ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра права та публічного управління

ЗАТВЕРДЖУЮ
Проректор з методичної роботи
_____ Ярослав ШТАНЬКО
“20” _____ 2024 р.

КРИМІНАЛЬНЕ ПРАВО В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	08 Право
Спеціальність:	081 Право
Освітньо-професійна (освітньо-наукова) програма:	«Право»
Освітній рівень:	перший (бакалаврський)
Статус дисципліни:	вибіркова
Мова викладання, навчання та оцінювання:	українська

Івано-Франківськ
2024

РОЗРОБНИК:
д.ю.н., професор, професор
кафедри права та
публічного управління Микола КАРЧЕВСЬКИЙ

ЗАТВЕРДЖЕНО:

на засіданні кафедри права та
публічного управління
протокол № 4 від 21.11.2024 р.
в.о. завідувача кафедри Олександра ПТАШНИК

УЗГОДЖЕНО:

Гарант ОП Євген ПИСЬМЕНСЬКИЙ

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 4 від 29.11.2024 р.

e-mail	mykola.karchevskyi@ukd.edu.ua
Номер аудиторії чи кафедри	Кафедра права та публічного управління
Посилання на сайт	Микола Карчевський
Сторінка курсу в СДО	Кримінальне право в умовах цифрової трансформації

ВСТУП

Анотація навчальної дисципліни «Кримінальне право в умовах цифрової трансформації»

Курс про те як засобами кримінально-правового регулювання забезпечується мінімізація негативних наслідків інформатизації, а також про можливості сучасних технологій розв'язувати одвічні проблеми кримінального права та створювати нові. Почнемо з дослідження «інформаційного вибуху», його причин та значення для розвитку технологій. Поміркуємо над тим, що таке «комп'ютерні» злочини та чому слід критично сприймати оцінки їх поширеності та заподіяної шкоди. Розглянемо ознаки складів кримінальних правопорушень в сфері використання інформаційних технологій (ст.ст. 361 – 363-1 КК України). Будемо досліджувати як під впливом розвитку комп'ютерів змінився найбільший сегмент злочинності – посягання на власність. Не залишимо поза увагою мейнстрім юридичного дискурсу: блокчейн, віртуальні активи та штучний інтелект. Нарешті проаналізуємо як діджиталізація може допомогти з кризою кримінального права.

Мета курсу – засвоєння студентами засад забезпечення мінімізації негативних наслідків інформатизації засобами кримінального права, а також можливостей сучасних технологій як засобів раціоналізації правового регулювання.

Основні завдання вивчення дисципліни:

- засвоєння положень чинного кримінального законодавства та інших джерел кримінального права, які використовуються в процесі здійснення кримінально-правової кваліфікації злочинів в сфері використання комп'ютерної техніки;
- набуття навичок правильного, точного та всебічного кримінально–правового аналізу суспільно небезпечних діянь в сфері використання комп'ютерної техніки, і застосування КК України поряд з іншими джерелами кримінального права та актами тлумачення при здійсненні кримінально-правової кваліфікації таких діянь;
- отримання знань, щодо перспектив розвитку кримінального права в сфері використання інформаційних технологій та можливостей використання цих технологій для раціоналізації правового регулювання.

У результаті вивчення дисципліни студент повинен **знати**:

· форми, причини, та прояви соціальних трансформацій, які відбуваються внаслідок інформатизації суспільства;

· ознаки складів кримінальних правопорушень, передбачених розділом XVI Особливої частини КК та злочинів проти власності, що вчиняються з використанням інформаційних технологій;

· засади правового регулювання віртуальних активів в Україні, тенденції злочинного використання віртуальних активів в Україні та світі, основні проблеми використання кримінального законодавства в цій сфері;

· засади правового регулювання штучного інтелекту, практичні кейси використання систем ШІ для протидії злочинності;

· основи роботи з великими даними щодо протидії злочинності, можливості оцінки ефективності кримінальної юстиції та розробки data-driven hsitym.

У результаті вивчення дисципліни студент повинен **вміти**:

· правильно кваліфікувати кримінальні правопорушення в сфері використання інформаційних технологій та злочини проти власності, що вчиняються з використанням інформаційних технологій;

· встановлювати та формулювати ознаки кримінально-протиправного використання віртуальних активів;

· визначати межі використання технологій ШІ в сфері протидії злочинності;

· аналізувати відкриті дані щодо протидії злочинності в Україні з використанням інформаційних технологій, розробляти пропозиції data-driven рішень в сфері кримінальної юстиції.

