КЛАСИЧНИЙ ПРИВАТНИЙ УНІВЕРСИТЕТ

Кафедра кримінального права, процесу та криміналістики

СИЛАБУС

навчальної дисципліни

ПП 5. Інноваційні технології у сучасній правоохоронній діяльності

2026 - 2027 навчальний рік

Викладач	Калюга Каріна Вікторівна, завідувач кафедри кримінального права, процесу та криміналістики, доктор юридичних наук, професор
Контактний телефон	+380676255963
Ідентифікатор та код доступу (Zoom / Google Meet)	556-226-5378, код доступу L7vMD3
E-mail:	kalugaalim@gmail.com
Сторінка курсу на сайті підтримки навчальних програм КПУ	http://www.zhu.edu.ua/cpu_edu/course/view.php?id=3645
Консультації	Консультації проводяться в дистанційному режимі за попереднім погодженням із викладачем через месенджери або електронну пошту

ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ

Рівень вищої освіти	Другий (магістерський)	
Галузь знань	К Безпека та оборона	
Спеціальність	К9 Правоохоронна діяльність	
Освітня програма	Правоохоронна діяльність	
Форма навчання	Очна (денна), заочна	
Мова викладання	Українська	
Курс (рік навчання), семестр	Курс 1, семестр 2	
Цикл підготовки	Професійної підготовки	
Статус дисципліни	Обов’язкова	
Обсяг дисципліни	Кількість кредитів ECTS	3
	Загальна кількість годин	90
	Аудиторних годин	34
	Лекції	18
	Практичні	16
	Самостійна робота	56
Форма контролю	Екзамен	
Попередні компоненти (Пререквізити)	Теоретико-правові засади правоохоронної діяльності в Україні, Сучасні доктринальні та концептуальні проблеми розвитку держави і права	
Паралельні та подальші компоненти (Постреквізити)	Методика наукових досліджень, Практична підготовка в правоохоронних органах, Підготовка та захист кваліфікаційної роботи	

МЕТА, ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни

Навчити обирати, застосовувати й оцінювати інноваційні технології у правоохоронній діяльності. Сформувати вміння обґрунтовувати їх упровадження з урахуванням потреб підрозділу, наявних ресурсів, вимог безпеки, захисту даних і прав людини.

Завдання навчальної дисципліни:

- розкрити можливості та обмеження технологічних і організаційних інновацій у правоохоронній діяльності;
- навчити визначати потреби підрозділу та порівнювати варіанти рішень за допомогою системного аналізу й імітаційного моделювання;
- навчити обґрунтовувати вибір технічних приладів, спеціальних засобів, інформаційних систем і програмного забезпечення для професійних завдань;
- розвинути практичні навички роботи з відкритими цифровими джерелами, базами даних, інструментами кримінального та геопросторового аналізу;
- навчити перевіряти результати автоматизованого аналізу, зокрема отримані за допомогою штучного інтелекту;
- ознайомити із засадами захищеного зв’язку, міжвідомчого інформаційного обміну, захисту даних і кібербезпеки;
- навчити готувати проєкт упровадження інновації, планувати його апробацію та оцінювати результативність.

У результаті вивчення дисципліни здобувачі вищої освіти повинні знати:

- види інновацій у правоохоронній діяльності та етапи їх обґрунтування, апробації й упровадження;
- методи системного аналізу та принципи побудови простих імітаційних моделей правоохоронних процесів;
- призначення, можливості та обмеження сучасних технічних приладів і спеціальних засобів забезпечення публічної безпеки;
- принципи роботи інформаційно-пошукових систем, баз даних і спеціалізованого програмного забезпечення;
- можливості технологій аналізу відкритих джерел, цифрової криміналістики та геоінформаційних систем;
- ризики помилок, упередженості та неправомірного використання результатів штучного інтелекту;
- призначення державної системи урядового зв’язку й Національної системи конфіденційного зв’язку, загальні засади захищеного інформаційного обміну;
- вимоги до захисту інформації, правомірності оброблення даних та дотримання прав людини;
- способи визначення ресурсів, строків, виконавців і показників результативності інноваційного проєкту.

