**Національний юридичний університет імені Ярослава Мудрого**
Кафедри кримінології та кримінально-виконавчого права

# С И Л Л А Б У С
## навчальної дисципліни
## «Кіберзлочинність та електронні докази»

**Рівень вищої освіти** – другий (магістерський) рівень

**Ступінь вищої освіти** – магістр

**Галузь знань** – 08 «Право»

**Спеціальність** – 081 «Право»

**Спеціалізація** – «Прокуратура та кримінальна юстиція»

**Статус навчальної дисципліни** – за вибором студента

Рік набору – 2021

Харків – 2021

**Силлабус навчальної дисципліни «Кіберзлочинність та електронні докази»** для здобувачів вищої освіти другого (магістерського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право» спеціалізації «Прокуратура та кримінальна юстиція» Інституту прокуратури та кримінальної юстиції. Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2021. 12 с.

Розробник:

Таволжанський Олексій Володимирович – доцент кафедри кримінології та кримінально-виконавчого права, кандидат юридичних наук, Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук, доцент

Затверджено на засіданні кафедри кримінології та кримінально-виконавчого права

(протокол № від 20__ р.)

Дата оновлення – _____ 20___ р.

Завідувач кафедри кримінології та кримінально-виконавчого права – Головкін Богдан Миколайович, доктор юридичних наук, професор

Гарант освітньої програми – завідуюча кафедри кримінального процесу Капліна Оксана Володимирівна, доктор юридичних наук, професор

*Формуляр розроблений робочої групою у складі:*

- *проф. Комаров В. – проректор з навчально-методичної роботи;*
- *проф. Клімова Г. – начальник навчально-методичного відділу;*
- *к.ю.н. Яригіна Є. – методист навчально-методичного відділу*

*та затверджено на засіданні Науково-методичної ради (протокол №2 від 23.03.2021 р.)*

***Голова Науково-методичної ради***

_____ *Комаров В.*

**Дані про викладача**

| | |
|---|---|
| **Назва навчальної дисципліни** | **Кіберзлочинність та електронні докази** |
| **Статус навчальної дисципліни** | За вибором студента |
| **Викладач** | Таволжанський Олексій Володимирович – доцент кафедри кримінології та кримінально-виконавчого права, доктор юридичних наук, Національного юридичного університету імені Ярослава Мудрого, кандидат юридичних наук, доцент |
| **Контактний телефон** | 380 (57) 704-92-62 |
| **E-mail** | criminology@nlu.edu.ua |
| **Консультації** | відповідно до розробленого графіку індивідуальних консультаці |
| **Онлайн консультації** | Ідентифікатор конференції Zoom: 0000000000 Код доступу: 999999 |

## *Анотація навчальної дисципліни*

Навчальна дисципліна «Кіберзлочинність та електронні докази» переслідує мету теоретично і практично озброїти студента знаннями про соціальну сутність і детермінацію кіберзлочинності та її окремих злочинних проявів (кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг, соціальна інженерія, мальваре, протиправний контент рефайлінг та ін.), основні напрями запобіжної діяльності державних органів, установ і громадських організацій, систему заходів, які ними розробляються і реалізуються відповідно до Конституції України, законів та інших нормативно-правових актів, спрямованих на недопущення вчинення кіберзлочинів, захист прав та законних інтересів громадян, зниження «страху населення» перед кіберзлочинністю.

## Модуль 1. Кіберзлочинність: поняття, види та запобігання.

Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів. Поняття та кримінологічна характеристика

кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності.

Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.

Детермінанти та основні напрямки запобігання кіберзлочинності

**Модуль 2. Кримінально-правове забезпечення боротьби з кіберзлочинністю.**

Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.

Система та загальна характеристика кіберзлочинів.

Реалізація форм кримінальної відповідальності за кіберзлочини.

**Модуль 3. Особливості методики розслідування кіберзлочинів. Електронні докази у кримінальному провадженні**

Особливості методики розслідування кіберзлочинів.

Поняття електронних доказів у кримінальному провадженні

Види електронних доказів

Способи збирання електронних доказів.

Використання електронних доказів під час судового розгляду

***Мета та завдання навчальної дисципліни***

***Мета*** **навчальної дисципліни** – Мета даної навчальної дисципліни– теоретично і практично озброїти студента знаннями про соціальну сутність і детермінацію кіберзлочинності та її окремих злочинних проявів (кардинг, фішинг, вішинг, онлайн-шахрайство, піратство, кард-шарінг, соціальна інженерія, мальваре, протиправний контент рефайлінг та ін.), основні напрями запобіжної діяльності державних органів, установ і громадських організацій, систему заходів, які ними розробляються і реалізуються відповідно до Конституції України, законів та інших нормативно-правових

актів, спрямованих на недопущення вчинення кіберзлочинів, захист прав та законних інтересів громадян, зниження «страху населення» перед кіберзлочинністю.

