КЛАСИЧНИЙ ПРИВАТНИЙ УНІВЕРСИТЕТ

Кафедра кримінального права, процесу та криміналістики

СИЛАБУС

навчальної дисципліни

ПП 8. Інформаційні технології у 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=3646
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	8
	Практичні	26
	Самостійна робота	56
Форма контролю	Залік	
Попередні компоненти (Пререквізити)	Теоретико-правові засади правоохоронної діяльності в Україні	
Паралельні та подальші компоненти (Постреквізити)	Інноваційні технології у сучасній правоохоронній діяльності Практична підготовка в правоохоронних органах Підготовка та захист кваліфікаційної роботи	

МЕТА, ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета навчальної дисципліни

Навчити застосовувати інформаційні технології для пошуку, перевірки й аналізу даних у правоохоронній діяльності, обґрунтовувати рішення за результатами аналізу та безпечно обмінюватися інформацією.

Завдання навчальної дисципліни:

- розкрити призначення інформаційних систем і цифрових ресурсів правоохоронної діяльності;
- сформувати навички роботи з електронними документами та перевірки електронного підпису;
- навчити шукати й перевіряти законодавство, судову практику та відомості з реєстрів і відкритих джерел;
- розвинути вміння готувати й аналізувати дані за допомогою електронних таблиць і баз даних;
- сформувати навички візуалізації інформації та застосування простих імітаційних моделей;
- ознайомити з правилами захисту даних, цифрової взаємодії та користування системами спеціального зв'язку;
- навчити перевіряти якість результатів і документувати виконані дії.

У результаті вивчення дисципліни студенти повинні знати:

- призначення інформаційних систем, баз даних і програмних засобів у правоохоронній діяльності;
- вимоги до електронних документів, метаданих, електронних підписів і перевірки цілісності файлів;
- способи пошуку інформації та критерії оцінювання достовірності джерел;
- методи очищення, структурування, аналізу й візуалізації даних;
- принципи побудови баз даних і виконання запитів;
- основи імітаційного моделювання та порівняння результатів модельних експериментів;
- вимоги до захисту персональних даних, розмежування доступу й реагування на інформаційні інциденти;
- призначення державної системи урядового зв'язку, Національної системи конфіденційного зв'язку та загальні правила захищеного інформаційного обміну;
- способи перевірки результатів автоматизованого опрацювання даних, зокрема із застосуванням штучного інтелекту, та документування виконаних дій.

Після вивчення дисципліни студенти повинні вміти:

- визначати інформаційні потреби підрозділу, джерела даних і права доступу;
- створювати електронні документи та перевіряти електронний підпис і цілісність файлів;
- знаходити нормативні акти, судові рішення й інші матеріали, фіксувати джерела та перевіряти їх достовірність;
- очищати навчальні набори даних, застосовувати формули, фільтри та зведені таблиці;
- створювати просту навчальну базу даних і виконувати запити;
- аналізувати дані, подавати результати в таблицях, діаграмах і картах та пояснювати обмеження висновків;
- застосовувати просту імітаційну модель, змінювати її параметри й порівнювати результати;

- оцінювати інформаційні ризики, визначати заходи захисту та безпечно обмінюватися повідомленнями й файлами в навчальному середовищі;
- перевіряти результати автоматизованого опрацювання даних, виявляти помилки й необґрунтовані висновки;
- укладати цифрове портфоліо виконаних робіт, пояснювати послідовність дій і обґрунтовувати отримані результати.

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 2. Здатність застосовувати знання у практичних ситуаціях.

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 10. Здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні (фахові) компетентності

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 13. Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію.

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.

ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

РОЗДІЛ 1. ІНФОРМАЦІЙНІ РЕСУРСИ ТА ОПРАЦЮВАННЯ ДАНИХ

Тема 1. Інформаційні системи та цифрове середовище правоохоронної діяльності.

Тема 2. Електронні документи, ідентифікація та документообіг.

Тема 3. Правові інформаційні ресурси, реєстри та пошукові технології.

Тема 4. Електронні таблиці та підготовка даних до аналізу.

Тема 5. Бази даних та інформаційно-пошукові системи.

РОЗДІЛ 2. АНАЛІТИЧНА РОБОТА, БЕЗПЕКА ТА ЦИФРОВА ВЗАЄМОДІЯ

Тема 6. Аналіз, візуалізація, просторове представлення даних та імітаційне моделювання правоохоронних процесів.

Тема 7. Відкриті цифрові джерела та перевірка матеріалів.

Тема 8. Інформаційна безпека та захист персональних даних.

Тема 9. Захищена цифрова взаємодія та системи спеціального зв'язку у правоохоронній діяльності.

Тема 10. Комплексне інформаційно-аналітичне завдання.

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:

Поточний контроль здійснюється протягом семестру під час виконання практичних завдань із пошуку, перевірки, оброблення та аналізу даних, роботи з електронними документами й базами даних, імітаційного моделювання, захищеного обміну інформацією та захисту цифрового портфоліо.

Семестровий (підсумковий) контроль проводиться у формі заліку за накопиченими результатами поточного контролю.

