ЗАКЛАД ВИЩОЇ ОСВІТИ
«УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА»

Факультет суспільних і прикладних наук

Кафедра права та публічного управління
Кафедра Інформаційних технологій

ЗАТВЕРДЖУЮ
Проректор з методичної роботи
_____ Ярослав ШТАНЬКО
“24” ____01____ 2025 р.

СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань:	26 Цивільна безпека
Спеціальність:	262 Правоохоронна діяльність
Освітньо-професійна (освітньо-наукова) програма:	Правоохоронна діяльність
Освітній рівень:	другий (магістерський)
Статус дисципліни:	обов’язкова
Мова викладання, навчання та оцінювання:	українська

Івано-Франківськ
2025

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

ЗАТВЕРДЖЕНО:
на засіданні кафедри інформаційних технологій
протокол № 1 від 18.09.24 р.

Завідувач кафедри Сергій ВАЩИШАК

УЗГОДЖЕНО:

Гарант ОП Сергій РЕПЕЦЬКИЙ

на засіданні кафедри права та публічного
правління протокол № 6 від 24.01. 2025 р.

В.о. Завідувач кафедри Олександра ПТАШНИК

СХВАЛЕНО:

на засіданні Науково-методичної ради, протокол № 6 від 29.01 2025 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	https://online.ukd.edu.ua/enrol/index.php?id=6707

Анотація навчальної дисципліни «Сучасні інформаційні технології в правоохоронній діяльності»

ВСТУП

Сучасний світ розвивається стрімкими темпами, а цифровізація охоплює всі сфери суспільного життя, включаючи правоохоронну діяльність. Використання інформаційних технологій стає необхідністю для ефективного запобігання злочинам, їх розслідування та підтримки громадської безпеки. Новітні технології відкривають можливості для аналізу великих масивів даних, відстеження фінансових потоків у криптовалютах, автоматизованого моніторингу злочинних схем та кіберзагроз.

З одного боку, цифровізація дозволяє правоохоронним органам швидко обробляти інформацію, проводити криміналістичний аналіз цифрових доказів, використовувати штучний інтелект для прогнозування злочинності та захищати критичну інфраструктуру. З іншого боку, сучасні технології стають інструментом злочинців, які використовують анонімні фінансові транзакції, обхідні технології у даркнеті, deepfake та злом IoT-пристроїв.

Ця дисципліна надає студентам знання про сучасні інформаційні технології, їх застосування в боротьбі зі злочинністю та захисті суспільства. Особливий акцент робиться на таких напрямках, як цифрова криміналістика, кіберзлочинність, аналітика великих даних, блокчейн та криптовалюти, біометричні технології, використання хмарних сховищ та штучного інтелекту у правоохоронній діяльності.

Опанування курсу забезпечить студентам комплексне розуміння принципів функціонування сучасних технологій, їх переваг та ризиків у правоохоронній сфері, а також допоможе оволодіти практичними методами їх застосування в боротьбі зі злочинністю.

- Згідно з вимогами освітньо-професійних та освітньо-кваліфікаційних програм студенти повинні **знати**:
- Основні напрями цифровізації правоохоронної діяльності, їх переваги та виклики.
- Методи збору та аналізу цифрових доказів, правила роботи з електронною інформацією.
- Основи блокчейн-технологій, їх використання у злочинній діяльності та методи розслідування криптовалютних злочинів.
- Сучасні методи кіберзахисту, аналізу кібератак та механізми запобігання злочинам у кіберпросторі.
- Використання штучного інтелекту у сфері криміналістики, прогнозування злочинності та моніторингу загроз.
- Роль великих даних у розслідуванні злочинів, методи виявлення закономірностей та аналізу соціальних зв’язків у кримінальних угрупованнях.
- Біометричні технології та їх правові аспекти у правоохоронній діяльності.
- Особливості захисту конфіденційних даних, цифрової безпеки правоохоронних органів та критичної інфраструктури.

- Вплив IoT-технологій та хмарних сервісів на діяльність правоохоронних органів, методи їхнього захисту від атак.
- Нормативно-правові засади використання інформаційних технологій у сфері боротьби зі злочинністю.

- **вміти**:
- Використовувати сучасні інформаційні технології для моніторингу, аналізу та розслідування злочинів.
- Збирати, аналізувати та документувати цифрові докази відповідно до міжнародних стандартів цифрової криміналістики.
- Виявляти та розслідувати злочини, пов'язані з використанням віртуальних активів та криптовалют.
- Аналізувати великі дані та прогнозувати криміногенні тенденції за допомогою сучасних аналітичних інструментів.
- Визначати слабкі місця кіберзахисту, розробляти заходи безпеки для захисту інформаційних систем та даних.
- Використовувати алгоритми штучного інтелекту для аналізу відеоспостереження, розпізнавання осіб та аналізу кримінальних схем.
- Застосовувати технології розпізнавання облич, біометричних даних та методи цифрової ідентифікації в правоохоронній діяльності.
- Оцінювати ризики цифровізації правоохоронної діяльності, розробляти стратегії їх мінімізації та впроваджувати сучасні технології безпеки.
- Працювати з хмарними сховищами, захищати конфіденційну інформацію та використовувати технології кіберзахисту.
- Виявляти злочинні схеми, пов'язані з кіберзлочинністю, цифровими фінансами, соціальною інженерією та інтернет-шахрайством.