***Завдання:***

- вивчення актуальних проблем запобігання кіберзлочинності;
- формування у студентів уявлення про поняття кіберзлочинність та електронні докази;
- визначення прикладних проблем при збиранні електронних доказів.

***Навчальна дисципліна у структурі освітньо-професійної програми. Міждисциплінарні зв'язки***

***Пререквізити:*** «Кримінальне право»; «Кримінально-процесуальне право»; «Адміністративне право; Кримінально-виконавче право».

***Кореквізити:*** "Кримінальне право»; «Кримінально-процесуальне право; криміналістика»; «Правові засади запобігання корупції».

***Постреквізити:*** "Кримінальне право»; «Кримінально-процесуальне право; криміналістика»; «Правові засади запобігання корупції».

Мова навчання – українська.

***Очікувані результати навчання здобувача вищої освіти*** *

У результаті засвоєння навчальної дисципліни здобувач вищої освіти має демонструвати такі результати навчання:

РНП НД – 1. Розкрити поняття злочинності, проаналізувати її онтологію, визначити гносеологічні засади пізнання.

РНП НД – 2. Здатність продемонструвати уміння формулювати нові гіпотези щодо пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку.

РНП НД – 3. Проаналізувати феноменологію кіберзлочинності на підставі статистичної звітності.

РНП НД – 4. Здатність пояснити різницю між різними концепціями причин злочинної поведінки.

РНП НД – 5. Розкрити природу кримінологічної детермінації кіберзлочинності, продемонструвати зв'язки і залежності з суспільними явищами і процесами.

РНП НД – 6. Класифікувати і охарактеризувати детермінанти кіберзлочинності.

РНП НД – 7. Розкрити основні положення вчення про особистість злочинця та охарактеризувати гносеологічні засади її пізнання.

РНП НД – 8. Проаналізувати особливості інноваційної діяльності органів охорони правопорядку та інноваційного менеджменту у сфері запобігання кіберзлочинності.

РНП НД – 9. Проаналізувати систему запобігання кіберзлочинності в Україні та визначити індикатори якості й ефективності її функціонування.

РНП НД – 10. Здатність здійснювати кримінологічні прогнози та розробляти плани заходів запобігання кіберзлочинності.

РНП НД – 11. Знати істотні ознаки кіберзлочинності, проаналізувати її детермінанти, визначати стратегічні напрями і заходи запобігання.

РНП НД – 12. Продемонструвати знання основних тенденцій поширення злочинів проти довкілля, причини та умов їх вчинення, сформулювати заходи запобігання.

***Види навчальних занять та самостійна робота***
***для здобувачів вищої освіти денної форми навчання***

| **№ п/п** | **Аудиторні заняття (контактні)** | | **Самостійна робота ( в годинах)** |
|---|---|---|---|
| | **Теми лекцій** | **Теми практичних занять** | |
| 1 | Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів. | Поняття кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів | |
| 2 | Поняття та кримінологічна характеристика кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності. | Поняття та кримінологічна характеристика кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності. | |
| 3 | Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система. | Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система. | |

| | | | |
|---|---|---|---|
| 4 | Детермінанти та основні напрямки запобігання кіберзлочинності<br>Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.<br>Система та загальна харктеристика кіберзлочинів.<br>Реалізація форм кримінальної відповідальності за кіберзлочини. | Детермінанти та основні напрямки запобігання кіберзлочинності<br>Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.<br>Система та загальна характеристика кіберзлочинів.<br>Реалізація форм кримінальної відповідальності за кіберзлочини. | |
| 5 | Особливості методики розслідування кіберзлочинів.<br>Поняття електронних доказів у кримінальному провадженні<br>Види електронних доказів<br>Способи збирання електронних доказів.<br>Використання електронних доказів під час судового розгляду. | Особливості методики розслідування кіберзлочинів.<br>Поняття електронних доказів у кримінальному провадженні<br>Види електронних доказів<br>Способи збирання електронних доказів.<br>Використання електронних доказів під час судового розгляду. | |

