Національний юридичний університет імені Ярослава Мудрого

Кафедри кримінології та кримінально-виконавчого права

П Р О Г Р А М А
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

Затверджено на засіданні
Вченої ради
протокол № від р.

Ректор
_____ Анатолій Гетьман

Харків 2021

Програма 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.____ с.

Розробник:
Таволжанський Олексій Володимирович – доцент кафедри кримінології та кримінально-виконавчого права 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.*

ЗМІСТ

1. Вступ

1.1. Мета та завдання 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.

1.2. Статус навчальної дисципліни у структурі освітньо-професійної програми: за вибором студента

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

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

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

1.3. Перелік предметних компетентностей здобувача вищої освіти:

ПК – 1. Знання та розуміння предмету кримінології і її місця в системі правових наук.

ПК – 3. Знання поняття кіберзлочинності, розуміння її онтології, опанування гносеологічних засадах її пізнання.

ПК – 6. Уміння орієнтуватися в концепціях причин злочинної поведінки.

ПК – 9. Знання основних положень вчення про особистість злочинця та розуміння гносеологічних засад її пізнання.

ПК – 11. Знання системи запобігання злочинності в Україні та розуміння меж.

ПК – 12. Знання стану наркозлочиності, її детермінації та особливостей запобігання.

ПК – 4. Уміння орієнтуватися в інноваційних підходах до пояснення феномену злочинності, закономірностей її функціонування і розвитку.

ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.

ПК – 8. Здатність до класифікації детермінантів кіберзлочинності та надання їх загальної характеристики.

ПК – 11. Знання системи запобігання злочинності в Україні та розуміння механізму її функціонування.

ПК – 8. Здатність до класифікації детермінантів кіберзлочинності та надання їх загальної характеристики.

ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.

ПК – 2. Знання методології і методів кримінологічних досліджень та уміння їх застосовувати у прикладних цілях.

ПК – 6. Уміння орієнтуватися в концепціях причин злочинної поведінки.

ПК – 5. Знання феноменології кіберзлочинності, здатність до аналізу та інтерпретації статистичних показників вимірювання кіберзлочинності.

ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.

ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.

ПК – 6. Уміння орієнтуватися в концепціях причин злочинної поведінки

ПК – 10. Знання правових засад державної політики України у сфері запобігання кіберзлочинності.

ПК – 8. Здатність до класифікації детермінантів кіберзлочинності та надання їх загальної характеристики.

ПК – 2. Знання методології і методів кримінологічних досліджень та уміння їх застосовувати у прикладних цілях.

ПК – 3. Знання поняття кіберзлочинності, розуміння її онтології, опанування гносеологічних засадах її пізнання..

ПК – 4. Уміння орієнтуватися в інноваційних підходах до пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку.

1.4. Перелік результатів навчання здобувача вищої освіти:**:**

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

РНП НД – 7. Розкрити основні положення вчення про особистість злочинця та охарактеризувати гносеологічні засади її 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 – 3. 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 – 12. Продемонструвати знання основних тенденцій поширення кіберзлочинів, причини та умов їх вчинення, сформулювати заходи запобігання.

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

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

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

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

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

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

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

Експлікація результатів освоєння навчальної дисципліни і результатів навчання за спеціальністю і спеціалізацією визначається в карті результатів навчання, сформульованих у термінах компетентностей (Додаток 2)

1.5. Модулі програми навчальної дисципліни.

Модуль 1. Кіберзлочинність: поняття, види та запобігання.

Модуль 2. Кримінально-правове забезпечення боротьби з кіберзлочинністю. Особливості методики розслідування кіберзлочинів. Електронні докази у кримінальному провадженні

Експлікація модулів компетентнісно-орієнтованої програми навчальної дисципліни визначається у матриці зв'язків між модулями навчальної дисципліни, результатами навчання та предметними компетентностями (Додаток 3).