Після вивчення дисципліни здобувачі вищої освіти повинні вміти:

- визначати проблему в роботі підрозділу та обґрунтовувати потребу в технологічних або організаційних змінах;
- порівнювати альтернативні рішення за результативністю, надійністю, витратами та ризиками;
- будувати просту імітаційну модель правоохоронного процесу й використовувати результати моделювання для вибору рішення;

- обґрунтовувати добір технічних приладів і спеціальних засобів для визначеної ситуації з урахуванням їхніх можливостей та правових обмежень;
- знаходити, перевіряти, опрацьовувати й узагальнювати інформацію в доступних навчальних системах та програмах;
- застосовувати інструменти аналізу відкритих джерел і геопросторових даних, документувати походження матеріалів та результати їх опрацювання;
- перевіряти висновки автоматизованих систем, виявляти помилки й пояснювати, коли потрібна додаткова перевірка людиною;
- моделювати захищений міжвідомчий обмін інформацією, визначати права доступу, загрози та заходи захисту даних;
- розробляти план упровадження інновації із визначенням ресурсів, строків, відповідальних осіб та показників результативності;
- обґрунтовувати висновок про впровадження, доопрацювання або відхилення запропонованої інновації.

КОМПЕТЕНТНОСТІ ТА ПРОГРАМНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Інтегральна компетентність

Здатність розв’язувати складні задачі і проблеми у сфері правоохоронної діяльності та/або у процесі навчання, що передбачає проведення досліджень та/або здійснення інновацій та характеризується невизначеністю умов і вимог.

Загальні компетентності

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 9. Здатність генерувати нові ідеї (креативність).

Спеціальні (фахові) компетентності

СК 9. Здатність обирати оптимальні методи й засоби забезпечення публічної безпеки і порядку.

СК 10. Здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час рішення професійних завдань.

СК 12. Здатність до використання технічних приладів та спеціальних засобів, інформаційно-пошукових систем та баз даних, спеціальної техніки, оперативних та оперативно-технічних засобів, здійснення оперативно-розшукової діяльності.

Програмні результати навчання

РН 9. Використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення.

РН 10. Користуватись державною системою урядового зв’язку, Національною системою конфіденційного зв’язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв’язку спеціального призначення, урядового фельд’єгерського зв’язку.

РН 14. Розробляти та управляти проектами у сфері правоохоронної діяльності та з дотичних міждисциплінарних напрямів, аналізувати вимоги, визначати цілі, завдання, ресурси, строки, виконавців.

РН 16. Використовувати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань.

РН 17. Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальних засобів, засобів

фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності).

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

РОЗДІЛ 1. ОБҐРУНТУВАННЯ ТА ВИБІР ІННОВАЦІЙ У ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

Тема 1. Технологічні та організаційні інновації у правоохоронній діяльності. Визначення потреб підрозділу.

Тема 2. Системний аналіз та імітаційне моделювання для порівняння варіантів правоохоронних рішень.

Тема 3. Інноваційні технічні прилади та спеціальні засоби забезпечення публічної безпеки і порядку: можливості, обмеження та критерії вибору.

Тема 4. Інформаційно-пошукові системи, бази даних і спеціалізоване програмне забезпечення у правоохоронній діяльності.

РОЗДІЛ 2. ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ ТА УПРАВЛІННЯ ЇХ ВПРОВАДЖЕННЯМ

Тема 5. Аналіз відкритих цифрових джерел і технології кримінального аналізу.

Тема 6. Цифрова криміналістика, геоінформаційні технології та цифрова фіксація подій.

Тема 7. Штучний інтелект у правоохоронній діяльності: перевірка результатів, упередженість і контроль людини.

Тема 8. Захищений зв’язок та міжвідомчий інформаційний обмін у правоохоронній діяльності.

Тема 9. Захист даних, кібербезпека та правові обмеження застосування інноваційних технологій.

Тема 10. Проєктування, апробація та оцінювання результативності впровадження інновації у правоохоронному підрозділі.