## Види навчальних занять та самостійна робота для здобувачів вищої освіти заочної форми навчання

| № п/п | Аудиторні заняття (контактні) | | Самостійна робота ( в годинах) |
|---|---|---|---|
| | Теми лекцій | Теми практичних занять | |
| 1 | Поняття | Поняття | |

| | | | |
|---|---|---|---|
| | кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів. | кіберзлочинності та її місце в загальній структурі злочинності. Види кіберзлочинів | |
| 2 | Поняття та кримінологічна характеристика кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності. | Поняття та кримінологічна характеристика кіберзлочинності. Особистість кіберзлочинця. Причини та умови вчинення кіберзлочинів. Запобігання кіберзлочинності. | |
| 3 | Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система. | Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система. | |
| 4 | Детермінанти та основні напрямки запобігання кіберзлочинності Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю. Система та загальна харктеристика кіберзлочинів. Реалізація форм кримінальної відповідальності за кіберзлочини. | Детермінанти та основні напрямки запобігання кіберзлочинності Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю. Система та загальна характеристика кіберзлочинів. Реалізація форм кримінальної відповідальності за кіберзлочини. | |
| 5 | Особливості методики | Особливості методики розслідування | |

| | | | |
|---|---|---|---|
| | розслідування кіберзлочинів. Поняття електронних доказів у кримінальному провадженні Види електронних доказів Способи збирання електронних доказів**.** Використання електронних доказів під час судового розгляду. | кіберзлочинів. Поняття електронних доказів у кримінальному провадженні Види електронних доказів Способи збирання електронних доказів**.** Використання електронних доказів під час судового розгляду. | |

## Самостійна робота студентів

Самостійна робота студентів здійснюється у таких формах:

– опрацювання нової наукової та навчальної літератури, узагальнення практики тощо;

– робота над кейсами;

– виконання практичних завдань, самотестування;

– написання есе та рефератів тощо.

Завдання та методичні рекомендації до самостійної роботи наведено у Навчально-методичному посібнику з навчальної дисципліни «Кіберзлочинність та електронні докази».

## Навчально-методичне та інформаційне забезпечення навчальної дисципліни

### Нормативно-правові акти

1. Конституція України від 28.06.1996 № 254к/96-ВР (в редакції від 30.09.2016) URL: http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

2. Закон України «Про основні засади забезпечення кібербезпеки України» [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/2163-19

3. Рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України".[Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/96/2016

4. Конвенція про кіберзлочинність, chttp://zakon.rada.gov.ua/laws/show/994_575

5. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/537-16

6. Закон України «Про захист інформації в інформаційно-

телекомунікаційних системах» [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

7. Закон України «Про Державну службу спеціального зв'язку та захисту інформації України», [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/3475-15

8. Рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/32/2017

9. Про стан виконання рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32 [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/n0006525-17

10. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [Електрон. ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF

**11.** Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави [Електрон. ресурс]. – Режим доступу: https://www.kmu.gov.ua/ua/npas/249267402

**Література**

1. Тихомиров О.О. Кіберзлочин: теоретико-правові проблеми / О.О.Тихомиров //Зб. матеріалів наук.-практ. конф. “Інформаційна безпека: виклики і загрози сучасності”; 5 квітня 2013 р.—К. : Наук.-вид. центр НА СБ України.—2013.—С. 179-182

2. Пфо, О. М. Основні поняття і класифікація кіберзлочинності / О. М. Пфо // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листоп. 2016 р. — Кропивницький : КНТУ, 2016. — С. 33-34.

3. Погорецький М. Кіберзлочини: до визначення поняття / М. Погорецький, В. Шеломенцев // Вісник прокуратури. — 2012. — № 8. — С. 89-96.

4. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству / Н. Мыщук // Вісник Львівського університету. Серія економічна. — 2014. — Випуск 51. — С. 173-179

5. Марків С. І. Кіберзлочинність. Нова кримінальна загроза / С. І. Марків // [Електронний ресурс]. — Режим доступу : http://gurt.org.ua/articles/34602/

6. Бельський Ю. Щодо визначення поняття кіберзлочину/ Ю. Бельський //Юридичний вісник. — 2014. — № 6. — С. 414-418

7. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. — Режим доступу : http://anticyber.com.ua/article_detail.php?id=140

8. Поняття та сутність кібернетичної злочинності [Електронний ресурс]. — Режим доступу : http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425%3A091216-07&catid=170%3A5-1216&Itemid=211&lang=en

9. Словник термінів з кібербезпеки / за заг. ред. О. Копана, Є. Скулиша. — К. : ВБ «Аванпост-Прим», 2012. — 214 с.

10. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка [Електронний ресурс]. — Режим доступу : http:// www.niss.gov.ua/articles/454

11. Стратегія забезпечення кібернетичної безпеки України (Проект) [Електронний ресурс]. — Режим доступу : www.niss.gov.ua/public/File/2013_nauk…/kiberstrateg.pdf

12. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини Навчальний посібник. — Х.: Право, 2014. — 513 с.

13. Конвенція про кіберзлочинність від 23.11.2001 р. // Офіційний вісник України від 10.09.2007 — 2007 р., — № 65. — стор. 107. — стаття 2535.

14. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р. // Офіційний вісник України. — 2010 р., № 56, / № 31, 2006, ст. 2202 /, — стор. 73, — стаття 1920.

15. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В. Бутузов. – К. : КИТ, 2010. – 148 с.

16. Всестороннее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора // UNODC/CCPCJ/EG.4/2013/2.