2. Опис навчальної дисципліни (навчальні одиниці)

Курс	Рівень освіти, галузь знань, спеціальність, спеціалізація	Дидактична структура та кількість годин
Кількість кредитів ЄКТС: 2 Кількість модулів*: 2 Загальна кількість годин: 60 Тижневих годин: 2-4	Галузь знань – 08 «Право» Спеціальність – 081 «Право» Спеціалізація – «Прокуратура та кримінальна юстиція» Рівень освіти – другий (магістерський)	**Модуль 1** Лекції: 4 Практичні/семінарські заняття/ колоквіум: 4 Самостійна робота: 16 **Модуль 2** Лекції: 12 Практичні/семінарські заняття/колоквіум: 10 Самостійна робота: 14 поточний контроль; підсумковий контроль знань (залік)

3. Зміст програми навчальної дисципліни

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.

---

* рекомендується: не більше 2-3 модулів для навчальних дисципліни, які вивчаються один семестр; не більше 4-6 модулів для навчальних дисциплін, які вивчаються два семестри.

Європейський конвенційний механізм запобігання кіберзлочинності: поняття та система.

Детермінанти та основні напрямки запобігання кіберзлочинності

Модуль 2. Кримінально-правове забезпечення боротьби з кіберзлочинністю. Особливості методики розслідування кіберзлочинів. Електронні докази у кримінальному провадженні

Сучасний стан кримінально-правового забезпечення боротьби з кіберзлочинністю.

Система та загальна характеристика кіберзлочинів.

Реалізація форм кримінальної відповідальності за кіберзлочини.

Особливості методики розслідування кіберзлочинів.

Поняття електронних доказів у кримінальному провадженні

Види електронних доказів

Способи збирання електронних доказів**.**

Використання електронних доказів під час судового розгляду.

4. Ресурсне забезпечення навчальної дисципліни

4.1. *Форми організації освітнього процесу та види навчальних занять*
Навчальні заняття:
- лекції;
- практичні заняття

Самостійна робота

4.2. *Самостійна робота здобувачів вищої освіти*

Самостійна робота полягає в додатковому поглибленому опрацюванні студентами окремих питань навчальної дисципліни. Необхідно самостійно ознайомитись, критично осмислити та зробити висновки з рекомендованого наукового матеріалу.

Формами самостійної роботи та додаткових освітніх досягнень студентів є:

- виконання домашніх завдань;
- доопрацювання матеріалів лекцій;
- активна участь у обговоренні питань в ході практичних занять;
- робота у студентському науковому гуртку кафедри;
- наукове повідомлення за вузькоспеціальною проблематикою;

- створення портфоліо навчального курсу та його презентація;
- розробка кейсів;
- розробка схем, таблиць, слайдів з тем навчальної дисципліни;
- підготовка тематичних презентацій;
- підготовка та публікація наукових статей, тез;
- анотування наукових статей і монографій;
- здійснення аналізу законопроектів та змін до законодавства;
- інші здобутки, що підтверджені документально (грамоти, дипломи тощо);
- відвідування навчальних занять (є обов'язковим).

4.3. *Освітні технології та методи навчання*

Освітні технології:

- проблемне навчання;
- аудіо-візуальні технології;
- технологія студентоцентристського навчання.

Методи навчання:

- прес-конференція;
- дискусія;
- ділові ігри;
- підготовка судової промови за фабулою справи та виступ з нею;
- підготовка і проведення відео-презентації;

розробка кейсів.

4.4. *Форми педагогічного контролю та система оцінювання якості сформованих компетентностей за результатами засвоєння навчальної дисципліни*

Розподіл балів між формами організації освітнього процесу і видами контрольних заходів навчальної дисципліни «Кіберзлочинність та електронні докази» для здобувачів вищої освіти денної форми навчання при підсумковому контролі у формі заліку:

Поточний контроль			Самостійна робота студентів	Підсумкова оцінка знань (залік)
Практичні заняття				
Модуль № 1	Модуль № 2			
Max 20	Max 30		Max 10	max 100

Вид контролю	Кількість балів	Критерії (за кожною з оцінок)
Поточний контроль	Max 4	Відмінне засвоєння навчального матеріалу з теми, можливі окремі несуттєві недоліки.