Професійні компетентності та результати навчання, яких набувають здобувачі освіти внаслідок вивчення навчальної дисципліни «Кримінальне право в умовах цифрової трансформації» (шифри та зміст компетентностей та програмних результатів навчання вказано відповідно до ОП «Право», введеної в дію ЗВО «Університет Короля Данила» “01”вересня 2024 року.

Шифр та назва компетентності	**Шифр та назва програмних результатів навчання**
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу	ПРН 3. Проводити збір і інтегрований аналіз матеріалів з різних джерел.
ЗК2. Здатність застосовувати знання у практичних ситуаціях.	ПРН 5. Давати короткий правовий висновок щодо окремих фактичних обставин з достатньою обґрунтованістю.
СК7. Здатність застосовувати норми та інститути права, щонайменше з таких галузей, як: конституційне право, адміністративне право і адміністративне процесуальне право, цивільне і цивільне процесуальне право, трудове право, кримінальне і кримінальне процесуальне право.	ПРН 2. Знати та розуміти міжнародні стандарти прав людини, положення Конвенції про захист прав людини та основоположних свобод, а також практику Європейського суду з прав людини. ПРН 19. Пояснювати природу та зміст основних правових явищ і процесів.
СК8. Здатність застосовувати правові принципи та доктрини	ПРН 18. Застосовувати в професійній діяльності основні сучасні правові доктрини, цінності та принципи функціонування національної правової системи.
СК9. Здатність використовувати бази даних органів юстиції та інформаційні технології необхідні під час здійснення юридичної діяльності.	ПРН 14. Використовувати статистичну інформацію, отриману з першоджерел та вторинних джерел для правничої діяльності. ПРН 15. Вільно використовувати для правничої діяльності доступні інформаційні технології і бази даних.

	ПРН 16. Використовувати комп'ютерні програми, необхідні у правничій діяльності.
СК11. Здатність визначати належні та прийнятні для юридичного аналізу факти.	ПРН 20. Виокремлювати і аналізувати юридично значущі факти і робити обґрунтовані правові висновки.
СК12. Здатність аналізувати правові проблеми та обґрунтовувати правові позиції.	ПРН 6. Оцінювати недоліки і переваги певних правових аргументів, аналізуючи відому проблему.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**4**		
Семестр	**8**		
Кількість кредитів ЄКТС	**3**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	**14 (в годинах)**	**4 (в годинах)**
	семінари, практичні	**16 (в годинах)**	**4 (в годинах)**
Самостійна робота		**60 (в годинах)**	**82 (в годинах)**
Форма підсумкового контролю	**залік 2 (в годинах)**		

Структурно-логічна схема вивчення навчальної дисципліни[1]:

Пререквізити	Постреквізити
Потребує володіння базовими знаннями з кримінального права.	

[1] тільки для обов'язкових дисциплін

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Як інформатизація змінює світ.

Вплив інформатизації на сучасне суспільство, економіку, культуру та кримінально-правове регулювання. Роль інформаційних технологій у трансформації суспільних відносин, формуванні інформаційного суспільства та впливі на безпеку. Технологічний детермінізм, рефлексивна модернізація, інформаційна економіка та культура. Основні виклики кримінально-правого регулювання у контексті цифрової трансформації. Синхронізація кримінально-правового регулювання та технологій інформатизації.

Самостійна робота: дослідження наукових статей з використанням ChatGPT, підготовка до діалогу щодо позитивних та негативних наслідків інформатизації.

Тема 2. «Комп'ютерні» злочини: чому в лапках?

Загальна характеристика кримінальних правопорушень в сфері використання електронно-обчислювальних машин, систем, комп'ютерних мереж та мереж електрозв'язку (ст.ст. 361 – 363-1 КК України).

Інформаційні відносини як родовий об'єкт кримінальних правопорушень. Комп'ютерна інформація як предмет кримінальних правопорушень. Право власності на комп'ютерну інформацію як об'єкт кримінальних правопорушень.

Несанкціоноване втручання в роботу комп'ютеризованих засобів обробки інформації. Втрата, виток, підробка, блокування комп'ютерної інформації, порушення порядку маршрутизації, спотворення процесу обробки інформації.

Створення, розповсюдження, збут шкідливих програмних або технічних засобів.