ФОРМИ КОНТРОЛЮ ТА ОЦІНЮВАННЯ

Контроль результатів навчання та рівня сформованості компетентностей здобувачів здійснюється на засадах прозорості та академічної доброчесності відповідно до Положення про критерії оцінювання результатів навчання здобувачів вищої освіти у Класичному приватному університеті. http://virtuni.education.zp.ua/info_cpu/node/5478

У процесі вивчення навчальної дисципліни використовуються такі види контролю:

1. **Поточний контроль:** здійснюється протягом семестру під час практичних занять, виконання завдань самостійної роботи, підготовки мініпроєкту та проходження тестів за матеріалом розділів у Віртуальній аудиторії КПУ.

2. **Семестровий (підсумковий) контроль:** проводиться у формі **екзамену** за білетами.

Кожне завдання поточного контролю та екзамен оцінюються за 100-бальною шкалою.

Для оцінювання студентів використовується система накопичування балів. Згідно з «Положенням про організацію освітнього процесу в КПУ» підсумкова оцінка з дисципліни виставляється за 100-бальною шкалою з наступним переведенням у національну шкалу та шкалу ECTS.

Підсумкова оцінка визначається як середньозважена оцінок за практичні завдання, мініпроєкт, тести та екзамен. Частка поточного контролю становить 60%, екзамену — 40%.

$$\textbf{Підсумковий бал} = (B_1 \times k_1) + (B_2 \times k_2) + \ldots + (B_n \times k_n) + (B_{екз.} \times k_{екз.})$$

де:

$B_1, B_2, B_3, \ldots, B_n$ – бали за виконання завдань поточного контролю на практичних (семінарських) заняттях, самостійної та індивідуальної роботи, виставлені за 100-бальною шкалою; $k_1, k_2, k_3, \ldots, k_n$ – вагові коефіцієнти відповідного виду контролю;

$B_{екз.}$ – бал за підсумковий семестровий контроль (екзамен), виставлений за 100-бальною шкалою; $k_{екз.}$ – ваговий коефіцієнт підсумкового семестрового контролю (екзамену).

Сума вагових коефіцієнтів поточного та підсумкового контролю дорівнює 1

$$k_1 + k_2 + k_3 + \ldots + k_n + k_{екз.} = 1$$

Структура компонентів оцінювання та їх питома вага

Види навчальної діяльності здобувача	Шкала оцінювання завдання	Ваговий коеф.	Питома вага у загальній оцінці, %
Розділ 1. Обґрунтування та вибір інновацій у правоохоронній діяльності			
Практичне завдання 1. Визначення потреб правоохоронного підрозділу та підготовка обґрунтування необхідності інновації	100	0,04	4
Практичне завдання 2. Побудова простої імітаційної моделі правоохоронного процесу та порівняння результатів за різними умовами	100	0,06	6
Практичне завдання 3. Порівняння технічних приладів і спеціальних засобів та обґрунтування їх вибору для професійної ситуації	100	0,05	5
Практичне завдання 4. Пошук, відбір та оброблення інформації в доступній навчальній інформаційній системі з документуванням результатів	100	0,05	5
Тест за матеріалом розділу 1 (теми 1–4)	100	0,05	5
Розділ 2. Застосування технологій та управління їх впровадженням			
Практичне завдання 5. Перевірка відкритих цифрових джерел, побудова схеми зв’язків та оцінювання достовірності висновків	100	0,05	5
Практичне завдання 6. Створення карти подій за умовними даними та плану цифрової фіксації із заходами збереження цілісності матеріалів	100	0,05	5
Практичне завдання 7. Перевірка результату ШІ-інструменту на навчальному прикладі з визначенням помилок, обмежень і ризиків	100	0,05	5
Практичне завдання 8. Моделювання захищеного міжвідомчого обміну інформацією в доступному навчальному середовищі: визначення учасників, прав доступу, порядку передавання повідомлень, ризиків і заходів захисту даних.	100	0,05	5
Мініпроєкт. План упровадження інновації з визначенням альтернатив, ресурсів, строків, виконавців, порядку апробації та показників результативності	100	0,10	10
Тест за матеріалом розділу 2 (теми 5–10)	100	0,05	5
Екзамен	**100**	**0,40**	**40**
Разом	**100**	1	**100**
Додаткові досягнення з навчальної дисципліни (за наявністю) Результати науково-дослідної діяльності здобувача, зокрема за такі активності: – участь у предметних олімпіадах, конкурсах студентських наукових робіт з навчальної дисципліни; – участь у засіданнях наукових гуртків, зокрема в обговореннях у форматі круглих столів, присвячених актуальним темам з навчальної дисципліни; – публікації результатів досліджень у вигляді наукових статей, тез доповідей, а також виступи на наукових конференціях.	**До 10 балів**		