на практичному/ семінарському занятті	3	Добре засвоєння матеріалу з теми, але є окремі помилки
	2	Задовільний рівень засвоєння матеріалу, значна кількість помилок
	1	Мінімальні результати, достатні для отримання позитивної оцінки
	Min 0	Незадовільний рівень засвоєння матеріалу.
Оцінка самостійної роботи студента	Max 10	Глибоке знання проблем, пов'язаних із темою дослідження, вільне володіння матеріалом, вміння самостійно й творчо мислити, знаходити, узагальнювати, аналізувати матеріал, робити самостійні теоретичні та практичні висновки.
	8	В роботі розкрито основні положення теми, але є деякі неточності у викладанні матеріалу, теоретичні поняття недостатньо підкріплено фактичними даними
	6	Основні положення теми розкрито, але деякі питання висвітлено неповно. Студент добре володіє матеріалом, але відсутня творчість та самостійність у дослідженні
	4	Основні теоретичні питання висвітлено поверхнево, немає висновків або висновки не мають самостійного характеру; студент слабко володіє матеріалом
	2	Основні положення теми висвітлено поверхнево, теоретичні положення не підкріплені фактичним матеріалом; немає висновків; студент слабко володіє матеріалом роботи.
	Min 0	Основні положення теми висвітлено поверхнево, з великою кількістю помилок; немає висновків; студент не володіє матеріалом роботи.
ЗАЛІК	Max 60	1. Всебічне, систематичне і глибоке знання матеріалу, передбаченого програмою навчальної дисципліни, у тому числі орієнтація в основних наукових доктринах та концепціях дисципліни. 2. Засвоєння основної та додаткової літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни та використання отриманих знань у практичній роботі.
	55	1. Повне знання матеріалу, передбаченого програмою навчальної дисципліни. 2. Засвоєння основної літератури та знайомство з додатковою літературою, рекомендованою кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	50	1. Достатньо повне знання матеріалу, передбаченого програмою навчальної дисципліни, за відсутності у відповіді суттєвих неточностей. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
	45	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Засвоєння основної літератури, рекомендованої

		кафедрою. 3. Помилки та суттєві неточності у відповіді на іспиті за наявності знань для їх самостійного усунення або за допомогою викладача.
	40	1. Знання основного матеріалу, передбаченого програмою навчальної дисципліни, в обсязі, достатньому для подальшого навчання і майбутньої роботи за професією. 2. Ознайомлення з основною літературою, рекомендованою кафедрою. 3. Помилки у відповіді на іспиті за наявності знань для усунення найсуттєвіших помилок за допомогою викладача.
	35	1. Прогалини в знаннях з певних частин основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Наявність помилок у відповіді на іспиті.
	Min 0	1. Відсутність знань значної частини основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Неможливість продовжити навчання або здійснювати професійну діяльність без проходження повторного курсу з цієї дисципліни.

Методи педагогічного контролю

Традиційні методи:

- методи усного контролю: індивідуальне опитування, розв'язання практичних завдань, складання процесуальних документів;

- методи письмового контролю: розв'язання тестових завдань, контрольні роботи, есе у рамках запропонованих тем; аналіз чинного законодавства або проектів законів, рішень Європейського Суду з прав людини тощо.

Інноваційні методи:

- участь у модельному судовому засіданні, інших ділових грах;
- підготовка судової промови за фабулою справи та виступ з нею;
- підготовка і проведення відео-презентації;
- розробка кейсів.

Методи самоконтролю:

- уміння самостійно оцінювати свої знання;
- здійснення аналізу відповідей або виступів інших студентів.

4.5. *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. Стратегічні комунікації: [словник] / Т. В. Попова, В. А. Ліпкан ; за заг. ред. доктора юридичних наук В. А. Ліпкана. — К. : ФОП Ліпкан О.С., 2016. — 416 с.

2. 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

3. 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.

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

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

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

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

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

9. 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

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

11. 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

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

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

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

15. 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.

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

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

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

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

20. Интерпол: киберпреступления являются самой опасной

криминальной угрозой [Электронный ресурс]. –Режим доступа: http://www.virusovnet.org/main/309.

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

22. 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.