Компетентності та результати навчання, яких набувають здобувачі освіти внаслідок вивчення навчальної дисципліни (шифри та зміст компетентностей та програмних результатів навчання вказано відповідно до ОПП "Правоохоронна діяльність" (2024/2025).

Шифр та назва компетентності	Результати навчання
СК3. Здатність професійно оперувати категоріальнопонятійним апаратом права і правоохоронної діяльності. СК4. Здатність до критичного та системного аналізу правових явищ і застосування набутих знань та навичок у професійній діяльності..	РН9. 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.

СК5. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел. СК6. Здатність аналізувати та систематизувати одержані результати, формулювати аргументовані висновки та рекомендації.	РН11. Знати і розуміти сучасні правові доктрини, цінності та принципи функціонування національної правової системи.

ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Курс	**1**		
Семестр	**2**		
Кількість кредитів ЄКТС	**3**		
Аудиторні навчальні заняття		**денна форма**	**заочна форма**
	лекції	16	-
	семінари, практичні	14	-
Самостійна робота		60	_
Форма підсумкового контролю	**екзамен**		

Тема 1. Вступ до сучасних інформаційних технологій у правоохоронній діяльності

Значення цифрових технологій у правоохоронній діяльності.

Основні інформаційні системи, що використовуються правоохоронними органами.

Виклики та загрози цифровізації у сфері безпеки.

Етичні та правові аспекти використання інформаційних технологій у правоохоронній сфері.

Завдання:

1. Проаналізувати міжнародний досвід впровадження інформаційних технологій у правоохоронній діяльності (на прикладі ЄС, США).

2. Дослідити цифрові ризики для правоохоронних органів та запропонувати механізми їх мінімізації.

Тема 2. Кіберзлочинність та методи її розслідування

Основні категорії кіберзлочинів (шахрайство, кібершпигунство, DDoS-атаки, злочини проти критичної інфраструктури тощо).

Інструменти кіберзлочинців та методи їхнього виявлення.

Цифрова криміналістика: методи збору, аналізу та збереження цифрових доказів.

Співпраця правоохоронних органів із приватним сектором у боротьбі з кіберзлочинністю.

Завдання:

1. Проаналізувати реальний кейс розслідування кіберзлочину (за даними CERT-UA або Європолу).

2. Описати принципи збору цифрових доказів, виходячи з міжнародних стандартів.

Тема 3. Віртуальні активи та технології блокчейн: як їх використовують злочинці та правоохоронці

Основи технології блокчейн: криптовалюти, NFT, смарт-контракти.

Способи використання криптовалют у злочинній діяльності (відмивання грошей, фінансування тероризму, фішингові схеми, «чорні» ринки).

Методи виявлення та аналізу криптотранзакцій (Chainalysis, Crystal Blockchain, Elliptic).

Державне регулювання та правоохоронна практика щодо криптовалют.

Конфіскація цифрових активів: досвід України та світу.

Завдання:

1. Проаналізувати методи відстеження криптовалютних транзакцій на основі відкритих блокчейн-досліджень.

2. Підготувати короткий огляд судових рішень, пов'язаних із конфіскацією криптовалют.

Тема 4. Штучний інтелект у протидії злочинності

Основи технології ШІ: машинне навчання, нейромережі, визначення меж використання ШІ, ризики використання ШІ.

Використання ШІ в розпізнаванні осіб та поведінковому аналізі.

Аналіз великих даних для прогнозування злочинності.

Автоматизовані системи моніторингу кіберзлочинів та виявлення фішингових атак.

Роль ШІ у криміналістиці: розшифровка аудіо- та відеозаписів, аналіз цифрових доказів.

Етичні ризики та зловживання ШІ у правоохоронній діяльності.

Завдання:

1. Дослідити реальні приклади використання ШІ у правоохоронних органах (наприклад, Predictive Policing у США).

2. Проаналізувати проблему зловживання ШІ в кримінальних схемах (генерація deepfake, автоматизація фішингових атак).

Тема 5. Великі дані та аналітика у розслідуванні злочинів

Використання великих даних для аналізу криміногенної ситуації.

Інструменти аналізу кримінальних даних: IBM i2, Palantir, Tableau.

Автоматизовані системи аналізу відеоспостереження.

Виявлення зв'язків між злочинними угрупованнями за допомогою соціального аналізу даних.

Персональні дані та захист конфіденційної інформації.

Завдання:

1. Розробити модель використання аналітики великих даних для прогнозування рівня злочинності у певному регіоні.

