Національний юридичний університет імені Ярослава Мудрого

Кафедра кримінології та кримінально-виконавчого права

РОБОЧА 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

Харків 2020

Робоча 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. 26 с.

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

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

Завідувач кафедри - Головкін Богдан Миколайович, доктор юридичних наук, професор

Зміст

1. *Опис навчальної дисципліни*

Робоча програма навчальної дисципліни «**Запобігання кіберзлочинам**» розроблена відповідно до освітньо-професійної програми «Право» першого (бакалаврського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право».

Найменування показників	Галузь знань, спеціальність, рівень освіти	Дидактична структура навчальної дисципліни	
		денна форма навчання	заочна форма навчання
Кількість кредитів ЄКТС – 6,0	Галузь знань – 08 «Право» Спеціальність – 081 «Право» Рівень освіти – перший (бакалаврський)	За вибором студента	За вибором студента
Кількість модулів – 3		Рік підготовки: 2021–2024	Рік підготовки: 2021–2024
		семестр	семестр
Загальна кількість годин - 180		3-8	3-8
Тижневих годин для денної форми навчання: аудиторних – 2-4, самостійної роботи студента – 6-8.		**Лекції**	**Лекції**
		32 год.	16 год.
		Практичні / семінарські заняття	**Практичні / семінарські заняття**
		36 год.	8 год.
		Самостійна робота	**Самостійна робота**
		112 год.	156 год.
		Види контролю: поточний контроль; підсумковий контроль знань (залік)	Види контролю: поточний контроль; підсумковий контроль знань (залік)

Мета викладання навчальної дисципліни – формування системи знань про кіберзлочинність та її характеристики, особу кіберзлочинця, причини та умови вчинення кримінальних правопорушень у віртуальному просторі, організаційні та правові засади функціонування системи запобігання кіберзлочинності, міжнародні стандарти боротьби із кіберзлочинністю, набуття здатності розв’язувати під час навчання складні задачі і проблеми, пов’язані із застосуванням законодавства щодо

запобігання і протидії кіберзлочинності, активізація аналітичної та науково-дослідницької діяльності студентів, а також формування 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.

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

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

Постреквізити: ----

2. *Очікувані результати навчання*

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

РН-1	Пояснювати соціально-правову природу кіберзлочинності
РН 2	Демонструвати вміння аналізувати рівень, структуру і динаміку кіберзлочинності
РН-3	Визначати й аналізувати причини та умови вчинення кримінальних правопорушень у віртуальному просторі
РН-4	Демонструвати вміння здійснювати типологію і класифікацію кіберзлочинців
РН-5	Демонструвати знання та розуміння міжнародних стандартів, зарубіжного досвіду і кращих практик боротьби із кіберзлочинністю
РН-6	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-7	Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти основ національної безпеки України
РН-8	Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинності
РН-9	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-10	Надавати кримінологічну характеристику і демонструвати знання заходів запобігання кіберзлочинам проти миру, безпеки людства та міжнародного порядку
РН-11	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-12	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).

Викладання навчальної дисципліни забезпечує формування у здобувача вищої освіти загальних і спеціальних компетентностей та досягнення результатів навчання, визначених стандартом вищої освіти відповідної спеціальності та освітньо-професійною програмою «Право», а саме:

***Загальних компетентностей**:*

ЗК1. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК3. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК6. Навички використання інформаційних і комунікаційних технологій.

ЗК7. Здатність вчитися і оволодівати сучасними знаннями.

ЗК1.2. Здатність грамотно і точно формулювати та висловлювати свої позиції, належним чином їх обґрунтовувати.

***Спеціальних компетентностей**:*

СК3. Повага до честі і гідності людини як найвищої соціальної цінності, розуміння їх правової природи.

СК4. Знання і розуміння міжнародних стандартів прав людини, положень Конвенції про захист прав людини та основоположних свобод, а також практики Європейського суду з прав людини.