23. 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/

Додаток 1

Карта предметних компетентностей з навчальної дисципліни

Шифр та назва компетентностей за спеціальністю і/або спеціалізацією	Шифр та назва компетентностей з навчальної дисципліни
ЗК – загальні (універсальні) компетентності.	**ПК – предметні компетентності з навчальної дисципліни**
ЗК-1.Знання та розуміння предметної галузі і професії.	ПК – 1. Знання та розуміння предмету кримінології і її місця в системі правових наук. ПК – 2. Знання методології і методів кримінологічних досліджень та уміння їх застосовувати у прикладних цілях.
ЗК-2.Здатність до вирішення проблем інноваційного характеру.	ПК – 5. Знання феноменології кіберзлочинності, здатність до аналізу та інтерпритації статистичних показників вимірювання кіберзлочинності. ПК – 6. Уміння орієнтуватися в концепціях причин злочинної поведінки.
ЗК-3.Здатність продукувати нові ідеї (креативність).	ПК – 7. Знання сутності кримінологічної детермінаціїі, розуміння зв'язків і залежностей кіберзлочинності з іншими явищами та процесами. ПК – 8. Здатність до класифікації детермінантів кіерзлочинності та надання їх загальної характеристики.
ЗК-4.Здатність до пошуку	ПК – 9. Знання основних положень вчення про

альтернативних рішень у професійній діяльності.	особистість злочинця та розуміння гносіологічних засад її пізнання.
ЗК-6.Уміння ефективно проводити наукові дослідження.	ПК – 10. Знання правових засад державної політики України у сфері запобігання кіберзлочинності.
ЗК-7.Уміння працювати в міждисциплінарній галузі.	ПК – 11. Знання системи запобігання злочинності в Україні та розуміння механізму її функціонування.
ЗК-8.Уміння розуміти великі обсяги інформації і критично-конструктивно її оцінювати.	ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.
ЗК-12.Уміння виявляти й використовувати джерела інформації (бібліографії, документи, web-сайти та ін.).	ПК – 4. Уміння орієнтуватися в інноваційних підходах до пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку. .
ЗК-13.Здатність оцінювати та підтримувати якість результату професійної діяльності.	ПК – 3. Знання поняття кіберзлочинності, розуміння її онтології, опанування гносіологічних засадах її пізнаня.
ЗК-14.Здатність формулювати особисту думку та доказово її представляти.	ПК – 9. Знання основних положень вчення про особистість злочинця та розуміння гносіологічних засад її пізнання.
ФКС – фахові компетентності за спеціальністю	
ФКС-1.Уміння розв’язувати складні задачі і проблеми у професійній діяльності або у процесі навчання, що передбачає проведення наукових досліджень та впровадження інновацій.	ПК – 1. Знання та розуміння предмету кримінології і її місця в системі правових наук. ПК – 2. Знання методології і методів кримінологічних досліджень та уміння їх застосовувати у прикладних цілях. ПК – 3. Знання поняття кіберзлочинності, розуміння її онтології, опанування гносіологічних засадах її пізнаня. ПК – 4. Уміння орієнтуватися в інноваційних підходах до пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку. ПК – 5. Знання феноменології кіберзлочинності, здатність до аналізу та інтерпретації статистичних показників вимірювання кіберзлочинності.
ФКС-2.Уміння орієнтуватися в проблемах юридичної науки.	ПК – 6. Уміння орієнтуватися в концепціях причин злочинної поведінки. ПК – 7. Знання сутності кримінологічної детермінаціїі, розуміння зв’язків і залежностей кіберзлочинності з іншими явищами та процесами.
ФКС-4.Здатність застосовувати	ПК – 8. Здатність до класифікації детермінантів