Кожне практичне завдання оцінюється за 100-бальною шкалою. Підсумкова оцінка визначається як середньозважена:

Підсумковий бал = $В_1 \times 0{,}10 + В_2 \times 0{,}10 + \ldots + В_{10} \times 0{,}10$,

де $В_1$–$В_{10}$ – оцінки за практичні завдання. Сума вагових коефіцієнтів дорівнює **1,00**.

Структура компонентів оцінювання та їх питома вага

Види навчальної діяльності здобувача	Шкала оцінювання завдання	Ваговий коеф.	Питома вага у загальній оцінці, %
Розділ 1. Інформаційні ресурси та опрацювання даних			
Практичне завдання 1. Побудова схеми інформаційних потоків і визначення прав доступу	100	0,10	10
Практичне завдання 2. Створення електронного документа та перевірка електронного підпису	100	0,10	10
Практичне завдання 3. Пошук законодавства й судової практики та перевірка джерел	100	0,10	10
Практичне завдання 4. Очищення й підготовка навчального набору даних	100	0,10	10
Практичне завдання 5. Створення навчальної бази даних і виконання запитів	100	0,10	10
Розділ 2. Аналітична робота, безпека та цифрова взаємодія			
Практичне завдання 6. Аналіз і візуалізація даних та порівняння результатів простої імітаційної моделі	100	0,10	10
Практичне завдання 7. Перевірка відкритого цифрового джерела та походження матеріалів	100	0,10	10
Практичне завдання 8. Оцінювання інформаційних ризиків і планування захисту даних	100	0,10	10
Практичне завдання 9. Захищений обмін повідомленнями й файлами в навчальному середовищі та визначення правил користування системами спеціального зв’язку	100	0,10	10
Практичне завдання 10. Захист цифрового портфоліо: відтворення виконаних дій та обґрунтування висновків	100	0,10	10
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	Зараховано	Здобувач самостійно знаходить, перевіряє, готує й аналізує дані. Правильно працює з електронними документами, підписами, таблицями та базами даних. Порівнює результати імітаційної моделі, обґрунтовує висновки та пояснює їхні обмеження. Дотримується правил захисту інформації. Під час захисту портфоліо пояснює і повторює виконані операції.
82–89	B	Зараховано	Правильно користується програмними засобами, перевіряє джерела та результати оброблення даних. Працює з моделлю й безпечно обмінюється інформацією в навчальному середовищі. Допускає незначні неточності, які не впливають на правильність висновків.
75–81	C	Зараховано	Переважно правильно виконує завдання з документами, таблицями, базами даних і моделлю. Допускає окремі помилки в перевірці джерел, налаштуванні запитів, візуалізації або документуванні дій. Виправляє їх після уточнювальних запитань.
67–74	D	Зараховано	Виконує типові операції за зразком. Потребує допомоги під час підготовки даних, побудови запитів, роботи з моделлю та пояснення результатів. Визначає основні інформаційні ризики й заходи захисту.
60–66	E	Зараховано	Володіє мінімально необхідними знаннями та виконує базові операції з навчальними даними. Допускає помилки, неповно документує дії й поверхово обґрунтовує висновки. Може пояснити основні результати власної роботи та правила безпечного обміну інформацією.
35–59	FX	Не зараховано	Має фрагментарні знання, допускає суттєві помилки в пошуку, обробленні та аналізі даних. Недостатньо перевіряє результати й не може відтворити послідовність виконаних операцій. Завдання та портфоліо потребують істотного доопрацювання.
0–34	F	Не зараховано	Не демонструє базових умінь роботи з інформаційними інструментами, не може виконати основні операції з даними та пояснити результати. Основні завдання не виконані або виконані неправильно.

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. Інформаційні технології : навчальний посібник / О. І. Зачек, В. В. Сеник, Т. В. Магеровська та ін. ; за ред. О. І. Зачека. Львів : Львівський державний університет внутрішніх справ, 2022. 432 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/6995.

2. 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.

Додаткові

3. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції : навчальний посібник. Львів : ЛьвДУВС, 2017. 244 с. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/318.

4. 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.

Нормативно-правові акти

5. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: https://zakon.rada.gov.ua/laws/show/851-15.

6. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII. URL: https://zakon.rada.gov.ua/laws/show/2155-19.

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

8. 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.

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

10. 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. Законодавство України. Офіційна база Верховної Ради України. URL: https://zakon.rada.gov.ua/.

2. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/.

3. Єдиний державний вебпортал відкритих даних. URL: https://data.gov.ua/.

4. Центральний засвідчувальний орган. Сервіс перевірки електронного підпису. URL: https://czo.gov.ua/verify.

5. LibreOffice Calc. Офіційна довідка українською мовою. URL: https://help.libreoffice.org/latest/uk/text/scalc/main0000.html.

6. SQLite. Офіційна документація з мови SQL. URL: https://www.sqlite.org/lang.html.

7. QGIS. Навчальний посібник. URL: https://docs.qgis.org/latest/en/docs/training_manual/.

8. Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA. URL: https://cert.gov.ua/.