Незаконні дії з комп'ютерною інформацією з обмеженим доступом.

Незаконне копіювання, зміна або знищення комп'ютерної інформації особами, які мають право доступу до комп'ютерної інформації.

Кримінально каране порушення правил експлуатації комп'ютерної техніки, порядку або правил захисту інформації.

Відповідальність за масове розповсюдження повідомлень електрозв'язку.

Самостійна робота: розв'язання задач щодо кримінально-правової кваліфікації кримінальних правопорушень в сфері використання інформаційних технологій.

Тема 3. Злочини проти власності, які вчиняються з використанням інформаційних технологій.

Співвідношення понять «чуже майно», «право на майно», «безготівкові гроші», «електронні гроші», «віртуальні активи». Дослідження судової практики в сфері кримінально-правової протидії несанкціонованим транзакціям.

Особливості об'єкта, предмета та об'єктивної сторони шахрайства, яке полягає у ініціації несанкціонованих транзакцій.

Трансформація традиційного шахрайства під впливом розвитку інформаційних технологій.

Самостійна робота: критичний аналіз судових рішень, пов'язаних з кримінально-правовою кваліфікацією несанкціонованих транзакцій у платіжних системах.

Тема 4. Bitcoin та BlockChain: що це таке та як працює?

Відмежування безготівкових грошей та віртуальних активів за природою, адмініструванням, порядком емісії та визначенням вартості.

Світові тенденції злочинного використання віртуальних активів. Несанкціоновані транзакції та шахрайство. Незаконний збут у тіньовому інтернеті, обіг наркотиків та засобів шахрайства. Шкідливе програмне забезпечення для вимагання. Легалізація коштів, здобутих злочинним шляхом, з використанням віртуальних активів.

Україна в контексті світових тенденцій «криптозлочинності». Розвиток та проблеми правового регулювання віртуальних активів в Україні.

Фізична ознака віртуальних активів. Розподілене (децентралізоване) зберігання даних щодо транзакцій. Блокчейн.

Економічна ознака віртуальних активів. Визначення вартості віртуальних активів. Отримання інформації з використанням обліків бірж віртуальних активів.

Юридична ознака віртуальних активів. Власність на віртуальні активи. Вилучення віртуальних активів, зберігання вилучених віртуальних активів.

Самостійна робота: дослідження реєстру транзакцій віртуальних активів, здійснення транзакцій з використанням тестових активів, вилучання тестових активів з використанням приватного ключа, вилучення віртуальних активів шляхом відновлення доступу до електронного гаманця за мнемонічною фразою.

Тема 5. Штучний інтелект та протидія злочинності.

Основи юридичного дискурсу щодо штучного інтелекту. Заборона чи регулювання. Суб'єктність та емерджентність. Технологічна сингулярність

Ключові компоненти систем штучного інтелекту: дані, програмне забезпечення для реалізації моделей, інтерфейси, менеджмент.

Загальний та вузькі ШІ. «Класичні» небезпеки використання систем ШІ. Порушення приватності в процесі використання ШІ. Алгоритмічна упередженість. Небезпека маніпуляцій поведінкою. Проблема «Black Box» та пояснюваний ШІ.

Можливості та небезпеки ШІ у сфері кримінальної юстиції.

Усвідомлення та реалізація потреби правового регулювання використання технологій ШІ. Класифікація сфер та ризиків використання відповідно до EU Artificial Intelligence Act.

Самостійна робота: дослідження наявних систем ШІ, які використовують правоохоронні та судові органи, з використання доступних відкритих даних та з використанням ШІ чат-ботів, порівняння отриманих результатів.

Тема 6. Криза кримінального права та інформаційні технології.

Ефективне кримінально-правове регулювання та криза кримінального права. Відкриті дані щодо протидії злочинності в Україні. Обчислювальне кримінологічне аргументування.

Тенденції протидії злочинності в Україні, встановлені на основі аналізу відкритих даних офіційної статистики. Примітивізація та пріоритизація. Проблемні аспекти збирання та обліку даних щодо протидії злочинності. Адвокація відкритих даних. Обмеженість кількісних та суб'єктивність якісних методів дослідження злочинності.

Проєкти аналізу даних в сфері кримінальної юстиції.

Самостійна робота: створення дашбордів, 3d візуалізацій, картограм на основі наданих викладачем наборів даних, аналіз тенденцій протидії злочинності з використанням онлайн платформи CrimeDataLab.

Тема 7. Ландшафт цифрової трансформації права

Комплексний підхід до впливу цифрових технологій на право та правову систему. Фокусування на оглядовому дослідженні інформаційних юридичних інновацій, які не було окремо розглянуто в межах курсу.

Електронне правосуддя, аналіз використання цифрових платформ для судових процесів, від подання позовів до винесення рішень, та пов'язані виклики, зокрема безпека даних та прозорість.

Регулювання цифрових платформ, правові аспекти діяльності платформ для обміну інформацією, цифрових ринків та соціальних мереж.

Автоматизація юридичних послуг, етичні, правові та соціальні виклики, пов'язані з автоматизованими юридичними консультаціями та іншими AI-рішеннями.

Цифрові права людини, адаптація правових норм до цифрового середовища, зокрема права на цифрову приватність, доступ до інформації та боротьбу з дезінформацією.

Електронне регулювання, як цифрові інструменти змінюють процеси нормотворчості та правозастосування.

Самостійна робота: підготовка та презентація коротких повідомлень про окремі аспекти цифрової трансформації кримінально-правового регулювання.

Зміст самостійної роботи здобувачів

Розподіл годин, виділених на вивчення дисципліни:

Найменування видів робіт	Розподіл годин за формами навчання	
	денна	заочна
Самостійна робота, год, у т.ч.:	60	84
Опрацювання матеріалу, викладеного на лекціях	-	-
Підготовка до практичних занять та контрольних заходів	20	20
Підготовка звітів з практичних робіт	20	20
Підготовка до поточного контролю	4	4
Опрацювання матеріалу, винесеного на самостійне вивчення	16	40

Підсумковий проєкт. Capstone project

Підсумковий контроль відбувається у формі підготовки та презентації аналітичного звіту щодо обвинувального вироку, пов’язаного з кримінально-правовою оцінкою діяння як кримінального правопорушення в сфері використання інформаційних технологій (ст.ст. 361 – 363-1 КК).

1. За допомогою Єдиного державного реєстру судових рішень необхідно обрати такий обвинувальний вирок, зробити висновок щодо правильності кримінально-правової кваліфікації та заповнити таблицю.

2. З використанням штучного інтелекту здійснити пошук наукової інформації, яка має відношення до проблеми кримінальної відповідальності за кримінальне правопорушення, з яким пов'язано обраний вирок. Здійснити аналіз цих джерел.

3. Використовуючи відкрити дані щодо протидії злочинності в Україні запропонувати візуалізації основних трендів протидії правопорушенням, подібним до тих, з яким пов'язано обране судове рішення

4. Представити отримані дані в презентації розміром до 5 слайдів

5. Представити результати свого Capstone Project та завантажити як відповідь презентацію у форматі *.PDF

Форма індивідуального аналітичного звіту.

Аналітичний звіт за результатами вивчення курсу «Кримінальне право в умовах цифрової трансформації»

Ім’я та прізвище розробника аналітичного звіту			
1.	**Джерело повідомлення** (для вироку суду – номер, дата, суд; для статті зі ЗМІ – назва видання, номер, рік видання, сторінка; для іншого видання – назва видання, видавництво, рік, сторінка; для відомостей з Інтернету – адреса інформаційного ресурсу до html файлу з вказівкою дати отримання інформації)		
2.	**Час вчинення кримінального правопорушення**		
3.	**Місце вчинення кримінального правопорушення**		
4.	**Кваліфікація відповідно до КК України** (якщо кримінальне правопорушення вчинене в співучасті – надати кваліфікацію кожного з співучасників та охарактеризувати юридичний та фактичні склади для кожного окремо; якщо має місце множинність - елементи юридичного та фактичного складів охарактеризувати окремо для кожного правопорушення)		
Аналіз фактичного та юридичного складів			
5.	**Елемент складу кримінального правопорушення**	**Юридичний склад**	**Фактичний склад**
6.	**Об’єкт**		
7.	**Предмет** (ознаки предмету)		

8.	**Об’єктивна сторона** (обов’язкові ознаки)		
9.	**Об’єктивна сторона** (факультативні ознаки)		
10.	**Суб’єкт**		
11.	**Суб’єктивна сторона** (характеристика інтелектуального та вольового моментів вини)		
12.	**Суб’єктивна сторона** (факультативні ознаки)		
13.	**Кваліфікуючі ознаки**		
Додаткові кримінально-правові характеристики вчиненого діяння			
14.	**Множинність** (якщо наявна - вказати вид)		
15.	**Стадії** (якщо кримінальне правопорушення не доведено до кінця вказати вид стадії, якщо доведено - обґрунтувати свій висновок)		
16.	**Співучасть** (якщо наявна – вказати види співучасників та форму співучасті)		
17.	**Відмежування від суміжних складів**		
Кримінально-правові наслідки			
18.	**Застосоване покарання (основне, додаткове), використання звільнення від покарання**		
19	**Інші кримінально-правові наслідки**		
Додаткові інструменти аналізу			
18.	**Висновок щодо використання ШІ для дослідження судового рішення**		
19.	**Встановлені з використанням інтерактивного довідника «Протидія злочинності в Україні: інфографіка» тенденції протидії аналогічним кримінальним правопорушенням**		
	Висновок розробника звіту		

ПОЛІТИКА КУРСУ

Коротко, з покликанням на відповідну нормативну базу УКД, висвітлити питання:[2]

[2] зміст пунктів може редагуватись з огляду на особливості курсу

1) щодо системи поточного і підсумкового контролю

Організація поточного та підсумкового семестрового контролю знань студентів, проведення практик та атестації, переведення показників академічної успішності за 100-бальною шкалою в систему оцінок за національною шкалою здійснюється згідно з «Положенням про систему поточного і підсумкового контролю, оцінювання знань та визначення рейтингу здобувачів освіти». Ознайомитись з документом можна за покликанням.

2) щодо оскарження результатів контрольних заходів

Здобувачі вищої освіти мають право на оскарження оцінки з дисципліни отриманої під час контрольних заходів. Апеляція здійснюється відповідно до «Положення про політику та врегулювання конфліктних ситуацій». Ознайомитись з документом можна за покликанням.

3) щодо відпрацювання пропущених занять

Згідно «Положення про організацію освітнього процесу» здобувач допускається до семестрового контролю з конкретної навчальної дисципліни (семестрового екзамену, диференційованого заліку), якщо він виконав усі види робіт, передбачені на семестр навчальним планом та силабусом/робочою програмою навчальної дисципліни, підтвердив опанування на мінімальному рівні результатів навчання (отримав ≥35 бали), відпрацював визначені індивідуальним навчальним планом всі лекційні, практичні, семінарські та лабораторні заняття, на яких він був відсутній. Ознайомитись з документом можна за покликанням.

4) щодо дотримання академічної доброчесності

«Положення про академічну доброчесність» закріплює моральні принципи, норми та правила етичної поведінки, позитивного, сприятливого, доброчесного освітнього і наукового середовища, професійної діяльності та професійного спілкування спільноти Університету, викладання та провадження наукової (творчої) діяльності з метою забезпечення довіри до результатів навчання. Ознайомитись з документом можна за покликанням.

5) щодо використання штучного інтелекту

«Положення про академічну доброчесність» визначає політику щодо використання технічних засобів на основі штучного інтелекту в освітньому процесі. Ознайомитись з документом можна за покликанням.[3] *«Положення про систему запобігання та виявлення академічного плагіату, самоплагіату, фабрикації та фальсифікації академічних творів» містить рекомендації щодо використання в академічних текстах генераторів на основі штучного інтелекту. Ознайомитись з документом можна за покликанням.*

6) щодо використання технічних засобів в аудиторії та правила комунікації

Використання мобільних телефонів, планшетів та інших гаджетів під час лекційних та практичних занять дозволяється виключно у навчальних цілях (для уточнення певних даних, перевірки правопису, отримання довідкової інформації тощо). На гаджетах повинен бути активований режим «без звуку» до початку заняття. Під час занять заборонено надсилання текстових повідомлень, прослуховування музики, перевірка електронної пошти, соціальних мереж тощо, окрім виробничої необхідності. Під час виконання заходів контролю використання гаджетів заборонено (за винятком, коли це передбачено умовами його проведення). У разі порушення цієї заборони результат анульовується без права перескладання.
Комунікація відбувається через електронну пошту і сторінку дисципліни в Moodle.

7) щодо зарахування результатів навчання, здобутих шляхом формальної/інформальної освіти

Процедури визнання результатів навчання, здобутих шляхом формальної/інформальної освіти визначаються «Положенням про порядок визнання результатів навчання, здобутих шляхом неформальної та / або інформальної освіти». Ознайомитись з документом можна за покликанням.[4]

Під час вивчення навчальної дисципліни «» студентам надається можливість перерахування неформальної освіти. До прикладу, із запропонованого переліку можна пройти сертифіковані (безкоштовні) курси на освітніх платформах, відтак сертифікат, який отримали під час навчання, – є підтвердженням засвоєння студентом окремих тем, що включені у зміст дисципліни.

№ п/п	Перелік сертифікованих (безкоштовних) онлайн-курсів	Перелік тем, які можуть бути перераховані (за умови наявності сертифіката на ім'я та прізвище студента/студентки)
1.		

[3] визначається політика використання ШІ в навчальній дисципліні - дозволене/заборонене, правила використання
[4] визначається перелік електронних та інших ресурсів та умови перезарахування

2.		

МЕТОДИ НАВЧАННЯ

При вивченні дисципліни застосовується комплекс методів для організації навчання студентів з метою розвитку їх логічного та абстрактного мислення, творчих здібностей, підвищення мотивації до навчання та формування особистості майбутнього фахівця.

Програмний результат навчання[5]	**Метод навчання**	**Метод оцінювання**
ПРН 2. Знати та розуміти міжнародні стандарти прав людини, положення Конвенції про захист прав людини та основоположних свобод, а також практику Європейського суду з прав людини.	словесні наочні практичні	усний контроль програмований контроль поточний контроль
ПРН 5. Давати короткий правовий висновок щодо окремих фактичних обставин з достатньою обґрунтованістю.	словесні наочні практичні	усний контроль програмований контроль поточний контроль
ПРН 6. Оцінювати недоліки і переваги певних правових аргументів, аналізуючи відому проблему.	словесні наочні практичні	усний контроль програмований контроль поточний контроль
ПРН 18. Застосовувати в професійній діяльності основні сучасні правові доктрини, цінності та принципи функціонування національної правової системи.	словесні наочні практичні	усний контроль програмований контроль поточний контроль
ПРН 19. Пояснювати природу та зміст основних правових явищ і процесів.	словесні наочні практичні	усний контроль програмований контроль поточний контроль

[5] для вибіркових навчальних дисциплін вказується результат навчання

ПРН 20. Виокремлювати і аналізувати юридично значущі факти і робити обґрунтовані правові висновки.	словесні наочні практичні	усний контроль програмований контроль поточний контроль

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Вид	**Зміст**	**% від загальної оцінки**	**Бал**	
			min	**max**
Поточні контрольні заходи	всього	60	35	60
Підсумкові контрольні заходи	залік	40	24	40
Всього:	-	100	60	100

Процедура проведення контрольних заходів, а саме поточного контролю знань протягом семестру та підсумкового семестрового контролю, регулюється «Положенням про систему поточного та підсумкового контролю оцінювання знань та визначення рейтингу студентів».

Фіксація **поточного** контролю здійснюється в «Електронному журналі обліку успішності академічної групи» на підставі чотирибальної шкали – «2»; «3»; «4»; «5». У разі відсутності студента на занятті виставляється “н”. За результатами поточного контролю у Журналі, автоматично визначається підсумкова оцінка, здійснюється підрахунок пропущених занять.

Критерії оцінювання:

«незадовільно»	володіє навчальним матеріалом на рівні елементарного розпізнавання і відтворення окремих фактів, елементів, об'єктів, що позначаються окремими словами чи реченнями; володіє матеріалом на елементарному рівні засвоєння, викладає його уривчастими реченнями, виявляє здатність висловити думку на елементарному рівні; володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу;
«задовільно»	володіє матеріалом на початковому рівні, значну частину матеріалу відтворює на репродуктивному рівні; володіє матеріалом на рівні, вищому за початковий, здатний за допомогою викладача логічно відтворити значну його частину; може відтворити значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, за допомогою викладача може аналізувати навчальний матеріал, порівнювати та робити висновки, виправляти допущені помилки;
«добре»	здатний застосовувати вивчений матеріал на рівні стандартних ситуацій, частково контролювати власні навчальні дії, наводити окремі власні приклади на підтвердження певних тверджень: вміє порівнювати, узагальнювати, систематизувати інформацію під керівництвом викладача, в цілому самостійно застосовувати її на практиці, контролювати власну діяльність, виправляти помилки і добирати аргументи на підтвердження певних думок під керівництвом викладача; вільно володіє вивченим обсягом матеріалу, та вміє застосовувати його на практиці; вільно розв'язує задачі в стандартних ситуаціях, самостійно виправляє допущені помилки, добирає переконливі аргументи на підтвердження вивченого матеріалу;
«відмінно»	виявляє початкові творчі здібності, самостійно визначає окремі цілі власної навчальної діяльності, оцінює окремі нові факти, явища, ідеї; знаходить джерела інформації та самостійно використовує їх відповідно до цілей, поставлених викладачем; вільно висловлює власні думки і відчуття, визначає програму особистої пізнавальної діяльності, самостійно оцінює різноманітні життєві явища і факти, виявляючи особисту позицію щодо них; без допомоги викладача знаходить джерела інформації і використовує одержані відомості відповідно до мети та завдань власної пізнавальної діяльності; використовує набуті знання і вміння в нестандартних ситуаціях; виявляє особливі творчі

	здібності, самостійно розвиває власні обдарування і нахили, вміє самостійно здобувати знання.

Усі пропущені заняття, а також негативні оцінки студенти зобов'язані відпрацювати впродовж трьох наступних тижнів. У випадку недотримання цієї норми, замість “н” в журналі буде виставлено “0” (нуль балів), без права перездачі. Відпрацьоване лекційне заняття в електронному журналі позначається літерою «в».[6]

Підсумковий контроль здійснюється у виді заліку. На залік необхідно підготувати презентацію на одну із запропонованих тем (див. с. 8) та здійснити її прилюдний захист.

До підсумкового контролю допускаються студенти які за результатами поточного контролю отримали не менше 35 балів. Усі студенти, що отримали 34 балів і менше, не допускаються до складання підсумкового контролю і на підставі укладання додаткового договору, здійснюють повторне вивчення дисципліни впродовж наступного навчального семестру. За результатами підсумкового контролю (екзамен) студент може отримати 40 балів. Студенти, які під час підсумкового контролю отримали 24 бали і менше, вважаються такими, що не здали екзамен/диференційований залік і повинні йти на перездачу.

Загальна семестрова оцінка з дисципліни, яка виставляється в екзаменаційних відомостях оцінюється в балах (згідно з **Шкалою оцінювання знань за ЄКТС**) і є сумою балів отриманих під час поточного та підсумкового контролю.

Шкала оцінювання знань за ЄКТС:

Оцінка за національною шкалою	**Рівень досягнень, %**	**Шкала ECTS**
Національна диференційована шкала		
Відмінно	90 – 100	A
Добре	83 – 89	B

[6] можна вказати теми чи завдання, які є обов’язковими до виконання, а також особисті підходи до оцінювання рівня знань здобувачів під час аудиторної роботи

	75 – 82	C
Задовільно	67 – 74	D
	60 – 66	E
Незадовільно	35 – 59	FX
	0 – 34	F
Національна недиференційована шкала		
Зараховано	60 – 100	-
Не зараховано	0 – 59	-

Студенти, які не з’явилися на залік без поважних причин, вважаються такими, що одержали незадовільну оцінку.

РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

1. Anderson, Ross, et al. "Measuring the cost of cybercrime." The economics of information security and privacy (2013): 265-300.
2. Brenner, Susan W. Cybercrime: criminal threats from cyberspace. Bloomsbury Publishing USA, 2010.
3. Dupont B., Stevens Y., Westermann H., Joyce M. Artificial Intelligence in the Context of Crime and Criminal Justice , Korean Institute of Criminology, Canada Research Chair in Cybersecurity, ICCC, Université de Montréal, (2018). URL : https://www.cicc-iccc.org/public/media/files/prod/publication_files/Artificial-Intelligence-in-the-Context-of-Crime-and-Criminal-Justice_KICICCC_2019.pdf
4. Karchevskyi, M., Losych, S., & Germanov, S. (2023). Socialization of artificial intelligence and transhumanism: legal and economic aspects. Baltic Journal of Economic Studies, 9(1), 61-70. https://doi.org/10.30525/2256-0742/2023-9-1-61-70
5. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) / Д.С. Азаров. – К. : Атіка, 2007. – 304 с.
6. Горбулін В.П. Проблеми захисту інформаційного простору України : монографія / В.П. Горбулін, М.М. Биченок; Інститут проблем національної безпеки. – К. : Інтертехнологія. – 2009. – 136 с.
7. Карчевський М. В. BlockChain та Bitcoin що це таке та «як працює»? Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка. 2018. № 4(84), С. 108-117. https://doi.org/10.33766/2524-0323.84.108-117
8. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с. https://karchevskiy.files.wordpress.com/2020/04/karchevskiy-m.pdf
9. Карчевський М.В. Злочини у сфері використання інформаційних технологій. [Електронний ресурс]: навч. посіб. / М.В. Карчевський. – 2020, Сєвєродонецьк: РВВ ЛДУВС. – Режим доступу: https://karchevskiy.org/cybercrimes/
10. Карчевський, М (2023) Протидія злочинності в Україні : інфорграфіка : інтерактивний довідник. Версія 3.0. URL : https://ioyfgl-nikolay-karchevskiy.shinyapps.io/ukraine3_0/
11. Міхайліна Т.В. Кримінальна відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут : автореф. дис. … кандидата юрид. наук : 12.00.08 / Тетяна Вікторівна Михайліна. – К., 2011. – 20 с.

12. Орлов С.О. Кримінально-правова охорона інформації в комп'ютерних системах та телекомунікаційних мережах : дис. ... кандидата юрид. наук: 12.00.08 / С.О. Орлов. – Х., 2004. – 213 с.
13. Плугатир М.В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації : автореф. дис. ... кандидата юрид. наук: 12.00.08 / Плугатир Максим Віталійович. – К., 2010. – 18 с.
14. Протидія злочинам у сфері використання інформаційних технологій : інтегр. навч.-практ. посіб. / М. В. Карчевський, В. В. Коваленко, В. Є. Комлєв та ін.; за ред. М. В. Карчевського. Харків : Право, 2019. 188 с.
15. Рудик М.В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : дис. ... кандидата юрид. наук: 12.00.08 / Михайло Вікторович Рудик. – Х., 2007. – 229 с.
16. Савінова Н.А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія / Н.А. Савінова. – К. 2012. – 340 с.
17. Тихомиров О.О. Забезпечення інформаційної безпеки як функція держави : автореф. дис. ... кандидата юрид. наук : 12.00.01 / Тихомиров О. О. – К., 2011. – 19 с.

Перелік додаткової літератури, яку необхідно опрацювати до кожного практичного заняття, у разі потреби, буде подаватися щонайменше за тиждень до дати проведення заняття.

Інтернет-ресурси для додаткового навчання:

1. FBI's Internet Crime Complaint Center (IC3): The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). It serves as a reporting mechanism for victims of cybercrime and provides valuable information about various types of cyber threats.– URL: https://www.ic3.gov/
2. Europol's European Cybercrime Centre (EC3): EC3 is the European Union's law enforcement agency that focuses on combating cybercrime. It provides reports, threat assessments, and resources related to cybercrime in Europe. – URL: https://www.europol.europa.eu/ec3
3. Future of Life Institute (FLI). – URL: https://futureoflife.org/
4. The AI Act. Site, dedicated to European discussion on artificial intelligence regulation. – URL: https://artificialintelligenceact.eu/the-act/
5. Threatpost. Threatpost is a cybersecurity news website that offers articles, analysis, and insights into the latest cyber threats and attacks, including those related to cybercrime. – URL: https://threatpost.com/
6. SANS Institute: SANS provides a wealth of cybersecurity resources,

including whitepapers, webcasts, and training courses. – URL: https://www.sans.org/emea/
7. Dark Reading: Dark Reading is a cybersecurity news and information website that covers a variety of topics, including cybercrime, threat intelligence, and security best practices. – URL: https://www.darkreading.com/
8. The Hacker News: This is a popular online platform that covers a wide range of cybersecurity topics, including cybercrime news, data breaches, vulnerabilities, and hacking incidents. – URL: https://thehackernews.com/
9. KrebsOnSecurity: Brian Krebs is a well-known investigative journalist who covers cybersecurity and cybercrime. His blog, KrebsOnSecurity, provides in-depth analysis of various cyber incidents, security trends, and news related to cybercrime. – URL: https://krebsonsecurity.com/
10. The Register of Known Spam Operations (ROKSO) database. The Spamhaus Project. – URL: http://www.spamhaus.org/statistics/spammers.lasso.