загальнонаукові та спеціальні юридичні методи дослідження.	кіерзлочинності та надання їх загальної характеристики.
ФКС-5.Знання феномену інновацій в контексті правової епістемології.	ПК – 9. Знання основних положень вчення про особистість злочинця та розуміння гносіологічних засад її пізнання.
ФКС-6.Знання особливостей інновацій в правовій сфері	ПК – 10. Знання правових засад державної політики України у сфері запобігання кіберзлочинності.
ФКС-11. Уміння інтерпретувати юридичну діяльність і соціально-правовий досвід як основних компонентів змісту юридичної практики	ПК – 11. Знання системи запобігання злочинності в Україні та розуміння механізму її функціонування. ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.
ФКС-12.Знання механізмів оцінки ефективності юридичної практики за видами юридичної діяльності	ПК – 11. Знання системи запобігання злочинності в Україні та розуміння механізму її функціонування.
ФКС-13.Знання гносеологічних і онтологічних підстав правового регулювання і правового впливу.	ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.
ФКС-14.Знання механізму вирішення юридичних колізій у правовому регулюванні суспільних відносин.	ПК – 12. Знання істотних ознак кіберзлочинності, розуміння її детермінантів та формулювання ідей щодо шляхів і заходів запобігання.
ФКС-16.Знання юридичної техніки та її прикладних аспектів (правотворчості, законодавчої техніки, техніки створення корпоративних актів, юридичних документів, систематизації юридичних актів, юридичної термінології тощо).	ПК – 11. Знання системи запобігання злочинності в Україні та розуміння механізму її функціонування.
ФКС-17. Уміння вживати організаційні заходи із взаємодії різних суб'єктів юридичної діяльності	ПК – 11. Знання системи запобігання злочинності в Україні та розуміння механізму її функціонування.
ФКС-18.Уміння застосовувати наукові принципи юридичного менеджменту та прийняття управлінських рішень у сфері юридичної діяльності	ПК – 3. Знання поняття кіберзлочинності, розуміння її онтології, опанування гносіологічних засадах її пізнаня. ПК – 4. Уміння орієнтуватися в інноваційних підходах до пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку.
ФКС-19.Знання структури та стандартів правничої професії та ролі правника в суспільстві	ПК – 4. Уміння орієнтуватися в інноваційних підходах до пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку.

Додаток 2

Карта результатів навчання здобувача вищої освіти, сформульованих у термінах компетентностей

Шифр та назва РН за спеціальністю і / або спеціалізацією	Модуль НД	Шифр та назва РН з навчальної дисципліни
РНС – результати навчання за спеціальністю		**Результати навчання з навчальної дисципліни**
РНС-1.Здатність продемонструвати знання й розуміння юриспруденції в сучасному наукознавстві.	№1	РНП НД – 1. Розкрити поняття злочинності, проаналізувати її онтологію, визначити гносеологічні засади пізнання.
РНС-2.Здатність продемонструвати знання й розуміння проблематики глобалізації та формування сучасних правових систем	№1	РНП НД – 2. Здатність продемонструвати уміння формулювати нові гіпотези щодо пояснення феномену кіберзлочинності, закономірностей її функціонування і розвитку.
РНС-3.Проаналізувати детермінант розвитку правової теорії.	№1	РНП НД – 3. Проаналізувати феноменологію кіберзлочинності на підставі статистичної звітності.
РНС-4.Проаналізувати методологічні аспекти взаємодії юридичної науки і юридичної практики	№1	РНП НД – 4. Здатність пояснити різницю між різними концепціями причин злочинної поведінки.
РНС-5.Інтерпретувати феномен юридичної практики як об'єкта науково-правових досліджень в юриспруденції	№1	РНП НД – 5. Розкрити природу кримінологічної детермінації кіберзлочинності, продемонструвати зв’язки і залежності з суспільними явищами і процесами.
РНС-6.Здатність продемонструвати уміння формулювати нові гіпотези та наукові проблеми в галузі права, обирати належні напрями й відповідні методи для їх дослідження	№1	РНП НД – 6. Класифікувати і охарактеризувати детермінанти кіберзлочинності.
РНС-7. Доводити епістемологічну правомірність висунення теоретичних альтернатив при проведенні наукових досліджень	№1	РНП НД – 7. Розкрити основні положення вчення про особистість злочинця та охарактеризувати гносеологічні засади її пізнання.
РНС-8.Проаналізувати особливості інноваційної діяльності та інноваційного менеджменту у правовій сфері	№1	РНП НД – 8. Проаналізувати особливості інноваційної діяльності органів охорони правопорядку та інноваційного менеджменту у сфері запобігання кіберзлочинності.
РНС-9.Охарактеризувати методи дослідження ефективності	№2	РНП НД – 9. Проаналізувати систему запобігання кіберзлочинності в Україні та

