Національний юридичний університет імені Ярослава Мудрого

Кафедра кримінології та кримінально-виконавчого права

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

Рівень вищої освіти – перший (бакалаврський) рівень

Ступінь вищої освіти – бакалавр

Галузь знань – 08 «Право»

Спеціальність – 081 «Право»

Статус навчальної дисципліни – за вибором студента

Рік набору – 2020

Затверджено на засіданні
вченої ради
протокол № від р.

Ректор
_____ В.Я. Тацій

Харків 2020

Програма навчальної дисципліни «Запобігання кіберзлочинам» для здобувачів вищої освіти першого (бакалаврського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право». Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2020. 29 с.

Розробник:
Таволжанський Олексій Володимирович
кандидат юридичних наук, доцент, доцент кафедри
кримінології та кримінально-виконавчого права

Затверджено на засіданні кафедри
кримінології та кримінально-виконавчого права,
(протокол № 1 від 03 вересня 2020 р.)

***Завідувач кафед*ри —** Головкін Богдан Миколайович, доктор юридичних наук, професор

Зміст

1. Вступ

1.1. *Мета та завдання навчальної дисципліни.*

Мета навчальної дисципліни – формування системи наукових знань про правове регулювання запобігання кіберзлочинам, особу кіберзлочинця, причини та умови вчинення кримінальних правопорушень у віртуальній сфері, вивчення вітчизняних та зарубіжних підходів до розуміння змісту запобіжних заходів, вироблення основних умінь і навичок застосування національного законодавства, активізація аналітичної діяльності студентів, проведення науково-дослідницької роботи, а також практичних навичок діяльності правника.

Завдання:

– формування знань про кіберзлочинність, системи теоретичних знань про інститут кібербезпеки, його змістовне наповнення;

- опанування інструментарієм інституту запобігання кіберзлочинам, базовими категоріями кібербезпеки;

- визначення стану кіберзлочинності: рівня, структури, динаміки та інших показників;

– осмислення змісту актуальних проблем дослідження особи кіберзлочинця, формування криміногенної спрямованості особистості та мотивації кримінальної поведінки, типології і класифікації злочинців у віртуальній сфері;

- аналіз і дослідження прикладних проблем порядку формування та реалізації державної політики в сфері забезпечення кібербезпеки, спрямованих на набуття (підтвердження) суб’єктивних прав та покладення на приватних осіб передбачених законом обов’язків;

- наведення характеристики класифікацій та видів кіберзлочинів, аналіз їх структури, визначення стадій та етапів, окреслення повноважень суб’єктів запобігання кіберзлочинам;

- розвиток навичок і умінь запровадження та застосування заходів

запобігання кіберзлочинам.

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

1.3. Пререквізити: «Теорія права», «Логіка», «Історія держави і права України».

1.4. Кореквізити: «Адміністративне право», «Кримінальне право (Загальна частина)», «Кримінальне право (Особлива частина)», «Кримінальний процес».

1.5. Постреквізити: ----

1.6. Перелік предметних компетентностей здобувача вищої освіти:

ПК 1. Здатність оперувати основними поняттями і категоріями в сфері забезпечення кібербезпеки.

ПК 2. Знання і розуміння соціально-правової природи кіберзлочинності.

ПК 3. Здатність аналізувати рівень, структуру і динаміку кіберзлочинності.

ПК 4. Навички використання цифрових технологій і баз даних при оцінці стану кіберзлочинності в Україні, визначенні поточних і прогнозованих кримінальних загроз.

ПК 5. Знати і розуміти основні положення кримінологічного вчення про особу кіберзлочинця.

ПК 6. Здатність аналізувати структуру особи кіберзлочинця за сукупністю соціально-демографічних, морально-психологічних, кримінально-правових ознак.

ПК 7. Здатність здійснювати типологію і класифікацію кіберзлочинців.

ПК 8. Здатність до критичного та системного аналізу криміногенних явищ і процесів, що детермінують кіберзлочинність і застосування набутих знань у професійній діяльності.

ПК 9. Здатність грамотно і точно формулювати та висловлювати свої позиції щодо причин та умов вчинення кримінальних правопорушень у віртуальній сфері, належним чином їх обґрунтовувати.

ПК 10. Здатність розуміти зміст та роль віктимної поведінки у вчиненні кіберзлочину та інших кримінальних правопорушень.

ПК 11. Знання системи законодавства та механізму правового регулювання у сфері запобігання і протидії кіберзлочинності.

ПК 12. Знання і розуміння основ забезпечення національної безпеки України, структури, завдань та повноважень суб'єктів сектору кібербезпеки та оборони України, організаційних засад їх діяльності.

ПК 13. Здатність до логічного, критичного і системного аналізу документів стратегічного планування у сфері забезпечення кібербезпеки України, розуміння їх правового характеру та значення.