СК 6. Знання і розуміння основ права Європейського Союзу.

СК13. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань у професійній діяльності.

СК16. Здатність до логічного, критичного і системного аналізу документів, розуміння їх правового характеру і значення.

СК 1.1. Знання системи права та законодавства, а також механізмів правового регулювання в різних галузях права.

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.

Програмних результатів навчання:

ПРН 4. Формулювати власні обґрунтовані судження на основі аналізу відомої проблеми.

ПРН 12. Доносити до респондента матеріал з певної проблематики доступно і зрозуміло.

ПРН 14. Належно використовувати статистичну інформацію, отриману з першоджерел та вторинних джерел для своєї професійної діяльності.

ПРН 15. Вільно використовувати для професійної діяльності доступні інформаційні технології і бази даних.

ПРН 20. Пояснювати природу та зміст основних правових явищ і процесів.

ПРН 21. Застосовувати набуті знання у різних правових ситуаціях, виокремлювати юридично значущі факти і формулювати обґрунтовані правові висновки

ПРН 22. Готувати проекти необхідних актів застосування права відповідно до правового висновку зробленого у різних правових ситуаціях.

ПРН 1.4 Демонструвати вміння застосовувати набуті правові знання за умов самостійного прийняття юридичних рішень відповідно щодо своїх професійних статусів.

ПРН 1.6. Демонструвати комплексні знання основ правового забезпечення національної безпеки та оборони держави, здійснювати характеристику суб'єктно-об'єктного складу сектору безпеки та оборони України, порядку взаємодії та координації його суб'єктів.

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. Обсяг і структура навчальної дисципліни

4.1. Для здобувачів вищої освіти денної форми навчання

№ п/п	**Дата проведення (згідно розкладу)**	**Тематика навчального курсу**	**Обсяг у годинах**			
			Усього	**У тому числі**		
				Лекції	**Практичні заняття, семінарські заняття, колоквіуми тощо**	**Самостійна робота**
		Модуль 1. Формування та реалізація державної політики в сфері кібербезпеки.				
		Тема 1. Основні цілі, напрями та принципи державної політики у сфері	**8**	**2**	**2**	**4**

		кібербезпеки.				
		Тема 2. Стан забезпечення кібербезпеки на сучасному етапі.	**18**	**4**	**4**	**10**
		Разом	**26**	**6**	**8**	**14**
		Модуль 2. Базові засади запобігання кіберзлочинам.				
		Тема 1. Поняття і визначення кіберзлочину.	**18**	**2**	**4**	**12**
		Тема 2. Кіберзлочинність та її вимірювання.	**20**	**4**	**4**	**12**
		Тема 3. Особа кіберзлочинця.	**18**	**2**	**4**	**12**
		Тема 4. Запобігання кіберзлочинності: поняття, зміст, значення.	**20**	**4**	**4**	**12**
		Разом	**76**	**12**	**16**	**48**
		Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання.				
		Тема 1. 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.	**22**	**4**	**4**	**14**
		Тема 2. Характеристика кіберзлочинів пов'язаних з використанням комп'ютера як	**20**	**4**	**4**	**12**

		засобу скоєння злочинів, а саме, як засіб маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерне підроблення тощо)				
		Тема 3. Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією)та інших кіберзлочинів	**22**	**4**	**4**	**14**
		Тема 4. Гібридна війна.	**14**	**2**	**2**	**10**
		Разом	**78**	**14**	**14**	**50**
		Усього годин / кредитів ECTS	**180/6,0**	**26**	**76**	**78**

4.2. Для здобувачів вищої освіти заочної форми навчання

№ п/п	**Дата проведення (згідно розкладу)**	**Тематика навчального курсу**	**Обсяг у годинах**			
			Усього	**У тому числі**		
				Лекції	**Практичні заняття, семінарські заняття, колоквіуми тощо**	**Самостійна робота**
		Модуль 1. Формування та реалізація державної політики в сфері кібербезпеки.				
		Тема 1. Поняття кібербезпеки, її основні категорії.	14	2	2	10
		Тема 2. Правові основи забезпечення	20	-	-	20