17. Преступления в сфере информационных технологий [Электронный ресурс]. –Режим доступа:http://www.ru.wikipedia.org/wiki.

18. Невидин С.Хейг: ущерб от киберпреступлений превышает $1 трлн [Электронный ресурс]. – Режим доступа: http://www.newsland.ru/news/detail/id/807021.

19. Интерпол: киберпреступления являются самой опасной криминальной угрозой [Электронный ресурс]. –Режим доступа: http://www.virusovnet.org/main/309.

20. Конвенция о борьбе с киберпреступностью [Электронный ресурс].–Режим доступа: http://194.8.63.186/portals.

21. АзаровД.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 / Д.С.Азаров. –К.: Ін-т держави і права НАН України, 2003. –18с.

**22.** Плугатир М.В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної

інформації: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.08 / М.В.Плугатир. –К.: Держ. наук.-дослід. ін-т МВС України, 2010.– 16с.

**Інтернет-ресурси**

Сайт Офісу Генерального прокурора - URL: http://www.gp.gov.ua/
Сайт Верховної Ради України - URL: http://rada.gov.ua
Офіційний веб-портал судової влади - http://court.gov.ua/ .
Сайт Національної поліції України - https://www.npu.gov.ua/

**Вимоги викладача**

Здобувачі вищої освіти *повинні*: регулярно відвідувати лекції й практичні/семінарські заняття; систематично та активно працювати на них; переконливо наводити аргументацію при розв'язанні завдань; якісно виконувати письмові й практичні завдання, контрольні та самостійні роботи тощо. Практичні заняття, пропущені за поважних причин, можуть бути відпрацьовані за попереднім узгодженням із викладачем.

Здобувачам вищої освіти *рекомендується*: брати участь в наукових конференціях, конкурсах наукових праць, роботі наукового гуртка кафедри, готувати тези наукових доповідей тощо.

*Обов'язкова вимога* - дотримання здобувачами вищої освіти норм «Кодексу академічної етики Національного юридичного університету імені Ярослава Мудрого» (https://nlu.edu.ua/files/norm_doc/kodeks_academichnoyi_etyky.pdf).

Викладач звертає особливу увагу на дотримання політики недопущення плагіату. У разі виявлення ознак порушення правил щодо недопущення плагіату або самостійності написання роботи може бути прийняте рішення про анулювання оцінки за роботу.

Присутність на лекційних на практичних заняття - обов'язкова. Під час як лекційних, так і практичних занять студенти мають право в будь який час ставити викладачеві запитання з відповідної теми та запрошуються брати активну участь у дискусії.

Під час аудиторних занять дозволяється використовувати ґаджети тільки у навчальних цілях (наприклад, для перегляду презентацій лекції). Дозволяється користуватися ноутбуками і планшетами для ведення конспектів лекцій та відстеження потрібної інформації.

**Контрольні заходи**

Оцінювання результатів засвоєння навчальної дисципліни «назва навчальної дисципліни» передбачає проведення поточного та підсумкового контролю і здійснюється на основі накопичувальної бально-рейтингової системи.

*Поточний контроль* знань включає:

- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни на *практичних заняттях* із застосуванням таких
- засобів: усне, письмове або експрес-опитування, виконання текстових завдань, вирішення практичних завдань або задач, участь у розробці кейсу, підготовка і захист есе або реферату за ініціативи студента;
- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни, що проводяться після модулів (колоквіуми, котрольні роботи тощо).

Протягом семестру студенти виконують завдання для *самостійної роботи* (підготовка презентації, есе, реферату тощо). Максимальна кількість балів за самостійну роботу – 10.

Формою *підсумкового контролю* знань здобувачів вищої освіти з навчальної дисципліни є залік.

***Шкала підсумкового педагогічного контролю:***

| **Оцінка за шкалою ECTS** | **Визначення** | **Оцінка за національною шкалою для заліку** | **Оцінка за 100- бальною шкалою, що використовується в НЮУ** |
|---|---|---|---|
| **A** | **Відмінно** – відмінне виконання, лише з незначною кількістю помилок | зараховано | 90 – 100 |
| **B** | **Дуже добре** – вище середнього рівня з кількома помилками | | 80 – 89 |
| **C** | **Добре** – у цілому правильна робота з певною кількістю незначних помилок | | 75 – 79 |
| **D** | **Задовільно** – непогано, але зі значною кількістю недоліків | | 70 – 74 |
| **E** | **Достатньо** – виконання задовольняє мінімальні критерії | | 60 – 69 |
| **FX** | **Незадовільно** – потрібно попрацювати перед тим, як перескладати | не зараховано | 35 – 59 |
| **F** | **Незадовільно** – необхідна серйозна подальша робота, обов’язковий повторний курс | | 0 – 34 |