ПК 14. Здатність розуміти принципи, цілі та пріоритети державної політики протидії кіберзлочинності.

ПК 15. Здатність характеризувати структуру, завдання та повноваження суб'єктів протидії кіберзлочинності.

ПК 16. Знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю.

ПК 17. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам проти основ національної безпеки України.

ПК 18. Здатність надавати кримінологічну характеристику і знати заходи запобігання кримінальним правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему .

ПК 19. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

ПК 20. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).

ПК 21. Здатність надавати кримінологічну характеристику і знати заходи запобігання наркозлочинності з використанням віртуального простору.

ПК 22. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинності у військовій сфері.

ПК 23. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку.

ПК 24. Здатність надавати кримінологічну характеристику і знати заходи запобігання терористичній кіберзлочинній діяльності.

ПК 25. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж).

ПК 26. Здатність надавати кримінологічну характеристику і знати заходи запобігання корупційним кримінальним правопорушенням, що вчиняються з використанням віртуального простору.

ПК 27. Здатність надавати кримінологічну характеристику і знати заходи запобігання організованої кіберзлочинності.

ПК 28. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, пов'язаних з порушенням авторського права і суміжних прав.

Експлікація загальних і спеціальних компетентностей визначається в карті предметних компетентностей (Додаток 1)

1.7. Перелік результатів навчання здобувача вищої освіти:

РН НД 1.1. Володіти основними поняттями і категоріями запобігання кіберзлочинам.

РН НД 1.2. Пояснювати соціально-правову природу кіберзлочинності.

РН НД 1.3. Демонструвати вміння аналізувати рівень, структуру і динаміку кіберзлочинності

РН НД 1.4. Використовувати цифрові технології і бази даних при оцінці стану кіберзлочинності в Україні, визначенні поточних і прогнозованих кримінальних загроз.

РН НД 1.5. Виявляти знання і розуміння основних положень кримінологічного вчення про особу кіберзлочинця.

РН НД 1.6. Аналізувати структуру особи кіберзлочинця за сукупністю соціально-демографічних, морально-психологічних, кримінально-правових ознак.

РН НД 1.7. Демонструвати вміння здійснювати типологію і класифікацію кіберзлочинців.

РН НД 2.1. Демонструвати вміння критичного та системного аналізу криміногенних явищ і процесів, що детермінують кіберзлочинність і застосування набутих знань у професійній діяльності.

РН НД 2.2. Визначати й аналізувати причини та умови вчинення кримінальних правопорушень у віртуальній сфері.

РН НД 2.3. Застосовувати знання змісту та ролі віктимної поведінки у вчиненні кіберзлочинів у різних правових ситуаціях.

РН НД 2.4. Виявляти знання системи законодавства та механізму правового регулювання у сфері запобігання і протидії кіберзлочинності.

РН НД 2.5. Демонструвати комплексні знання основ забезпечення національної безпеки України та кібербезпеки, структури, завдань та повноважень суб’єктів сектору безпеки та оборони України, організаційних засад їх діяльності.

РН НД 2.6. Здійснювати логічний, критичний і системний аналіз документів стратегічного планування у сфері забезпечення національної

безпеки України, демонструвати розуміння їх правового характеру та значення.

РН НД 2.7. Аналізувати принципи, цілі та пріоритети державної політики протидії кіберзлочинності.

РН НД 2.8. Характеризувати структуру, завдання та повноваження суб'єктів протидії кіберзлочинності.

РН НД 2.9. Демонструвати знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю.

РН НД 3.1. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти основ національної безпеки України.

РН НД 3.2. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кримінальним правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

РН НД 3.3. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).

РН НД 3.4. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).

РН НД 3.5. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання наркозлочинності з використанням віртуальної сфери.

РН НД 3.6. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинності у військовій сфері.

РН НД 3.7. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку.

РН НД 3.8. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання терористичній кіберзлочинній діяльності.

РН НД 3.9. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж).

РН НД 3.10. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання корупційним кримінальним правопорушенням з використанням віртуального простору.

РН НД 3.11. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам у сфері економіки.

РН НД 3.12. Надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, пов'язаних з порушенням авторського права і суміжних прав.

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

1.8. Модулі програми навчальної дисципліни.

Модуль 1. Формування та реалізація державної політики в сфері кібербезпеки.

Модуль 2. Поняття кіберзлочину та механізми його запобігання.

Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання.

