Національний юридичний університет імені Ярослава Мудрого

Кафедра кримінології та кримінально-виконавчого права

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ЗАПОБІГАННЯ КІБЕРЗЛОЧИНАМ»

Рівень вищої освіти – другий (магістерський) рівень

Ступінь вищої освіти – магістр

Галузь знань – 08 «Право»

Спеціальність – 081 «Право»

Статус навчальної дисципліни – за вибором курсанта

Рік набору – 2021

Харків 2021

Робоча програма навчальної дисципліни «Запобігання кіберзлочинам» для здобувачів вищої освіти другого (магістерського) рівня вищої освіти галузі знань 08 «Право» спеціальності 081 «Право». Харків: Нац. юрид. ун-т імені Ярослава Мудрого, 2021. 21 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 № 14 від 30 червня 2021 р.)

Оновлену редакцію (зі змінами та доповненнями) затверджено на засіданні кафедри кримінології та кримінально-виконавчого права
(протокол № 14 від 10 червня 2022 р.)

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

Зміст

1. Опис навчальної дисципліни……...4
2. Очікувані результати навчання…….……5
3. Зміст програми навчальної дисципліни……..8
4. Обсяг і структура навчальної дисципліни…….....12
5. Форми педагогічного контролю та засоби оцінювання результатів навчання
.....15
6. Критерії оцінювання результатів навчання……...16
7. Педагогічний контроль для здобувачів вищої освіти заочної форми навчання…….....18
8. Навчально-методичне та інформаційне забезпечення навчальної дисципліни…….18

1. Опис навчальної дисципліни

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

Найменування показників	Галузь знань, спеціальність, рівень освіти	Дидактична структура навчальної дисципліни
		денна форма навчання
Кількість кредитів ЄКТС – 4,0	Галузь знань – 08 «Право» Спеціальність – 081 «Право» Рівень освіти – другий (магістерський)	За вибором курсанта
Кількість модулів – 3		Рік підготовки: 2021-2022
		семестр
Загальна кількість годин - 120		2
Тижневих годин для денної форми навчання: аудиторних – 2 - 4, самостійної роботи студента - 6 - 8.		**Лекції**
		20 год.
		Практичні/ семінарські заняття
		20 год.
		Самостійна робота
		80 год.
		Види контролю: поточний контроль; підсумковий контроль знань (диференційований залік)

Мета навчальної дисципліни – формування системи наукових знань про правове регулювання запобігання кіберзлочинів, вивчення вітчизняних та зарубіжних підходів до розуміння змісту заходів забезпечення кібербезпеки, вироблення основних умінь і навичок застосування національного законодавства, активізація аналітичної діяльності студентів, проведення науково-дослідницької роботи, а також практичних навичок діяльності правника.

Завдання:

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

- опанування інструментарієм інституту запобігання кіберзлочинам,

базовими категоріями кібербезпеки;

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

- 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», «Конституційне право України», «Цивільне право», «Цивільний процес», «Кримінальне право», «Міжнародне право».

Кореквізити: «Інформаційні технології в контррозвідувальній діяльності», «Інформаційне право», «Організація контррозвідувальної діяльності підрозділів контррозвідувального захисту інтересів держави в сфері інформаційної безпеки».

Постреквізити: -

2. Очікувані результати навчання

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

РН-1.	Аналізувати понятійний апарат у сфері кіберзахисту, детермінанти та зміст кіберзлочинності.
РН 2.	Дискутувати зі складних правових проблем застосування європейських стандартів забезпечення кібербезпеки.
РН-3.	Здійснювати дослідження правового регулювання у віртуальній сфері.
РН-4	Здійснювати порівняльно-правовий аналіз національних актів із

	іншими актами спрямованими на запобігання кіберзлочинам.
РН-5	Демонструвати навички визначення стану кіберзлочинності.
РН-6	Розкривати зміст підзаконних актів якими впроваджуються заходи спрямовані на запобігання кіберзлочинам.
РН-7	Аналізувати способи припинення кібератак.
РН-8	Демонструвати знання актуальних детермінант кіберзлочиності.
РН-9	Розкривати особливості правового регулювання запобігання різним видам кіберзлочинів.
РН-10	Демонструвати навички застосування принципів забезпечення кібербезпеки.
РН-11	Формувати власне бачення змісту запобігання кіберзлочнам.
РН-12	Розробляти алгоритми проведення заходів із урахуванням базових ідей запобігання кіберзлочинам.

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. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК6. Здатність генерувати нові ідеї (креативність).

ЗК8. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів економічної діяльності).

ЗК1.1. Здатність вирішувати проблеми інноваційного характеру.

ЗК1.3. Здатність формулювати особисту думку та доказово її представляти.

ЗК1.5. Здатність до лідерства, відповідальності, ухвалення неупереджених і вмотивованих рішень.

Спеціальних компетентностей:

СК4. Здатність оцінювати взаємодію міжнародного права та

міжнародних правових систем з правовою системою України.

СК5. Здатність використовувати сучасні правові доктрини та принципи у правотворчості та в процесі застосовування інститутів публічного і приватного права, а також кримінальної юстиції.

СК6. Здатність обґрунтовувати та мотивувати правові рішення, давати розгорнуту юридичну аргументацію.

СК9. Здатність застосовувати міждисциплінарний підхід в оцінці правових явищ та правозастосовній діяльності.

СК 10. Здатність ухвалювати рішення у ситуаціях, що вимагають системного, логічного та функціонального тлумачення норм права, а також розуміння особливостей практики їх застосування.

СК13. Здатність доносити до фахівців і нефахівців у сфері права інформацію, ідеї, зміст проблем та характер оптимальних рішень з належною аргументацією.

СК1.1. Здатність аналізувати механізми оцінки ефективності юридичної практики за напрямами (галузями) юридичної діяльності.

СК1.2. Здатність демонструвати знання й розуміння правових систем в умовах глобалізації.

СК1.3. Здатність розрізняти принципи інститутів публічного і приватного права в юридичній діяльності.

Програмних результатів навчання:

ПРН3. Проводити збір, інтегрований аналіз та узагальнення матеріалів з різних джерел, включаючи наукову та професійну літературу, бази даних, цифрові, статистичні, тестові та інші, та перевіряти їх на достовірність, використовуючи сучасні методи дослідження.

ПРН4. Здійснювати презентацію свого дослідження з правової теми, застосовуючи першоджерела та прийоми правової інтерпретації складних комплексних проблем, що постають з цього дослідження, аргументувати висновки.

ПРН6. Обґрунтовано формулювати свою правову позицію, вміти опонувати, оцінювати докази та наводити переконливі аргументи.

ПРН7. Дискутувати зі складних правових проблем, пропонувати і обґрунтовувати варіанти їх розв'язання.

ПРН8. Оцінювати достовірність інформації та надійність джерел, ефективно опрацьовувати та використовувати інформацію для проведення наукових досліджень та практичної діяльності.

ПРН9. Генерувати нові ідеї та використовувати сучасні технології у наданні правничих послуг.

ПРН10. Аналізувати взаємодію міжнародного права та міжнародно-правових систем з правовою системою України на основі усвідомлення основних сучасних правових доктрин, цінностей та принципів функціонування права.

ПРН11. Використовувати передові знання і методики у процесі правотворення та правозастосування інститутів публічного та приватного права і кримінальної юстиції.

ПРН17. Інтегрувати необхідні знання та розв'язувати складні задачі правозастосування у різних сферах професійної діяльності.

ПРН1.2. Демонструвати знання й розуміння проблематики глобалізації в контексті розвитку сучасних правових систем.

ПРН1.3. Аналізувати механізми публічно-правового і приватно-правового регулювання в юридичній практиці.

ПРН 1.4. Характеризувати особливості інноваційної діяльності та інноваційного менеджменту у правовій сфері.

3. Зміст програми навчальної дисципліни

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

Основні цілі, напрями та принципи державної політики у сфері кібербезпеки. Правові основи забезпечення кібербезпеки України. Об'єкти

кібербезпеки та кіберзахисту. Суб'єкти забезпечення кібербезпеки. Передумови та чинники кіберзагроз. Заходи забезпечення кібербезпеки.

Стратегія, законодавство, напрямки сучасної політики у сфері кібербезпеки в Україні та зарубіжних країнах. Концепція розвитку науки щодо запобігання кіберзлочинності в Україні на початку XXI століття.

Модуль 2. Поняття кіберзлочину та механізми його запобігання.

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.

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.

Зміст поняття кіберзлочинець й основні підходи до його визначення. 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. Умови формування кримінальної мотивації та мотивів. Умови реалізації мотивів і рішення про вчинення кіберзлочину.

Політика в сфері 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.

Кіберзлочинність у сфері економіки. Характеристика кіберзлочинів у сфері економіки. Особистість кіберзлочинця, основні риси. Причини та умови кіберзлочинів у сфері економіки. Запобігання кіберзлочинам у сфері економіки.

Характеристика кіберзлочинів у сфері обігу наркотичних засобів. Причини та умови кіберзлочинів у сфері обігу наркотичних засобів. Запобігання кіберзлочинам у сфері обігу наркотичних засобів.

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.

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.

4.Обсяг і структура навчальної дисципліни

№ 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.	12	2	2	8

		Тема 2. Правові основи забезпечення кібербезпеки України.	12	2	2	8
		Тема 3. Об’єкти кібербезпеки та кіберзахисту.	12	2	2	8
		Тема 4. Стан сучасної кібербезпеки в Україні та у зарубіжних країнах.	12	2	2	8
		Разом	48	8	8	32
		Модуль 2. Базові засади запобігання кіберзлочинам.				
		Тема 1. Поняття і визначення кіберзлочину. Показники кіберзлочинності.	12	2	2	8
		Тема 2. Зміст поняття кіберзлочинець й основні підходи до його визначення. Структура особистості кіберзлочинця. Детермінація кіберзлочинності.	12	2	2	8
		Тема 3. Поняття і система запобігання кіберзлочинності, класифікація запобіжних заходів.	12	2	2	8
		Разом	36	6	6	24
		Модуль 3. Теорія окремих видів кіберзлочинів та їх запобігання.				
		Тема 1. Підходи до класифікації кіберзлочинів. Характеристика	12	2	-	8

		кіберзлочинності проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему.				
		Тема 2. 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) .	12	2	2	8
		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.	12	2	2	8
		Разом	36	6	6	24
		Усього годин / кредитів ECTS	**120/4,0**	**20**	**20**	**80**

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 опитування, експрес-опитування, вирішення практичних завдань, участь у розробці кейсу, підготовка презентації, есе, реферату тощо. Поточний контроль має на меті перевірку рівня підготовки студента у вивченні 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.

Обов'язковою формою самостійної роботи студентів є підготовка індивідуальної підсумкової письмової роботи. Максимальна кількість балів за результатами захисту індивідуальної підсумкової письмової роботи – 20 балів.

Формою *підсумкового контролю* знань здобувачів вищої освіти з навчальної дисципліни є диференційований залік. Мінімальна кількість балів для отримання диференційованого заліку – 60 балів.

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

Поточний контроль				Підсумкова оцінка знань (диференційований залік)
Модуль № 1	Модуль № 2	Модуль № 3	Самостійна робота студентів	

п/з	Колоквіум	п/з	Колоквіум	п/з	Колоквіум		
max 20	max 10	max 15	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	Max 10	Результати опрацювання матеріалу високі, можлива незначна кількість несуттєвих помилок.
	5	Задовільний рівень засвоєння матеріалу, значна кількість помилок.
	Min 0	Незадовільний рівень засвоєння матеріалу.
Індивідуальна підсумкова письмова робота	Max 20	Робота оформлена відповідно до вимог кафедри. Робота не містить методологічних помилок, є посилання на джерела та власні висновки. При захисті продемонстровані глибокі знання теми, а також доведеність висновків, позицій, класифікацій тощо.
	15	Робота оформлена відповідно до вимог кафедри. Робота містить незначні методологічні помилки, є посилання на джерела, є власні висновки. При захисті продемонстровані достатні знання теми, а також доведеність висновків, позицій, класифікацій тощо.
	10	Робота оформлена відповідно до вимог кафедри, але з незначними помилками. Робота містить методологічні та змістовні помилки, є посилання на джерела, є власні висновки. При захисті продемонстровані достатні знання теми, але виникли проблеми з аргументації окремих понять та суджень у роботі, доведеність висновків.
	5	Робота оформлена з помилками та порушеннями кафедральних вимог щодо форми роботи. Робота містить методологічні та змістовні помилки, використано недостатню кількість джерел для обґрунтування дослідження та висновків. При захисті виникли труднощі щодо розкриття змісту теми, наведення аргументів стосовно окремих положень роботи та обґрунтованості і доведеності висновків.

	Min 0	Робота оформлена неналежним чином, без посилання на джерела та містить методологічні помилки. При захисті автор роботи не може продемонструвати знання з обраної теми, навести аргументацію понять та здійснити аналіз інформації. Робота виконана з порушенням вимог академічної доброчесності.
Диференційований залік	100	1. Всебічне, систематичне і глибоке знання матеріалу, передбаченого програмою навчальної дисципліни, у тому числі орієнтація в основних наукових доктринах і концепціях навчальної дисципліни. 2. Засвоєння основної та додаткової літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з навчальної дисципліни й використання отриманих знань у практичній роботі.
	90	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.
	85	1. Достатньо повне знання матеріалу, передбаченого програмою навчальної дисципліни, за відсутності у відповіді суттєвих помилок. 2. Засвоєння основної літератури, рекомендованої кафедрою. 3. Здатність до самостійного поповнення знань з дисципліни, розуміння їх значення для практичної роботи.
зараховано	75	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 й суттєві неузгодженості у відповіді на заліку за наявності знань для їх самостійного усунення або за допомогою викладача.
	70	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 заліку за наявності знань для усунення найсуттєвіших помилок за допомогою викладача.
	60	1. Прогалини в знаннях з певних частин основного матеріалу, передбаченого програмою навчальної дисципліни. 2. Наявність помилок у відповіді на питання на заліку.
не зараховано	55	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.

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

Шкала підсумкового педагогічного контролю

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

8. Навчально-методичне та інформаційне забезпечення навчальної дисципліни

Нормативно-правові акти

1. Кримінальний кодекс України: Закон України від 05. 04. 2001 р. № 2341-III із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду. Електрон. дан. (1 файл). URL : https://zakon.rada.gov.ua/laws/show/2341-14.

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

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

4. Про бюро економічної безпеки України : Закон України від 28.01.2021 URL: https://zakon.rada.gov.ua/laws/show/1150-20#Text

5. 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

6. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII. URL : http://zakon4.rada. gov.ua/laws/show/2135-12.

7. Про організаційно-правові основи боротьби з організованою злочинністю: закон України від 30 червня 1993 року № 3341-XII. URL: .

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

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

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

11. «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#Text

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

13. «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

14. «Про Стратегію кібербезпеки України»: Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року URL : https://zakon.rada.gov.ua/laws/show/447/2021#Text

Література

Основна література

1. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи / Тарасюк А. В. : монографія / А. В. Тарасюк. – Київ; Одеса : Фенікс, 2020. – 404 с.

2. 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.

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

4. 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

5. . 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

Додаткова література

1. 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)

2. 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. (Scopus).

3. Таволжанський О.В. Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів.// Журнал східноєвропейського права. – 2018. - № 56. – С. 90-105. (0,71 д.а). Таволжанський О.В. (у співавт.) International Experience of the Process of Re-Socialization of Convicts // *Журнал східноєвпроейського права.* – 2019. - № 63. – С. 125-136.

4. Віктимологія : навч. посібник/ В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська та ін. ; за ред. В.В. Голіни і Б.М. Головкіна. – Харків : Право, 2017

5. Кримінологія : підручник / Б. М. Головкін, В. В. Голіна, О. Ю. Шостко та ін.; за ред. Б. М. Головкіна. – Харків : Право, 2020

6. 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.

7. Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація / О. В. Таволжанський // Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила

Галицького. Серія : Право. - 2017. - № 4. - С. 158-164. - Режим доступу: http://nbuv.gov.ua/UJRN/Nivif_2017_4_27

8. Гладка Н. М. Боротьба з кіберзлочинністю: напрями вдосконалення кримінального законодавства України [Електронний ресурс] / Н. М. Гладка // Науковий вісник Ужгородського національного університету. Серія : Право. - 2020. - Вип. 60. - С. 139-142.

9. Леонов Б. Д. Методичне забезпечення заходів з класифікації ідентифікації та фіксації кіберзлочинів [Електронний ресурс] / Б. Д. Леонов, В. С. Серьогін // Інформація і право. - 2021. - № 1. - С. 99-105

10. Саєнко М. І. Міжнародний досвід протидії кіберзлочинності та кібершахрайству [Електронний ресурс] / М. І. Саєнко, Є. А. Савела, Ю. Ю. Тополянський // Науковий вісник Ужгородського національного університету. Серія : Право. - 2021. - Вип. 64. - С. 386-391.

Інтернет-ресурси:

1. Офіційний веб-портал Верховної Ради України / [Електронний ресурс]. - Режим доступу: http://rada.gov.ua

2. Офіційний веб-портал Офісу Генерального прокурора [Електронний ресурс]. - Режим доступу: www.gp.gov.ua/

3. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. [Електронний ресурс]. - Режим доступу: https://cip.gov.ua/

4. Офіційний веб-сайт Міністерства внутрішніх справ України [Електронний ресурс]. - Режим доступу: http://www.mvs.gov.ua/ua/

5. Єдиний державний реєстр судових рішень [Електронний ресурс]. - Режим доступу: http://www.reyestr.court.gov.ua/

СЕНМК

Стандартизований електронний навчально-методичний комплекс кафедри кримінології та кримінально-виконавчого права. URL: http://library.nlu.edu.ua/index.php?option=com_k2&view=itemlist&task=category&id=199:kafedra-kriminologii-ta-kriminalno-vikonavchogo-prava&Itemid=151