юридичної практики.		визначити індикатори якості й ефективності її функціонування.
РНС-10.Визначати індикатори якості й ефективності юридичної практики	№2	РНП НД – 10. Здатність здійснювати кримінологічні прогнози та розробляти плани заходів запобігання кіберзлочинності.
РНС-11.Здатність продемонструвати знання та розуміння прикладних аспектів правової герменевтики	№2	РНП НД – 11. Знати істотні ознаки кіберзлочинності, проаналізувати її детермінанти, визначати стратегічні напрями і заходи запобігання.
РНС-12.Проаналізувати феномен публічного і приватного регулювання в контексті епістемології та методології правових досліджень та юридичних практик.	№2	РНП НД – 12. Продемонструвати знання основних тенденцій поширення злочинів проти довкілля, причини та умов їх вчинення, сформулювати заходи запобігання.
РНС-13.Інтерпретувати основні напрями правової глобалізації та інтернаціоналізації та визначати правові механізми реалізації права в різних правопорядках та юрисдикціях	№2	РНП НД – 5. Розкрити природу кримінологічної детермінації кіберзлочинності, продемонструвати зв'язки і залежності з суспільними явищами і процесами.
РНС-14.Проаналізувати феномен конституціоналізації національного права і правопорядку	№2	РНП НД – 12. Продемонструвати знання основних тенденцій поширення злочинів проти довкілля, причини та умов їх вчинення, сформулювати заходи запобігання.
РНС-16.Здатність продемонструвати знання юридичної техніки та її прикладних аспектів в дискурсі правової епістемології та юридичної практики	№2	РНП НД – 1. Розкрити поняття злочинності, проаналізувати її онтологію, визначити гносеологічні засади пізнання.
РНС-17.Проаналізувати обумовленість девіацій у правовій сфері.	№2	РНП НД – 12. Продемонструвати знання основних тенденцій поширення злочинів проти довкілля, причини та умов їх вчинення, сформулювати заходи запобігання.
РНС-18.Здійснювати правовий комплаенс в межах професійних обов'язків	№2	РНП НД – 1. Розкрити поняття злочинності, проаналізувати її онтологію, визначити гносеологічні засади пізнання.
РНС-19.Здатність продемонструвати знання й розуміння діяти відповідно до вимог юридичної деонтології у професійній діяльності	№2	РНП НД – 12. Продемонструвати знання основних тенденцій поширення злочинів проти довкілля, причини та умов їх вчинення, сформулювати заходи запобігання.

Додаток 3

Матриця зв'язків модулів навчальної дисципліни, результатів навчання та предметних компетентностей у програмі навчальної дисципліни

Результати навчання за навчальною дисципліною / модулями	*Предметні компетентності*																	
	ПК – 1	ПК – 2	ПК – 3	ПК– 4	ПК – 5	ПК – 6	ПК – 7	ПК – 8	ПК – 9	ПК – 10	ПК – 11	ПК – 12	ПК – 13	ПК – 14	ПК – 15	ПК – 16	ПК – 17	ПК – 18
Модуль 1 РНС НД – 1. 1	X	X																
РНС НД – 1. 2		X																
РНС НД – 1. 3			X															
РНС НД – 1. 4									X						X			
РНС НД – 1. 5		X																
РНС НД – 1. 6											X			X				X
РНС НД – 1. 9														X				
РНС НД – 1. 11											X							
РНС НД – 1. 12										X			X					
Модуль 2 РНС НД 2.7			X					X					X					
РНС НД – 2. 8														X	X			
РНС НД – 2. 10											X	X				X		
РНС НД – 2. 13										X								X
РНС НД – 2. 14														X				
РНС НД – 2. 15						X												
РНС НД – 2. 16													X				X	
РНС НД – 2. 17							X											
РНС НД – 2. 18										X							X	