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)

<table>
<tr><th>Курс</th><th>Рівень освіти, галузь знань, спеціальність</th><th>Дидактична структура та кількість годин</th></tr>
<tr><td rowspan="2">Кількість кредитів – 6</td><td rowspan="6">Галузь знань – 08 «Право»

спеціальність – 081 "Право"

Рівень освіти – перший «бакалавр»</td><td>Модуль 1
Лекції: 10
Практичні заняття: 12
Самостійна робота: 40</td></tr>
<tr><td rowspan="2">Модуль 2
Лекції: 10
Практичні заняття: 12
Самостійна робота: 32</td></tr>
<tr><td>Модулів – 3</td></tr>
<tr><td>Загальна кількість годин - 180</td></tr>
<tr><td rowspan="2">Тижневих годин для денної форми навчання: аудиторних – 4, самостійної роботи студента - 6-8</td><td>Модуль 3
Лекції: 12
Практичні заняття: 12
Самостійна робота: 40</td></tr>
<tr><td>Види контролю:
поточний контроль;
підсумковий контроль знань залік</td></tr>
</table>

3. Зміст програми навчальної дисципліни

Модуль **1. Формування та реалізація державної політики у сфері кібербезпеки.**

Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності. Запобігання кіберзлочинам як міжгалузева дисципліна. Класифікація кіберзлочинів. Запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі.

Модуль **2. Базові засади запобігання кіберзлочинам**

Поняття і визначення кіберзлочину. Кіберзлочин як соціально-правове явище, особа кіберзлочинця, детермінація кіберзлочинності, запобігання кіберзлочинності. Запобігання кіберзлочинам як міжгалузева дисципліна. Класифікація кіберзлочинів. Запобігання кіберзлочинності на сучасному етапі розвитку України і в перспективі.

Кіберзлочинність та її вимірювання. Поняття кіберзлочинності та основні науково-практичні підходи щодо її розуміння і визначення. Кількісно-якісне вимірювання кіберзлочинності. Рівень кіберзлочинності. Структура кіберзлочинності. Кримінально-правові ознаки структури кіберзлочинності. Кримінологічні ознаки структури кіберзлочинності. Динаміка кіберзлочинності. Технічні фактори, які впливають на динаміку кіберзлочинності. Соціальні фактори, які впливають на динаміку кіберзлочинності. Правові фактори, які впливають на динаміку кіберзлочинності. Географія кіберзлочинності. Топографія кіберзлочинності. Ціна кіберзлочинності. Латентність кіберзлочинності. Структура латентної кіберзлочинності. Загальна характеристика сучасної кіберзлочинності в Україні, тенденції її розвитку. Детермінанти кіберзлочинності. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину.

Особа кіберзлочинця. Структура особистості кіберзлочинця. Соціально-демографічні ознаки особистості кіберзлочинця. Морально-психологічні якості і особистісно-рольові властивості особистості кіберзлочинця. Соціальне і біологічне в особистості кіберзлочинця, їх співвідношення. Типологія кіберзлочинців. Наукове і практичне значення вивчення особистості кіберзлочинця та її типології. Поняття причини кіберзлочину. Умови, що сприяють вчиненню кіберзлочину.

Запобігання кіберзлочинності: поняття, зміст, значення. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів. Загально соціальне, спеціально-кримінологічне та індивідуальне запобігання кіберзлочинності і окремих злочинів. Об’єкти запобігання кіберзлочинності.

Суб’єкти запобігання кіберзлочинності та основні напрями їх діяльності. Прогнозування в сфері кіберзахисту. Поточне прогнозування. Короткострокове прогнозування. Середньострокове прогнозування. Перспективне прогнозування. Загальнодержавне планування. Регіональне планування. Відомче та галузеве планування. Головні етапи планування.

Модуль **3. Теорія окремих видів кіберзлочинів та їх запобігання.**

Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Основні кримінологічні риси особистості кіберзлочинців, які вчиняють злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Причини та умови злочинів проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему. Запобігання кіберзлочинності проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.

Характеристика кіберзлочинів пов’язаних з використанням комп’ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп’ютерне шахрайство та комп’ютерне підроблення тощо). Особистість кібершахрая, основні риси. Причини і умови кіберзлочинів, пов’язаних з використанням комп’ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп’ютерне шахрайство та комп’ютерне підроблення тощо). Запобігання кіберзлочинам, пов’язаним з використанням комп’ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп’ютерне шахрайство та комп’ютерне підроблення тощо).

Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією). Особистість кіберзлочинця, основні риси. Причини і умови кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією). Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав. Причини та умови кіберзлочинів пов'язаних з порушенням авторського права і суміжних прав. Запобігання кіберзлочинам пов'язаних з порушенням авторського права і суміжних прав. Поняття та кримінологічна характеристика кіберзлочинів, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж). Хуліганство у віртуальній сфері. Запобігання кіберзлочинам проти громадського порядку та моральності. Поняття та взаємозв'язок організованої злочинності та кіберзлочинності. Характеристика організованої кіберзлочинності. Причини та умови організованої злочинності. Запобігання організованій злочинності. Міжнародне співробітництво у сфері запобігання організованій злочинності. Корупція у віртуальній сфері. Визначення корупції як соціального явища та зв'язок з новітніми технологіями, види корупційних кіберпроявів. Характеристика корупційної кіберзлочинності. Причини та умови корупційної злочинності. Запобігання корупційній злочинності. Характеристика злочинності неповнолітніх у віртуальній сфері. Особистість неповнолітнього кіберзлочинця, основні риси. Причини та умови кіберзлочинності неповнолітніх. Запобігання кіберзлочинності неповнолітніх.