		кібербезпеки України.				
		Тема 3. Об’єкти кібербезпеки та кіберзахисту.	22	2	-	20
		Разом	***56***	***4***	***2***	***50***
		Модуль 2. Базові засади запобігання кіберзлочинам.				
		Тема 1. Поняття і визначення кіберзлочину. Показники кіберзлочинності.	14	2	2	10
		Тема 2. Зміст поняття кіберзлочинець й основні підходи до його визначення. Структура особистості кіберзлочинця. Детермінація кіберзлочинності.	22	2	-	20
		Тема 3. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів.	22	2	-	20
		Разом	**58**	**6**	**2**	**50**
		Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання.				
		Тема 1. Стан сучасної кібербезпеки в Україні та у зарубіжних країнах.	2	2	-	-
		Тема 2. Підходи до класифікації кіберзлочинів. Характеристика кіберзлочинності проти конфіденційності,	14	2	2	10

		цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.				
		Тема 3. 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) .	10	-	-	10
		Тема 4. Характеристика кіберзлочинів, пов'язаних з контентом (змістом даних), розміщених у комп'ютерних мережах (зокрема злочини, пов'язані з дитячою порнографією)та інших кіберзлочинів.	12	2	-	10
		Тема 5. Характеристика кіберзлочинів, пов'язаних з порушенням авторського права і суміжних прав.	12	-	2	10
		Тема 6. Гібридна війна. Характеристика кіберзлочинів у	16	-	-	16

		сфері охорони державної таємниці, недоторканності державних кордонів, забезпечення призову та мобілізації.				
		Разом	66	6	4	56
		Усього годин / кредитів ECTS	**180/6,0**	**16**	**8**	**156**

5. Форми педагогічного контролю та засоби оцінювання результатів навчання

Оцінювання результатів засвоєння навчальної дисципліни «Запобігання кіберзлочинам» 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, 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;

- виконання студентами впродовж семестру завдань 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

6. 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.

7. Педагогічний контроль для здобувачів вищої освіти денної/заочної форми навчання

Шкала підсумкового педагогічного контролю

Оцінка за шкалою ECTS	Визначення	Оцінка за національною шкалою	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

8. 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: http://rada.gov.ua/

Офіційний веб-портал Президента України. URL: http://www.president.gov.ua

Офіційний веб-портал Кабінету Міністрів України (єдиний веб-портал органів виконавчої влади України). URL: http://www.kmu.gov.ua

Офіційний веб-портал судової влади України. URL: https://court.gov.ua/

Офіційний веб-портал Верховного Суду. URL: https://supreme.court.gov.ua/supreme/gromadyanam/perelik_sprav/

Офіційний веб-портал Конституційного Суду України. URL: https://ccu.gov.ua/

Офіційний веб-портал Міністерства юстиції України. URL: https://minjust.gov.ua/

Офіційний веб-портал Офісу Генерального прокурора. URL: www.gp.gov.ua/

Офіційний веб-портал Національного антикорупційного бюро України. URL: https://nabu.gov.ua/

Офіційний веб-портал Державного бюро розслідувань. URL: https://dbr.gov.ua/

Офіційний веб-портал Міністерства внутрішніх справ України. URL: https://mvs.gov.ua/uk

Офіційний веб-портал Інтерполу. URL: https://www.interpol.int/

Офіційний веб-портал Євроюсту. URL: https://www.eurojust.europa.eu/

Офіційний веб-портал Європейського суду з прав людини. URL: https://www.echr.coe.int/Pages/home.aspx?p=applicants/ukr&c

Офіційний веб-портал Єдиного державного реєстру судових рішень. URL: http://www.reyestr.court.gov.ua/

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