21.pdf>

### **Семінарське заняття 7, Тема 7:**

**«Кримінально-правова та кримінологічна характеристика кіберзлочинів пов'язаних з комп'ютерами, включаючи підробку і шахрайство, вчинені з використанням комп'ютерів»**

**Методичні рекомендації:** при вивченні даної теми здобувачі повинні

набути знань про сучасні методологічні основи кримінально-правової кваліфікації кіберзлочинів пов'язаних з контентом, визначити основні проблеми правозастосовної практики в цій сфері, а також шляхи їх подолання.

### ***Питання:***

1. Загальна характеристика кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
2. Кримінально-правова характеристика та види кіберзлочинів пов'язаних з кримінальних правопорушень з комп'ютерами (включаючи підробку і шахрайство, вчинені з використанням комп'ютерів).
3. Кримінально-правова характеристика кримінальних правопорушень передбачених розділом XVI Особою частини Кримінального кодексу України.

### ***Завдання:***

1. Складіть задачу в основі якої ляже кіберзлочин корисливого характеру.
2. Складіть 15 тестових завдань про корисливі кіберзлочини.

### ***Список рекомендованої літератури:***

1. Бельський 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 електров'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 електров'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. Рубашенко ; 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., Пасека 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](http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_30(2)_18)

### **Семінарське заняття 8, Тема 8:**

#### **«Кримінально правова та кримінологічна характеристика кіберзлочинів пов'язаних з контентом»**

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

#### **Питання:**

1. Загальна характеристика кіберзлочинів пов'язаних з контентом.
2. Кримінально-правова характеристика та види кіберзлочинів пов'язаних з контентом:
  - порнографії,
  - ненависті, жорстокості, расизму і ксенофобії;
  - авторських та суміжних прав.

#### **Завдання:**

1. Складіть задачу основі якої буде кіберзлочин пов'язаний з забороненим контентом.
2. Складіть 15 тестових завдань про кіберзлочини пов'язаних з забороненим контентом.

#### **Список рекомендованої літератури:**

1. Грабар О., Жданова І. Проблема дитячої порнографії в інтернеті та кримінальну відповідальність. *Публічне право*. 2021. № 3(43). С. 120-126. URL: <https://doi.org/10.32782/2306-9082/2021-43-13>

2. Ємельянов В.П., Митрофанова Ю.С. Проблеми застосування та шляхи вдосконалення закону про кримінальну відповідальність за дитячу порнографію. Вісник Кримінологічної асоціації України. 2023. №1(28). С. 31-41. URL: <http://vca.univd.edu.ua/index.php/vca/article/view/35>

3. 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](https://essuir.sumdu.edu.ua/bitstream-download/123456789/76320/1/Sukhonos_KrumGpravo.pdf)

4. 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>

5. Цвіркун Н. Ю. Характеристика поняття «злочини на ґрунті ненависті». *Науковий вісник публічного та приватного права*. 2017. Вип. 4. С. 242-246. URL: <https://dspace.univd.edu.ua/handle/123456789/18212>

### **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 під час розслідування кіберзлочинів.

#### ***Питання:***

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.

#### ***Завдання:***

1. Підготуйте інформацію про види експертиз які здійснюються в межах досудового розслідування щодо 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](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, вчинених у 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://kcp.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

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсової роботи (проекту), практики	для заліку
90 – 100	A	Відмінно	Зараховано
82 – 89	B	Добре	
75 - 81	C		
67 -74	D		
60 - 66	E	Задовільно	Незараховано
1 – 59	Fx	Незадовільно	

## ПЕРЕЛІК 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. Бабенко О.О., Мокляк А.С. Теоретичний аналіз дослідження психологічного портрета кіберзлочинця. *Теорія і практика сучасної психології*. 2018. №2. С. 89-93. URL: [http://www.tpsp-journal.kpu.zp.ua/archive/2\\_2018/19.pdf](http://www.tpsp-journal.kpu.zp.ua/archive/2_2018/19.pdf)
3. \_\_\_\_ 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>
4. Бакалінська О.О, Бакалинський О.О. Правове гарантування кібербезпеки в Україні. *Підприємство, господарство і право*. 2019. № 9. С. 100-108. URL: <http://pgp-journal.kiev.ua/archive/2019/9/18.pdf>
5. \_\_\_\_ Бельський 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>
6. Бондаренко О. С., Репін 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\\_KIber\\_zlochinst.pdf](https://essuir.sumdu.edu.ua/bitstream/123456789/67982/1/Bondarenko_Repin_KIber_zlochinst.pdf)
7. \_\_\_\_ 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-ppsp.kpi.ua/article/view/140496/137578>
8. \_\_\_\_ 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>
9. 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.

10. 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. Соловійов]. – К., 2017. – 148 с. URL: <http://dspace.univd.edu.ua/xmlui/handle/123456789/9028>

11. 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>

12. Горощак К. О. Міжнародно-правове співробітництво держав у боротьбі з кіберзлочинністю / К. О. Горощак. – Львів, 2019. – 40 с.

13. Грабар О., Жданова І. Проблема дитячої порнографії в інтернеті та кримінальну відповідальність. *Публічне право*. 2021. № 3(43). С. 120-126. URL: <https://doi.org/10.32782/2306-9082/2021-43-13>

14. 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>

15. 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>

16. 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](http://zakon5.rada.gov.ua/laws/show/994_687)

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

18. Ємельянов В.П., Митрофанова Ю.С. Проблеми застосування та шляхи вдосконалення закону про кримінальну відповідальність за дитячу порнографію. *Вісник Кримінологічної асоціації України*. 2023. №1(28). С. 31-41. URL: <http://vca.univd.edu.ua/index.php/vca/article/view/35>

19. 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>

20. 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>

21. 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>

22. Казьмірук С.Д., Леонов Б.Д. Правове та організаційне забезпечення кіберзахисту систем детекції брехні від кібератак в умовах воєнного стану. *Інформація і право*. 2023. № 3(46). С. 135-141. URL: [https://doi.org/10.37750/2616-6798.2023.3\(46\).287217](https://doi.org/10.37750/2616-6798.2023.3(46).287217).

23. 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](http://ippi.org.ua/sites/default/files/ch-2_.pdf)

24. 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.

25. Конвенція про кіберзлочинність URL: [http://zakon5.rada.gov.ua/laws/show/994\\_575](http://zakon5.rada.gov.ua/laws/show/994_575)

26. 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://oduvsv.edu.ua/wp-content/uploads/2017/01/Kiberbezpeka-v-Ukrayini-final.pdf>

27. Красніков С.А. Шляхи посилення стану забезпечення кібербезпеки в умовах воєнного стану. *Інформація і право*. 2023. № 3(46). С. 118-121. URL: [https://doi.org/10.37750/2616-6798.2023.3\(46\).287214](https://doi.org/10.37750/2616-6798.2023.3(46).287214).

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

29. Кримінальне право України (Загальна та Особлива частини) : посіб. для підгот. до зовніш. незалеж. оцінювання / В. І. Тютюгін, М. А. Рубашенко ; відп. ред. В. І. Тютюгін. – 2-ге вид., перероб. і допов. – Харків : Право, 2021. – 336 с.

30. 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>

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

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

33. 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](http://ippi.org.ua/sites/default/files/14_18.pdf)

34. 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](http://ippi.org.ua/sites/default/files/14_18.pdf)

35. 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>

36. 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>

37. Лугіна Н.А. та ін. Кримінологічна характеристика сучасного кіберзлочинця. *Порівняльно-аналітичне право*. 2019. №6. С. 400-402. URL: [http://pap-journal.in.ua/wp-content/uploads/2020/08/PAP\\_6\\_2019-sai-t.pdf#page=400](http://pap-journal.in.ua/wp-content/uploads/2020/08/PAP_6_2019-sai-t.pdf#page=400)

38. 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.

39. 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>

40. 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>

41. Марущак А. 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](http://ippi.org.ua/sites/default/files/12_9.pdf)

42. 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>
43. Мігалатюк В.В. Удосконалення адміністративно-правового забезпечення кібербезпеки в Україні: досвід європейських країн. Наукові записки. Серія: Право. 2023. № 14. С. 143-147. URL: <https://pravo.cuspu.edu.ua/index.php/pravo/article/view/273/275>
44. 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%B0%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>
45. 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>
46. 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](https://fpmv.kubg.edu.ua/images/stories/Departaments/Ogoloshenia/00_2021/kpp/Zbirnyk_tez_2021_konferentsiya_z_prav_24.04.21.pdf#page=111)
47. Неділько Я.В. Типові ознаки особи кіберзлочинця (криміналістичний аспект). *Держава і право*. 2020. Вип. 88. С. 202-211. URL: [doi.org/10.33663/1563-3349-2020-88-202](https://doi.org/10.33663/1563-3349-2020-88-202)
48. 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>
49. 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-nbu.gov.ua/cgi-bin/irbis\\_nbu/cgiiirbis\\_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE\\_FILE\\_DOWNLOAD=1&Image\\_file\\_name=PDF/Pis\\_2016\\_3\(2\)\\_32.pdf](http://www.irbis-nbu.gov.ua/cgi-bin/irbis_nbu/cgiiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pis_2016_3(2)_32.pdf)
50. 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](http://nbuv.gov.ua/UJRN/Nvmgu_jur_2017_30(2)_18)
51. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділам
52. 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>
53. 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>
54. 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>
55. 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](http://nbuv.gov.ua/UJRN/Infpr_2014_1_16)
56. 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](http://journals.iir.kiev.ua/index.php/pol_n/article/view/3866/3526)
57. Рутьов І. Співвідношення кібертероризму та кіберзлочину. *Юридичний вісник*. 2021. № 3. С. 178–185. URL: <http://yuv.onua.edu.ua/index.php/yuv/article/view/2202>
58. 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](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)
59. 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>
60. Сайт ENISA – (Агентство ЄС з кібербезпеки). URL: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>
61. 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>
62. Самойленко О. А. Відкриття кримінального провадження щодо злочинів, вчинених у кіберпросторі. *Підприємство, господарство і право*. 2019. №8. С. 222-225

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

64. 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>

65. 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>

66. 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>

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

68. 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\\_KrumGravo.pdf](https://essuir.sumdu.edu.ua/bitstream-download/123456789/76320/1/Sukhonos_KrumGravo.pdf)

69. 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](https://juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf)

70. 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](http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y)

71. 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](#)

72. 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>

73. 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](https://www.juris.vernadskyjournals.in.ua/journals/2018/2_2018/24.pdf)

74. 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>

75. Guoqiang Fu, Криволап Є.В. Особливості термінології в англomовній літературі у сфері кібербезпеки. *Юридичний вісник*. №1 (66). Ст. 63-71. URL: [doi.org/10.18372/2307-9061.66.17419](https://doi.org/10.18372/2307-9061.66.17419)