КРИТЕРІЇ ОЦІНЮВАННЯ

100-бальна система	шкала ЄКТС	Національна шкала	Характеристика вимог та критеріїв оцінювання
90–100	A	Відмінно	Здобувач самостійно обґрунтовує вибір інноваційного рішення відповідно до потреб правоохоронного підрозділу. Правильно застосовує навчальні інформаційні системи, засоби аналізу даних та імітаційного моделювання, перевіряє достовірність результатів. Аргументовано оцінює можливості технічних засобів, помилки ШІ, ризики інформаційного обміну та обмеження щодо захисту даних і прав людини. Готує узгоджений проєкт упровадження з визначеними ресурсами, строками, виконавцями та вимірюваними показниками результативності.
82–89	B	Добре	Здобувач правильно порівнює технологічні рішення та виконує практичні завдання з використанням навчальних інструментів. Обґрунтовує вибір засобів, перевіряє джерела й результати автоматизованого аналізу, визначає основні ризики. Проєкт упровадження загалом узгоджений; незначні неточності в розрахунках, документації або показниках не впливають на правильність висновків.
75–81	C	Добре	Здобувач розуміє призначення та обмеження основних технологій, переважно правильно виконує пошук, оброблення й аналіз даних. Будує навчальну модель і порівнює альтернативи, але недостатньо повно перевіряє результати або враховує ризики. Проєкт містить основні елементи, проте окремі ресурси, заходи апробації чи показники результативності потребують уточнення.
67–74	D	Задовільно	Здобувач виконує типові практичні завдання за зразком, пояснює призначення технологій і визначає основні заходи захисту інформації. Потребує допомоги під час налаштування моделі, перевірки даних, порівняння рішень та обґрунтування висновків. План упровадження розроблений частково й потребує доопрацювання.
60–66	E	Задовільно	Здобувач володіє мінімально необхідними знаннями, виконує базові операції з навчальними інструментами та визначає очевидні ризики. Результати документує неповно, вибір технології обґрунтовує поверхово. Проєкт містить мету й основні заходи, але має недоліки у визначенні ресурсів, відповідальності та способів перевірки результативності.
35–59	FX	Незадовільно	Знання про можливості технологій неповні. Здобувач допускає суттєві помилки під час виконання практичних завдань, моделювання та перевірки результатів. Недостатньо обґрунтовує вибір рішення й заходів захисту даних. Практичні роботи та проєкт потребують істотного доопрацювання.
0–34	F	Незадовільно	Здобувач не демонструє базового розуміння технологій і не може виконати основні навчальні операції. Не визначає суттєвих ризиків та не обґрунтовує запропонованого рішення. Завдання не виконані або їхній зміст не підтверджує досягнення мінімально необхідних результатів навчання.