2. Дослідити методи маскування та підміни даних, які використовують злочинці для ухилення від розслідування.

Тема 6. Біометричні технології та їх застосування у правоохоронній діяльності

Системи розпізнавання обличчя та їхнє використання в кримінальних розслідуваннях.

Автоматизовані бази біометричних даних: можливості та загрози.

Використання відбитків пальців та ДНК-аналізу у криміналістиці.

Правові аспекти застосування біометрії та захист персональних даних.

Завдання:

1. Проаналізувати законодавчі обмеження використання біометрії у правоохоронній сфері.

2. Оцінити ефективність технологій розпізнавання обличчя на прикладі їх використання в різних країнах.

Тема 7. Хмарні технології, IoT та цифрова безпека у правоохоронній діяльності

Використання хмарних сховищ для роботи з доказами.

IoT-пристрої та їхнє використання у забезпеченні правопорядку.

Кіберзахист інфраструктури «розумного міста».

Захист інформації від несанкціонованого доступу.

Інструменти моніторингу та виявлення аномальної активності.

Проблеми цифрової безпеки правоохоронних органів.

Завдання:

1. Проаналізувати ризики використання хмарних технологій у кримінальних розслідуваннях.

2. Запропонувати методи підвищення безпеки збереження цифрових доказів у правоохоронних органах.

3. Дослідити кейси атак на IoT-пристрої та запропонувати шляхи їхнього запобігання.

Зміст самостійної роботи студентів

Розподіл годин, виділених на вивчення дисципліни «Кібербезпека і управління інформаційними ресурсами»

Найменування видів робіт	**Розподіл годин**

	денна форма	заочна форма
Самостійна робота, год, у т.ч.:	60	-
Опрацювання матеріалу, викладеного на лекціях	10	-
Підготовка до практичних занять та контрольних заходів	10	-
Підготовка звітів з практичних робіт	-	-
Підготовка до поточного контролю	10	-
Опрацювання матеріалу, винесеного на самостійне вивчення	20	-

ПОЛІТИКА 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. “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

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 в галузі права.

Програмний результат навчання	**Метод навчання**	**Метод оцінювання**
ПРН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.	словесні методи (лекція, розповідь пояснення); наочні методи (ілюстрування, комп’ютерні і мультимедійні методи);	усний контроль, поточний контроль, програмований контроль

	інтерактивні методи (Case study, дискусія, мозковий штурм, робота в команді (групах))	
ПРН9. 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.	словесні методи (лекція, розповідь пояснення); наочні методи (ілюстрування, комп'ютерні і мультимедійні методи); інтерактивні методи (дискусія, мозковий штурм, робота в команді (групах)).	усний контроль, поточний контроль, програмований контроль
ПРН3. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її.	словесні методи (лекція, розповідь пояснення); наочні методи (ілюстрування, комп'ютерні і мультимедійні методи); інтерактивні методи (Case study, дискусія, мозковий штурм, робота в команді (групах)	усний контроль, поточний контроль, програмований контроль

ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Вид	**Зміст**	**% від загальної оцінки**	**Бал**	
			min	**max**
Поточні контрольні заходи	всього	60	35	60
Підсумкові контрольні заходи	екзамен	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».

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 (диференційований залік/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
	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.

Основна література

1. Холод О.М. Комунікаційні технології: Підручник. К.: ЦНЛ, 2013.- 212с.

2. Томашевський О.М., Цегелик Г.Г., Вітер М.Б., Дубук В.І. Інформаційні технології та моделювання: Навч.посібник. К.: ЦУЛ, 2012.

296 с.

3. Буйницька О.П. Інформаційні технології та технічні засоби навчання: Навч.посібник. К.: ЦУЛ, 2012. 240 с.

Електронні інформаційні ресурси

4. Швачич Г. Г. Сучасні інформаційно-комунікаційні технології : навч. посіб. Г. Г. Швачич, В. В.Толстой, Л. М. Петречук [та ін.]. – Дніпро: НМетАУ, 2017. 230 с. URL: https://nmetau.edu.ua/file/ikt_tutor.pdf (дата звернення: 25.08. 2024).

5. Інформаційно-комунікаційні технології в бізнесі : навч. посіб. уклад. М. О. Чупріна. – К.: КПІ ім. Ігоря Сікорського, 2020. 116 с. URL: https://ela.kpi.ua/bitstream/123456789/33703/1/Infor_tech.pdf (дата звернення: 25.08. 2024).

6. Гуревич Р. С. Інформаційно-комунікаційні технології в професійній освіті : монографія. Р. С. Гуревич, М. Ю. Кадемія, М. М. Козяр; за ред. Р. С. Гуревича. Львів : Льв. держ. ун-т безпеки життєдіяльності, 2012. 506 с. URL: http://ito.vspu.net/repozitariy/Kademiia/stati/15last/7_15zIKT.pdf (дата звернення: 25.08. 2024).