Гібридна війна. Характеристика кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації. Причини та умови кіберзлочинів у сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення.

Поняття військових кіберзлочинів та їх характеристика. призову та мобілізації. Запобігання кіберзлочинам у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову та мобілізації.

4. Ресурсне забезпечення навчальної дисципліни

4.1. *Форми організації освітнього процесу та види навчальних занять:*

- форми організації освітнього процесу: навчальні заняття; самостійна робота; практична підготовка; контрольні заходи.

- види навчальних занять: лекції, практичні заняття, індивідуальні заняття, консультації.

4.2. Самостійна робота здобувачів вищої освіти

Самостійна робота – вид позааудиторної роботи навчального характеру, яка спрямована на вивчення програмного матеріалу навчального курсу. Під час цього виду роботи студент має самостійно опрацювати конспекти лекцій, рекомендовану літературу, нормативні акти, матеріали емпіричних досліджень до тем, що виносяться на практичні заняття.

Формами самостійної роботи студентів є: доопрацювання матеріалів лекції; робота в інформаційних мережах; наукове повідомлення за вузькоспеціальною проблематикою; підготовка тематичних презентацій; підготовка та публікація наукових статей, тез тощо; розробка схем, таблиць з тем навчальної дисципліни; анотування наукових статей і монографій; здійснення аналізу законопроєктів та змін законодавства й інше.

Самостійна робота студентів полягає у вивченні додаткової навчальної та наукової літератури, ознайомленні з рішеннями Європейського суду з прав людини, дослідженні практики застосування вітчизняного законодавства

тощо. Самостійна робота призначена для поглиблення знань студентів із тем, що передбачені навчальною дисципліною.

4.3. Освітні технології та методи навчання

- освітні технології: проблемне навчання, контекстне навчання, студентоцентроване навчання, аудіовізуальні технології, наукові дискусії, інтерактивні технології, ІТ-технології тощо;

- методи навчання: поєднання словесних, наочних і практичних методів, прес-конференції, метод проблемного викладання, ділові ігри, мозкові штурми, моделювання професійних ситуацій, кейс-метод, круглий стіл, метод дискусії та інші.

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

Формами контролю знань студентів є поточний та підсумковий контроль.

Поточний контроль знань студентів включає:

- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни на практичних заняттях із застосуванням таких засобів: усне, письмове або експрес-опитування, вирішення практичних завдань або задач, участь у розробці кейсів, захист есе або реферату за ініціативи студента. Поточний контроль має на меті перевірку рівня підготовки студента до вивчення поточного матеріалу. У ході практичного заняття студент може отримати оцінку за чотирибальною шкалою (0, 3, 4, 5);

- контроль якості засвоєння студентами програмного матеріалу навчальної дисципліни, що проводиться наприкінці модулів у формі колоквіумів або тестових завдань.

Впродовж семестру студенти виконують завдання для самостійної роботи (підготовка презентації, есе, реферату тощо). Максимальна кількість балів за самостійну роботу – 20 балів.

Формою підсумкового контролю знань здобувачів вищої освіти з навчальної дисципліни є залік. Мінімальна кількість балів для отримання заліку – 60 балів (за результатами проведення поточного контролю та оцінювання самостійної роботи студента).

Розподіл балів між формами організації освітнього процесу і видами контрольних заходів:

Поточний контроль						Самостійна робота студентів	Підсумкова оцінка знань (залік)
Модуль № 1		Модуль № 2		Модуль №3			
п/з	Колоквіум / тестові завдання	п/з	Колоквіум / тестові завдання	п/з	Колоквіум / тестові завдання		
max 10	max 10	max 25	max 10	max 15	max 10	max 20	мах 100

Критерії оцінювання результатів навчання:

Вид контролю	Кількість балів	Критерії (за кожною з оцінок)
Поточний контроль на практичному занятті	Max 5	Відмінне засвоєння навчального матеріалу з теми, можливі окремі несуттєві недоліки.
	4	Добре засвоєння матеріалу з теми, але є окремі помилки.
	3	Задовільний рівень засвоєння матеріалу, значна кількість помилок.
	Min 0	Незадовільний рівень засвоєння матеріалу.
Колоквіум / тестові завдання	Max 10	Результати опрацювання матеріалу високі, можлива незначна кількість несуттєвих помилок.
	8	Добре засвоєння матеріалу з теми, але є окремі помилки.
	6	Задовільний рівень засвоєння матеріалу, значна кількість несуттєвих помилок.
	4	Задовільний рівень засвоєння матеріалу, значна кількість суттєвих помилок.
	2	Прогалини в знаннях, студент слабко володіє матеріалом роботи.
	Min 0	Незадовільний рівень засвоєння матеріалу.
Оцінка самостійної роботи студента	Max 20	Глибоке знання проблем, пов'язаних із темою дослідження, вільне володіння матеріалом, вміння самостійно і творчо мислити, знаходити, узагальнювати, аналізувати матеріал, робити самостійні теоретичні та практичні висновки.
	15	У роботі розкрито основні положення теми, але є деякі неточності у викладенні матеріалу, теоретичні поняття недостатньо підкріплені фактичними даними.
	10	Основні положення теми розкрито, але деякі питання

		висвітлено неповно. Студент добре володіє матеріалом, але відсутня творчість і самостійність у дослідженні.
	5	Основні теоретичні питання висвітлено поверхнево та/або не підкріплені фактичним матеріалом; відсутні висновки або висновки не мають самостійного характеру; студент слабко володіє матеріалом роботи.
	0	Основні положення теми висвітлено поверхнево, з великою кількістю помилок; немає висновків; студент не володіє матеріалом роботи.
Залік	Min 60	Достатнє засвоєння матеріалу з дисципліни.
	Max 100	Відмінне володіння матеріалом із дисципліни.

4.5. Навчально-методичне та інформаційне забезпечення навчальної дисципліни

Нормативно-правові акти

Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду. URL : https://zakon.rada.gov.ua/laws/show/2341-14/ed20200813#Text .

Про Національну поліцію: Закон України від 02 липня 2015 року № 580-VIII. URL : https://zakon.rada.gov.ua/laws/show/580-19/ed20200703#Text

Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.2019 № 361-IX. URL: https://zakon.rada.gov.ua/laws/show/361-20/ed20200816#Text

Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. URL : https://zakon.rada.gov.ua/laws/show/2135-12/ed20200703#Text

Про організаційно-правові основи боротьби з організованою злочинністю: закон України від 30 червня 1993 року № 3341-XII. URL: https://zakon.rada.gov.ua/laws/show/3341-12/ed20200703#Text .

Про інформацію : Закон України від від 02.10.1992 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI URL : // https://zakon.rada.gov.ua/laws/show/2297-17/ed20200320#Text

Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text

Про основні засади забезпечення кібербезпеки України : Закону України від 05.10.2017 р. № 2163-VIII URL : https://zakon.rada.gov.ua/laws/show/2163-19/ed20200703#Text

Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII URL : https://zakon.rada.gov.ua/laws/show/2469-19/ed20200815#Text

Про кіберзлочинність : Конвенція ратифіковано із застереженнями і заявами Законом N 2824-IV ( ) від 07.09.2005, URL : https://zakon.rada.gov.ua/laws/show/994_575#Text

Література

Бідняк Г.С. Теорія і практика використання спеціальних знань при розслідуванні шахрайств: монограф. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2019. 152 с.

Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. Інформація і право. № 1(28)/2019. С. 108-117.

Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с.

Карчевський М.В. Правове регулювання соціалізації штучного інтелекту. Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. Науково-теоретичний журнал. 2017. С. 99-08.

Світличний О. П. Право інтелектуальної власності: Підручник. Вид. 2, змін. і доп. К.: Н УБіП України, 2017. 355 с.

Таволжанський О.В. Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів. Журнал східноєвропейського права. – 2018. - № 56. – С. 90-105.

Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація. Науково-інформаційний вісник Івано-

Франківського університету права імені Короля Данила Галицького. Серія : Право. - 2017. - № 4. - С. 158-164.

Viacheslav V. Vapniarchuk, Iryna I. Puchkovska, Oleksii V. Tavolzhanskyi, Roman I. Tashian Protection of ownership right in the court: the essence and particularities (Захист права власності в суді). Asia life science, Supplement 21(2), December 2019. Iss. 2. P. 863-879. Філіпини. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85077221643&origin=resultslist

V. V. Tsypko, K. I. Alieksieieva, I. A. Venger, *O. V. Tavolzhanskyi*, N. I. Galunets, A. V. Klyuchnik. Information policy of the enterprise as the basis for the reproduction of human potential in the structure of public social interaction. Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). - 2019. Румыния. - Vol. 10 Issue 6.- P.1664-1672. (Scopus) https://www.scopus.com/record/display.uri?eid=2-s2.0-85087468504&origin=resultslist

O. E. Kostyuchenko, T. V. Kolesnik, Z. V. Bilous, O. V. Tavolzhanskyi Robotization of manufacturing process: economic and social problems and legal ways of their solution (Роботизація виробничого процесу: економічні і соціальні проблеми та правові шляхи їх вирішення). Financial and credit activity:problems of theory and practice (Фінансово-кредитна діяльність: проблеми теорії та практики). - Харків, 2019. - Том 3, № 30. - С. 454-462. (Web of Science Core Collection)

Ovcharenko, Mykola O., *Tavolzhanskyi, Oleksii V.,* Radchenko, Tetiana M., *Kulyk, Kateryna D., Smetanina, Nataliia V.* Combating Illegal Drugs Trafficking Using the Internet by Means of the Profiling Method (Противодействие незаконному обороту наркотиков через Интернет с помощью метода профилирования). Journal of Advanced Research in Law and Economics (Журнал перспективных исследований в области права и экономики). Румыния. Vol. 11, n. 4 (2020), p. 1296-1304.

Інтернет-ресурси

Офіційний веб-портал Верховної Ради України. URL:

Офіційний веб-портал Президента України. URL:

Офіційний веб-портал Кабінету Міністрів України (єдиний веб-портал органів виконавчої влади України). URL:

Офіційний веб-портал судової влади України. URL:

Офіційний веб-портал Верховного Суду. URL:

Офіційний веб-портал Конституційного Суду України. URL:

Офіційний веб-портал Міністерства юстиції України. URL:

Офіційний веб-портал Офісу Генерального прокурора. URL:

Офіційний веб-портал Національного антикорупційного бюро України. URL:

Офіційний веб-портал Державного бюро розслідувань. URL:

Офіційний веб-портал Міністерства внутрішніх справ України. URL:

Офіційний веб-портал Інтерполу. URL:

Офіційний веб-портал Євроюсту. URL:

Офіційний веб-портал Європейського суду з прав людини. URL:

Офіційний веб-портал Єдиного державного реєстру судових рішень. URL:

СЕНМК

Стандартизований електронний навчально-методичний комплекс кафедри кримінології та кримінально-виконавчого права. URL: https://library.nlu.edu.ua/senmk/itemlist/category/199-kafedra-kriminologii-ta-kriminalno-vikonavchogo-prava.html

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. (обрати компетентності згідно зі змістом навчальної дисципліни)	**ПК – предметні компетентності з навчальної дисципліни**
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.	ПК 1. Здатність оперувати основними поняттями і категоріями в сфері забезпечення кібербезпеки. ПК 2. Знання і розуміння соціально-правової природи кіберзлочинності. ПК 3. Здатність аналізувати рівень, структуру і динаміку кіберзлочинності. ПК 4. Навички використання цифрових технологій і баз даних при оцінці стану кіберзлочинності в Україні, визначенні поточних і прогнозованих кримінальних загроз. ПК 5. Знати і розуміти основні положення кримінологічного вчення про особу кіберзлочинця.
ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.	ПК 6. Здатність аналізувати структуру особи кіберзлочинця за сукупністю соціально-демографічних, морально-психологічних, кримінально-правових ознак. ПК 7. Здатність здійснювати типологію і класифікацію кіберзлочинців. ПК 8. Здатність до критичного та системного аналізу криміногенних явищ і процесів, що детермінують кіберзлочинність і застосування набутих знань у професійній діяльності.
ЗК 6. Навички використання інформаційних і комунікаційних технологій.	ПК 9. Здатність грамотно і точно формулювати та висловлювати свої позиції щодо причин та умов вчинення кримінальних правопорушень у віртуальній сфері, належним чином їх обґрунтовувати. ПК 10. Здатність розуміти зміст та роль= віктимної поведінки у вчиненні кіберзлочину та інших кримінальних правопорушень. ПК 11. Знання системи законодавства та механізму правового регулювання у сфері запобігання і протидії кіберзлочинності. ПК 12. Знання і розуміння основ забезпечення національної безпеки України, структури, завдань та повноважень суб'єктів сектору кібербезпеки та оборони України, організаційних засад їх діяльності.
ЗК 7. Здатність вчитися і оволодівати сучасними знаннями.	ПК 13. Здатність до логічного, критичного і системного аналізу документів стратегічного планування у сфері забезпечення кібербезпеки України, розуміння їх правового характеру та значення. ПК 14. Здатність розуміти принципи, цілі та пріоритети державної політики протидії кіберзлочинності. ПК 15. Здатність характеризувати структуру, завдання та повноваження суб'єктів протидії кіберзлочинності. ПК 16. Знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю. ПК 17. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам

	проти основ національної безпеки України. ПК 18. Здатність надавати кримінологічну характеристику і знати заходи запобігання кримінальним правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему . ПК 19. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).
ЗК 1.2. Здатність грамотно і точно формулювати та висловлювати свої позиції, належним чином їх обґрунтовувати.	ПК 20. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією). ПК 21. Здатність надавати кримінологічну характеристику і знати заходи запобігання наркозлочинності з використанням віртуального простору. ПК 22. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинності у військовій сфері. ПК 23. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку. ПК 24. Здатність надавати кримінологічну характеристику і знати заходи запобігання терористичній кіберзлочинній діяльності. ПК 25. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж). ПК 26. Здатність надавати кримінологічну характеристику і знати заходи запобігання корупційним кримінальним правопорушенням, що вчиняються з використанням віртуального простору. ПК 27. Здатність надавати кримінологічну характеристику і знати заходи запобігання організованої кіберзлочинності. ПК 28. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, пов'язаних з порушенням авторського права і суміжних прав.
СК – спеціальні компетентності (обрати компетентності згідно зі змістом навчальної дисципліни)	
СК 6. Знання і розуміння основ права Європейського Союзу.	ПК 1. Здатність оперувати основними поняттями і категоріями в сфері забезпечення кібербезпеки. ПК 2. Знання і розуміння соціально-правової природи кіберзлочинності. ПК 3. Здатність аналізувати рівень, структуру і динаміку кіберзлочинності. ПК 4. Навички використання цифрових технологій і баз даних при оцінці стану кіберзлочинності в Україні, визначенні поточних і прогнозованих кримінальних загроз. ПК 5. Знати і розуміти основні положення кримінологічного вчення про особу кіберзлочинця. ПК 6. Здатність аналізувати структуру особи кіберзлочинця за сукупністю соціально-демографічних, морально-психологічних, кримінально-правових ознак. ПК 7. Здатність здійснювати типологію і

	класифікацію кіберзлочинців. ПК 8. Здатність до критичного та системного аналізу криміногенних явищ і процесів, що детермінують кіберзлочинність і застосування набутих знань у професійній діяльності.
СК 13. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності.	ПК 9. Здатність грамотно і точно формулювати та висловлювати свої позиції щодо причин та умов вчинення кримінальних правопорушень у віртуальній сфері, належним чином їх обґрунтовувати. ПК 10. Здатність розуміти зміст та роль= віктимної поведінки у вчиненні кіберзлочину та інших кримінальних правопорушень. ПК 11. Знання системи законодавства та механізму правового регулювання у сфері запобігання і протидії кіберзлочинності. ПК 12. Знання і розуміння основ забезпечення національної безпеки України, структури, завдань та повноважень суб'єктів сектору кібербезпеки та оборони України, організаційних засад їх діяльності.
СК 16. Здатність до логічного, критичного і системного аналізу документів, розуміння їх правового характеру і значення.	ПК 13. Здатність до логічного, критичного і системного аналізу документів стратегічного планування у сфері забезпечення кібербезпеки України, розуміння їх правового характеру та значення. ПК 14. Здатність розуміти принципи, цілі та пріоритети державної політики протидії кіберзлочинності. ПК 15. Здатність характеризувати структуру, завдання та повноваження суб'єктів протидії кіберзлочинності. ПК 16. Знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю. ПК 17. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам проти основ національної безпеки України. ПК 18. Здатність надавати кримінологічну характеристику і знати заходи запобігання кримінальним правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему . ПК 19. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо).
СК 1.1. Знання системи права та законодавства, а також механізмів правового регулювання в різних галузях права.	ПК 20. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією). ПК 21. Здатність надавати кримінологічну характеристику і знати заходи запобігання наркозлочинності з використанням віртуального простору. ПК 22. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинності у військовій сфері. ПК 23. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку. ПК 24. Здатність надавати кримінологічну характеристику і знати заходи запобігання терористичній

	кіберзлочинній діяльності.
СК 1.6. Знання і розуміння основ забезпечення національної безпеки України, структури, завдань та повноважень суб'єктів сектору безпеки та оборони України, організаційних основ їх діяльності.	ПК 25. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, зафіксованих в окремому протоколі (акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж). ПК 26. Здатність надавати кримінологічну характеристику і знати заходи запобігання корупційним кримінальним правопорушенням, що вчиняються з використанням віртуального простору. ПК 27. Здатність надавати кримінологічну характеристику і знати заходи запобігання організованої кіберзлочинності. ПК 28. Здатність надавати кримінологічну характеристику і знати заходи запобігання кіберзлочинам, пов'язаних з порушенням авторського права і суміжних прав.

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
ПРН – результати навчання за спеціальністю / спеціалізацією (обрати результати навчання згідно зі змістом навчальної дисципліни)		**Результати навчання з навчальної дисципліни**
ПРН 4. Формулювати власні обґрунтовані судження на основі аналізу відомої проблеми.	№1	РН НД 1.1. Володіти основними поняттями і категоріями запобігання кіберзлочинам. РН НД 1.2. Пояснювати соціально-правову природу кіберзлочинності.
ПРН 12. Доносити до респондента матеріал з певної проблематики доступно і зрозуміло.	№1	РН НД 1.3. Демонструвати вміння аналізувати рівень, структуру і динаміку кіберзлочинності. РН НД 1.4. Використовувати цифрові технології і бази даних при оцінці стану кіберзлочинності в Україні, визначенні поточних і прогнозованих кримінальних загроз.
ПРН 14. Належно використовувати статистичну інформацію, отриману з першоджерел та вторинних джерел для своєї професійної діяльності.	№1	РН НД 1.5. Виявляти знання і розуміння основних положень кримінологічного вчення про особу кіберзлочинця. РН НД 1.6. Аналізувати структуру особи кіберзлочинця за сукупністю соціально-демографічних, морально-психологічних, кримінально-правових ознак.
ПРН 15. Вільно використовувати для професійної діяльності доступні інформаційні технології і бази даних.	№1	РН НД 1.7. Демонструвати вміння здійснювати типологію і класифікацію кіберзлочинців.
ПРН 20. Пояснювати природу та зміст основних правових явищ і процесів.	№2	РН НД 2.1. Демонструвати вміння критичного та системного аналізу криміногенних явищ і процесів, що детермінують кіберзлочинність і застосування набутих знань у професійній діяльності. РН НД 2.2. Визначати й аналізувати причини та умови вчинення кримінальних правопорушень у

		віртуальній сфері.
ПРН 21. Застосовувати набуті знання у різних правових ситуаціях, виокремлювати юридично значущі факти і формулювати обґрунтовані правові висновки	№2	РН НД 2.3. Застосовувати знання змісту та ролі віктимної поведінки у вчиненні кіберзлочинів у різних правових ситуаціях. РН НД 2.4. Виявляти знання системи законодавства та механізму правового регулювання у сфері запобігання і протидії кіберзлочинності. РН НД 2.5. Демонструвати комплексні знання основ забезпечення національної безпеки України та кібербезпеки, структури, завдань та повноважень суб'єктів сектору безпеки та оборони України, організаційних засад їх діяльності.
ПРН 22. Готувати проекти необхідних актів застосування права відповідно до правового висновку зробленого у різних правових ситуаціях.	№2	РН НД 2.6. Здійснювати логічний, критичний і системний аналіз документів стратегічного планування у сфері забезпечення національної безпеки України, демонструвати розуміння їх правового характеру та значення. РН НД 2.7. Аналізувати принципи, цілі та пріоритети державної політики протидії кіберзлочинності.РН НД 2.8. Характеризувати структуру, завдання та повноваження суб'єктів протидії кіберзлочинності. РН НД 2.9. Демонструвати знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю.
ПРН1.1. Виявляти проблеми у правовому регулюванні і пропонувати способи їх вирішення відповідно до принципів захисту прав людини і її основоположних свобод.	№3	РН НД 3.1. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти основ національної безпеки України. РН НД 3.2. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кримінальним правопорушенням проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.
ПРН1.7. Демонструвати навички планування та здійснення досудового розслідування кримінальних проваджень, контррозвідувальної та оперативно-розшукової діяльності, конфіденційного співробітництва.	№3	РН НД 3.3. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинів пов'язаних з використанням комп'ютера як засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо). РН НД 3.4. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією).

		РН НД 3.5. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання наркозлочинності з використанням віртуальної сфери. РН НД 3.6. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинності у військовій сфері. РН НД 3.7. Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку.

Додаток 3

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

Результати навчання за навчальною дисципліною / модулями	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	ПК 19	ПК 20	ПК 21	ПК 22	ПК 23	ПК 24	ПК 25	ПК 26	ПК 27	ПК 28
Засадничі положення криміно-логії / Модуль 1																												
РН НД 1.1.	**x**																											
РН НД 1.2.		**x**																										
РН НД 1.3.			**x**																									
РН НД 1.4.				**x**																								
РН НД 1.5.					**x**																							
РН НД 1.6.						**x**																						
РН НД 1.7.							**x**																					
Теоретичні проблеми криміно-логії / Модуль 2																												
РН НД 2.1.								**x**																				
РН НД 2.2.									**x**																			
РН НД 2.3.										**x**																		
РН НД 2.4.											**x**																	
РН НД 2.5.												**x**																
РН НД 2.6.													**x**															
РН НД 2.7.														**x**														
РН НД 2.8.															**x**													
РН НД 2.9.																**x**												
Прикладні проблеми запобігання /Модуль 3.																												
РН НД 3.1																	**x**											
РН НД 3.2																		**x**										
РН НД 3.3																			**x**									
РН НД 3.4																				**x**								
РН НД 3.5																					**x**							
РН НД 3.6.																						**x**						
РН НД 3.7.																							**x**					
РН НД 3.8.																								**x**				

РН НД 3.9.																								**x**			
РН НД 3.10.																									**x**		
РН НД 3.11.																										**x**	
РН НД 3.12.																											**x**