ШКАЛА ОЦІНЮВАННЯ: 100-БАЛЬНА, НАЦІОНАЛЬНА ТА ECTS

Сума балів за всі види навчальної діяльності	Оцінка за шкалою ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи), практики	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
75-81	C		
67-74	D	задовільно	
60-66	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Політика щодо термінів виконання завдань та перескладання	З огляду на безпекову ситуацію, повітряні тривоги та перебої з електропостачанням, освітній процес базується на принципах гнучкості та академічної підтримки. Усі завдання виконуються здобувачами в асинхронному режимі без застосування штрафних санкцій чи зниження балів за порушення первинних термінів, якщо затримка зумовлена об'єктивними обставинами непереборної сили. Здавання та перескладання пропущених завдань чи тем здійснюється у зручному для студента темпі протягом семестру за погодженням із викладачем без будь-яких обмежень.
Політика академічної доброчесності	Здобувачі освіти зобов'язані неухильно дотримуватись принципів академічної доброчесності під час виконання усіх видів навчальної, наукової та творчої діяльності. Порушеннями академічної доброчесності вважаються: академічний плагіат, самоплагіат, фабрикація, фальсифікація, списування, обман, хабарництво, необ'єктивне оцінювання та академічне шахрайство. Здобувачам освіти забороняється вдаватися до будь-яких форм академічного шахрайства, зокрема: використовувати під час контрольних заходів заборонені матеріали або технічні засоби; посилатися на джерела, які не використовувались у роботі; здавати роботи з однаковим змістом, підготовлені різними особами. У разі встановлення порушення академічної доброчесності до здобувача освіти можуть бути застосовані такі заходи академічної відповідальності, як повторне проходження оцінювання (контрольна робота, екзамен, залік тощо), повторне вивчення відповідного освітнього компонента або відрахування з університету.
Політика щодо відвідування занять в умовах воєнного стану	Відвідування навчальних занять здобувачами вищої освіти є обов'язковим відповідно до затвердженого розкладу. *Організація освітнього процесу в умовах загрози та повітряних тривог* У разі включення сигналу «Повітряна тривога» під час проведення занять у режимі реального часу (Zoom / Google Meet) або перебування в приміщеннях Університету, проведення синхронного заняття негайно припиняється, а всі учасники освітнього процесу зобов'язані перейти до укриттів. Навчальне заняття, перерване через сигнал «Повітряна тривога» або яке не відбулося через її тривалість, автоматично переводиться в асинхронний режим. Відсутність здобувача освіти на синхронній конференції під час повітряної тривоги, відсутності електроенергії або зв'язку не є підставою для виставлення заборгованості чи зниження підсумкової оцінки, за умови опрацювання навчального матеріалу та виконання завдань в асинхронному режимі. *Застосування дистанційних технологій та форс-мажорних обставин* У разі переходу університету або його окремих структурних підрозділів на навчання із використанням дистанційних технологій через безпекову ситуацію чи інші форс-мажорні обставини, освітній процес регулюється *«Положенням про організацію освітнього процесу здобувачів вищої освіти з використанням дистанційних технологій при обмежені або відсутності фізичного відвідування закладів освіти здобувачами з причин непереборної сили (природні катаклізми, заходи карантинного порядку та інші форс-мажорні обставини) в «Класичному приватному університеті».* Формат участі у дистанційних заняттях адаптується до поточних технічних можливостей та умов безпеки здобувачів і викладачів.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основні

1. Федчак І. А. Основи кримінального аналізу : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2021. 288 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/3723.
2. Europol. AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement. 2024. URL: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing.
3. INTERPOL, UNICRI. Toolkit for Responsible AI Innovation in Law Enforcement. Оновлена версія. 2024. URL: https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit.
4. Office of the United Nations High Commissioner for Human Rights; Human Rights Center, University of California, Berkeley. Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law. New York ; Geneva : United Nations, 2022. URL: https://searchlibrary.ohchr.org/record/30334.

Додаткові

5. Томашевський В. М. Моделювання систем : підручник. Київ : Видавнича група BHV, 2005. 352 с. URL: https://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Tomashevsky_Model.system_2005.pdf.
6. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response. NIST Special Publication 800-86. 2006. URL: https://doi.org/10.6028/NIST.SP.800-86.

Нормативно-правові акти

7. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.
8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: https://zakon.rada.gov.ua/laws/show/2297-17.
9. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр.
10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.
11. Про Національну систему конфіденційного зв’язку : Закон України від 10.01.2002 № 2919-III. URL: https://zakon.rada.gov.ua/laws/show/2919-14.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

1. Єдиний державний вебпортал відкритих даних. URL: https://data.gov.ua/.
2. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua/.
3. QGIS. Навчальний посібник із роботи з геоінформаційною системою. URL: https://docs.qgis.org/latest/en/docs/training_manual/.
4. INTERPOL. Artificial Intelligence Toolkit — матеріали щодо відповідального впровадження штучного інтелекту в правоохоронній діяльності. URL: https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit.