

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ
ПЕНІТЕНЦІАРНА АКАДЕМІЯ УКРАЇНИ

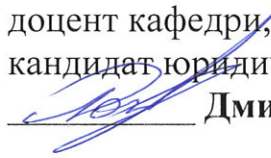
КАФЕДРА ВОГНЕВОЇ ТА СПЕЦІАЛЬНОЇ ПІДГОТОВКИ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
Інформаційні системи та технології в правоохоронній діяльності

для підготовки фахівців на другому (магістерському) рівні вищої освіти
за спеціальністю К9 Правоохоронна діяльність

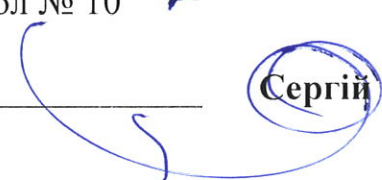
РОЗРОБНИК:

доцент кафедри,
кандидат юридичних наук

 **Дмитро ПОКРИШЕНЬ**

Розглянуто та затверджено
на засіданні кафедри
«01» вересня 2026 року,
протокол № 10

Узгоджено з гарантом освітньої програми _____

 **Сергій ІВАШКО**

Обсяг: 3 кредити ECTS .

Чернігів – 2026

АНОТАЦІЯ КУРСУ

Одним з основних підходів при досягненні цілей реформи правоохоронної системи визнається інформатизація професійної діяльності, що передбачає підвищення ефективності роботи і взаємодії правоохоронних органів шляхом максимального використання інформаційно-комунікаційних технологій.

Курс Інформаційні системи та технології в правоохоронній діяльності формує уявлення про сучасні тенденції та перспективи розвитку інформаційного суспільства загалом та можливість використання засобів інформаційних технологій для ефективного виконання професійних обов'язків, зокрема.

Предметом вивчення навчальної дисципліни є: апаратне забезпечення засобів обчислювальної техніки, програмне забезпечення засобів обчислювальної техніки; алгоритмічні засоби взаємодії апаратного з програмним забезпеченням та користувачем.

Навчальна дисципліна Інформаційні системи та технології в правоохоронній діяльності встановлює і реалізує міждисциплінарні зв'язки з наступними курсами:

- Філософія – історія розвитку та дуалістичність поняття «інформація»;
- Діловодство – підготовка й оформлення службових документів;
- Соціологія та Політологія – збір та обробка статистичних даних;
- Економічна теорія – обробка табличної інформації, побудова графіків, зведених таблиць та баз даних.
- Тактико-спеціальна підготовка – особливості роботи технічних засобів охорони; засобів збору, обробки та відображення інформації; робота систем відео-спостереження та управління доступом у приміщення;
- Криміналістика – застосування автоматизованих систем оперативно-розшукового і оперативно-довідкового призначення;

Мета навчальної дисципліни: є формування у здобувачів вищої освіти інформативної компетентності та здатності ефективно, безпечно й правомірно застосовувати інформаційні системи і технології у правоохоронній діяльності.

Завдання навчальної дисципліни:

1. Збирати необхідну інформацію з різних джерел, аналізувати і оцінювати її. Здійснювати пошук інформації у доступних джерелах;
2. Формулювати і перевіряти гіпотези, аргументувати висновки;
3. Здійснювати координацію діяльності суб'єктів забезпечення публ. Безпеки і порядку, а також комунікацію з фізичними та юридичними особами;
4. Працювати автономно та в команді;
5. Застосовувати інформаційні системи і технології, технології захисту даних, методи оброблення, накопичення та оцінювання інформації, засоби інформаційно-аналітичної роботи, бази даних, мережеві технології, автоматизовані інформаційно-пошукові системи, електронні бібліотеки та проблемно-тематичні банки даних для виконання професійних завдань;
6. Використовувати основні засоби та методи забезпечення правопорядку; попередження та припинення загроз національної безпеки (кібербезпеку, економічну та інформаційну безпеку);
7. Брати участь у формуванні та реалізації державної політики у сфері захисту інформації.

Дисципліна спрямована на формування таких програмних компетентностей:

Загальні компетентності (ЗК):

- ЗК 1. Здатність до абстрактного мислення, аналізу та синтезу.
- ЗК 2. Здатність застосовувати знання у практичних ситуаціях.
- ЗК 5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні (фахові, предметні) компетентності (СК):

7	Комп'ютерні мережі, інформаційна безпека та спільна робота в мережі	6	2	2		2
8	Використання мережевих технологій в професійній діяльності	12			4	8
	Всього за розділом	90	8	4	20	58
	Всього за навчальним планом	90	8	4	20	58

Тематичний план (заочна форма навчання)

№ теми	Назви розділів і тем	Кількість годин				
		Усього	Л	СЗ	ПЗ	СР
Розділ 1. Теорія інформатики та інформаційно-комп'ютерної техніки						
1	Предмет інформатики. Основи функціонування ІКТ. Властивості Інформації	10	2			10
2	Види та характеристика засобів інформаційно-комп'ютерної техніки	10				10
Розділ 2 Програмне забезпечення засобів інформаційно-комп'ютерної техніки						
3	Загальна характеристика та основи ефективного використання програмного забезпечення в професійній діяльності	12		2		10
4	Створення та обробка службових документів за допомогою текстового процесора.	14			2	10
5	Створення та обробка службових документів за допомогою табличного процесора.	12				10
6	Використання мультимедійних засобів в професійній діяльності	10				10
Розділ 3. Комп'ютерні мережі						
7	Комп'ютерні мережі, інформаційна безпека та спільна робота в мережі	10				10
8	Використання мережевих технологій в професійній діяльності	12			4	10
	Всього за розділом	90	2	2	6	80
	Всього за навчальним планом	90	2	2	6	80

ЗАВДАННЯ ДО СЕМІНАРІВ ТА ПРАКТИЧНИХ ЗАНЯТЬ

СЕМІНАРСЬКІ ЗАНЯТТЯ

Готуючись до семінарського заняття Ви маєте підготувати конспект питань, що містяться в плані відповідної теми. Наявність конспекту всіх (!) питань та ваша присутність на занятті є запорукою успішної роботи та отримання балів (їх кількість залежить від вашої активності та якості підготовки). Відсутність конспекту або неповний конспект, навіть за умови вашої присутності на семінарі, оцінюється в 0 балів.

Тема 3. Загальна характеристика та основи ефективного використання програмного забезпечення у професійній діяльності

Навчальні питання:

1. Класифікація і призначення програмного забезпечення.
2. Операційні системи та організація взаємодії користувача з комп'ютером.
3. Службові програми, оновлення, резервне копіювання та ліцензування.
4. Критерії вибору програмних засобів для правоохоронної діяльності.

Контрольні питання

1. Чим системне програмне забезпечення відрізняється від прикладного?
2. Які функції виконує операційна система?
3. Як ліцензування програм впливає на законність їх професійного використання?
4. Які критерії доцільно застосовувати під час вибору програмного засобу?

Методичні рекомендації до підготовки. Опрацюйте навчальні матеріали та рекомендовані джерела, визначте практичне значення розглянутих технологій і підготуйте аргументовані відповіді. Приклади мають ураховувати вимоги інформаційної безпеки, захисту персональних даних, законності й професійної етики.

Тема 7. Комп'ютерні мережі, інформаційна безпека та спільна робота в мережі

Навчальні питання:

1. Призначення, види й компоненти комп'ютерних мереж.
2. Спільне використання мережевих ресурсів.
3. Пошук і перевірка інформації в мережі Інтернет та правових базах даних.
4. Основні мережеві загрози й правила безпечної комунікації.

Контрольні питання

1. Які основні види комп'ютерних мереж?
2. Як організовується спільний доступ до ресурсів?
3. За якими критеріями перевіряють надійність мережевого джерела?
4. Які мережеві загрози є найбільш актуальними для правоохоронних органів?

Методичні рекомендації до підготовки. Опрацюйте навчальні матеріали та рекомендовані джерела, визначте практичне значення розглянутих технологій і підготуйте аргументовані відповіді. Приклади мають ураховувати вимоги інформаційної безпеки, захисту персональних даних, законності й професійної етики.

ПРАКТИЧНІ ЗАНЯТТЯ

До практичних занять необхідно опрацювати відповідний теоретичний матеріал і підготуватися до виконання завдань у визначеному програмному середовищі. Результат роботи подається у встановленому викладачем електронному форматі.

Тема 2. Види та характеристика засобів інформаційно-комп'ютерної техніки.

Для успішного виконання практичного завдання необхідно повторити матеріал лекційного заняття:

1. Логічну схему функціонування засобів інформаційно-комп'ютерної техніки.
2. Які апаратні пристрої впливають на продуктивність роботи інформаційно-комп'ютерної техніки.
3. Основні характеристики центрального мікропроцесора, пристроїв оперативної та постійної пам'яті.

4. Базову конфігурація комп'ютера та види периферійних пристроїв.

Додатково самостійно необхідно підготувати матеріал на теми:

1. Загальні налаштування, види і основні характеристики сканерів.
2. Загальні налаштування, види і основні характеристики принтерів
3. Загальні налаштування і основні характеристики фото, відео- та веб-камер.
4. Загальні налаштування, види і основні характеристики мікрофонів та акустичних систем.
5. Загальні налаштування, види і основні характеристики текстових та цифрових клавіатур.
6. Загальні налаштування, види і основні характеристики вказівних (координатних) пристроїв: миша, джойстик, touchpad, touchscreen, графічний планшет.
7. Загальні налаштування, види і основні характеристики моніторів.
8. Загальні налаштування, види і основні характеристики мультимедійних проекторів.

Контрольні питання

1. Які компоненти визначають продуктивність комп'ютера?
2. Як обрати периферійне обладнання відповідно до службового завдання?

Методичні рекомендації до підготовки. Перед виконанням створіть окрему робочу копію файлу. Дотримуйтеся послідовності операцій, використовуйте зрозумілі назви файлів і

об'єктів, регулярно зберігайте результат. Після завершення перевірте відповідність роботи завданню, коректність відображення, відсутність зайвих персональних або службових даних і можливість відкриття файлу на іншому пристрої.

Тема 4. Створення та обробка службових документів за допомогою текстового процесора.

Для успішного виконання практичного завдання необхідно знати:

1. Основи ефективної роботи при створенні та обробці службової документації.
2. Вимоги нормативно-правових актів щодо виготовлення документації за допомогою друкувальних засобів.
3. Елементи інтерфейсу текстового процесора.
4. Основні налаштування текстового процесора
5. Порядок форматування та редагування документації
6. Форматування документу на рівні шрифту, абзацу, аркуша.
7. Використання комбінацій клавіш для оперативного форматування тексту та навігації по документу.
8. Порядок роботи з таблицями в текстовому процесорі.

Перелік тем для реферативних доповідей та самостійного опрацювання:

1. Редагування та форматування графічних об'єктів в середовищі текстового процесора MS Word .
2. Редагування та форматування таблиць в середовищі текстового процесора MS Word .
3. Використання діаграм та SmartArt об'єктів в середовищі текстового процесора MS Word .
4. Можливості додаткової вкладки «Розробник» текстового процесора MS Word .

Контрольні питання

1. Які параметри сторінки необхідно встановити до початку роботи?
2. Чим стильове форматування відрізняється від прямого?

Методичні рекомендації до підготовки. Перед виконанням створіть окрему робочу копію файлу. Дотримуйтеся послідовності операцій, використовуйте зрозумілі назви файлів і об'єктів, регулярно зберігайте результат. Після завершення перевірте відповідність роботи завданню, коректність відображення, відсутність зайвих персональних або службових даних і можливість відкриття файлу на іншому пристрої.

Тема 5. Створення та обробка службових документів за допомогою табличного процесора.

Для успішного виконання практичного завдання необхідно знати:

1. Випадки ефективної оптимізації офісної діяльності за допомогою інструментів табличних процесорів.
2. Елементи інтерфейсу табличного процесора.
3. Основні налаштування табличного процесора.
4. Порядок навігації, редагування та форматування аркушів робочої книги;
5. Синтаксис формул (аргументи, функції, оператори та їх поєднання);
6. Основні операції аналізу даних;
7. Основні операції систематизації даних;
8. Основні операції візуалізації даних.
9. Консолідація (об'єднання) табличних даних з текстовими документами

Перелік тем для реферативних доповідей та самостійного опрацювання:

1. Масиви даних. Формули масивів даних.
2. Зведені таблиці та проміжні підсумки.
3. Аналіз даних за допомогою діаграм.
4. Безпека та захист даних інструментами табличного процесора.
5. Інструменти «Перевірка даних» та «Умовне форматування».

Контрольні питання

1. Як забезпечити читабельність таблиці?

2. Які правила розміщення графічних об'єктів у службовому документі?

Методичні рекомендації до підготовки. Перед виконанням створіть окрему робочу копію файлу. Дотримуйтеся послідовності операцій, використовуйте зрозумілі назви файлів і об'єктів, регулярно зберігайте результат. Після завершення перевірте відповідність роботи завданню, коректність відображення, відсутність зайвих персональних або службових даних і можливість відкриття файлу на іншому пристрої.

Тема 6. Використання мультимедійних засобів в професійній діяльності.

Для успішного виконання практичного завдання необхідно знати:

1. Основні правила оформлення текстової та графічної інформації
2. Структура та типові моделі мультимедійних презентацій
3. Елементи інтерфейсу редактора мультимедійних презентацій
4. Порядок створення активних та пасивних об'єктів презентації
5. Особливості роботи зі схемами, текстом та таблицями в середовищі редактора мультимедійних презентацій

6. Порядок та правила налаштування візуальних ефектів презентації

Перелік тем для реферативних доповідей та самостійного опрацювання:

1. Історія графічної культури. Дизайн і його тенденції.
2. Психологія сприйняття інфографіки
3. Створення інтерактивної презентації
4. Інтеграція об'єктів сумісних з нею застосунків.
5. Мультимедійне обладнання.

Контрольні питання

1. Які переваги надають шаблони?
2. Як захистити службовий бланк від випадкового редагування?

Методичні рекомендації до підготовки. Перед виконанням створіть окрему робочу копію файлу. Дотримуйтеся послідовності операцій, використовуйте зрозумілі назви файлів і об'єктів, регулярно зберігайте результат. Після завершення перевірте відповідність роботи завданню, коректність відображення, відсутність зайвих персональних або службових даних і можливість відкриття файлу на іншому пристрої.

Тема 7. Комп'ютерні мережі, інформаційна безпека, спільна робота в мережі.

Для успішного виконання практичного завдання необхідно знати:

1. Призначення комп'ютерних мереж
2. Види комп'ютерних мереж
3. Базові компоненти комп'ютерних мереж.
4. Технічне та програмне забезпечення комп'ютерних мереж.
5. Налаштування спільного використання ресурсів комп'ютера в мережі.
6. Робота з веб-браузером. Використання ресурсів мережі Інтернет у роботі фахівців-юристів.
7. Пошукові сервери.
8. Електронна пошта. Робота з поштовим клієнтом.
9. Використання в роботі правових інформаційно-пошукових систем www.nau.kiev.ua, www.ligazakon.ua, zakon.rada.gov.ua
10. Поняття захисту інформації.
11. Класифікація мережевих загроз та комп'ютерних вірусів.
12. Класифікація комп'ютерних злочинів. В якості реферативного завдання необхідно підготувати презентацію будьякого web-сервісу, додатку або web-проекту в ракурсі використання його, як інструменту для підвищення якості навчання за спеціальністю.

Контрольні питання

1. Які типи даних підтримує табличний процесор?
2. Коли доцільно використовувати абсолютне посилання?

Методичні рекомендації до підготовки. Перед виконанням створіть окрему робочу копію файлу. Дотримуйтеся послідовності операцій, використовуйте зрозумілі назви файлів і

об'єктів, регулярно зберігайте результат. Після завершення перевірте відповідність роботи завданню, коректність відображення, відсутність зайвих персональних або службових даних і можливість відкриття файлу на іншому пристрої.

Тема 8. Використання мережевих технологій в професійній діяльності.

Для успішного виконання практичного завдання необхідно знати:

1. Нейтралізація загроз
2. Захист доступу до пристроїв
3. Призначення адміністративних ролей
4. Розробка комплексної політики безпеки.

Перелік тем для реферативних доповідей та самостійного опрацювання:

1. Правила ідентифікації і аутентифікації;
2. Політики паролів;
3. Правила допустимого використання;
4. Політики віддаленого доступу;
5. Політики технічного обслуговування мережі;
6. Політики обробки інцидентів.

Контрольні питання

1. З яких елементів складається формула?
2. Як перевірити коректність автоматизованих розрахунків?

Методичні рекомендації до підготовки. Перед виконанням створіть окрему робочу копію файлу. Дотримуйтеся послідовності операцій, використовуйте зрозумілі назви файлів і об'єктів, регулярно зберігайте результат. Після завершення перевірте відповідність роботи завданню, коректність відображення, відсутність зайвих персональних або службових даних і можливість відкриття файлу на іншому пристрої.

ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Ряд питань навчальної дисципліни виносяться на самостійне опрацювання. Виконання самостійної роботи оцінюється окремо та є невід'ємною складовою успішного проходження курсу.

1. **Використання штучного інтелекту у діяльності правоохоронних органів**
Дослідження можливостей застосування AI для аналізу відеоспостереження, прогнозування правопорушень, автоматичного аналізу документів та ризиків порушення прав людини.

2. **Кіберзлочинність в Україні: сучасні загрози та методи протидії**
Аналіз найпоширеніших видів кіберзлочинів (фішинг, шахрайство, злам акаунтів), статистики та цифрових інструментів боротьби з ними.

3. **OSINT-технології у правоохоронній діяльності**
Дослідження методів збору інформації з відкритих джерел, аналіз соціальних мереж, геолокації та цифрових слідів під час розслідувань.

4. **Електронні докази у кримінальному провадженні**
Вивчення особливостей отримання, зберігання та використання цифрових доказів, проблем їх автентичності та процесуального оформлення.

5. **Безпека персональних даних у цифровому середовищі правоохоронних органів**
Аналіз загроз витоку інформації, способів захисту службових баз даних та відповідальності за порушення інформаційної безпеки.

6. **Соціальні мережі як інструмент виявлення правопорушень**
Дослідження використання Telegram, TikTok, Instagram та інших платформ для моніторингу протиправної діяльності й інформаційних загроз.

7. **Біометричні технології та їх використання в системі безпеки**
Аналіз технологій розпізнавання обличчя, відбитків пальців, голосу; оцінка ефективності та етичних ризиків їх застосування.

8. Інформаційні системи та електронний документообіг у правоохоронній сфері
Дослідження сучасних цифрових платформ, автоматизації обліку, переваг та проблем електронного документообігу.

9. Вплив дезінформації та фейкових новин на громадську безпеку
Аналіз механізмів поширення фейків, інформаційно-психологічних впливів та ролі правоохоронних органів у протидії дезінформації.

10. Цифровий профіль особи та проблеми приватності
Дослідження того, як цифрові сліди користувача можуть використовуватися під час розслідувань, а також правових меж такого використання.

Індивідуальні завдання

Індивідуальні завдання виконуються у вигляді рукописного есе обсягом до 5 сторінок за темою яка обирається з нижченаведеного переліку або індивідуальною темою погодженою з викладачем. При написанні есе доцільним буде скористатись порадами за посиланням: <https://zno.if.ua/?p=985>

Тематика есе:

1. Роль інформаційних систем у сучасній правоохоронній діяльності.
2. Цифрова трансформація правоохоронних органів України.
3. Поняття, структура та класифікація інформаційних систем правоохоронних органів.
4. Інформаційно-аналітичне забезпечення управлінських рішень у правоохоронній діяльності.
5. Використання інформаційних технологій для запобігання, виявлення та розкриття кримінальних правопорушень.
6. Єдина інформаційна система Міністерства внутрішніх справ України: призначення та основні складові.
7. Інформаційно-комунікаційна система «Інформаційний портал Національної поліції України».
8. Використання інформаційних підсистем Національної поліції України.
9. Інформаційні ресурси Державної кримінально-виконавчої служби України.
10. Інформаційне забезпечення діяльності установ виконання покарань і слідчих ізоляторів.
11. Єдиний реєстр засуджених та осіб, узятих під варту: призначення і порядок використання.
12. Інформаційні технології в діяльності органів пробації.
13. Використання електронного моніторингу в правоохоронній діяльності.
14. Системи відеоспостереження як засіб забезпечення правопорядку і безпеки.
15. Застосування систем розпізнавання облич у правоохоронній діяльності.
16. Використання біометричних інформаційних систем правоохоронними органами.
17. Автоматизовані дактилоскопічні інформаційні системи та їхнє значення для розкриття кримінальних правопорушень.
18. Інформаційні системи обліку вогнепальної зброї, боєприпасів і спеціальних засобів.
19. Геоінформаційні системи в діяльності правоохоронних органів.
20. Використання електронних карт для аналізу криміногенної обстановки.
21. Кримінальний аналіз із використанням сучасних інформаційних технологій.
22. Інтелектуальний аналіз даних у правоохоронній діяльності.
23. Технології Big Data у запобіганні та протидії злочинності.
24. Штучний інтелект у правоохоронній діяльності: можливості та ризики.
25. Використання машинного навчання для прогнозування кримінальних правопорушень.
26. Автоматизоване прийняття рішень у правоохоронній діяльності: правові та етичні проблеми.

27. Технології розпізнавання номерних знаків транспортних засобів.
28. Використання безпілотних літальних апаратів у правоохоронній діяльності.
29. Мобільні інформаційні технології в роботі правоохоронця.
30. Нагрудні відеореєстратори поліцейських: правові та організаційні засади використання.
31. Інформаційні технології під час документування кримінальних і адміністративних правопорушень.
32. Електронний документообіг у правоохоронних органах.
33. Електронні докази: поняття, види та особливості використання.
34. Збирання, збереження і дослідження цифрових доказів.
35. Використання відкритих джерел інформації в правоохоронній діяльності.
36. OSINT-технології як засіб інформаційно-аналітичної роботи правоохоронних органів.
37. Соціальні мережі як джерело інформації для правоохоронних органів.
38. Інформаційні технології у протидії кіберзлочинності.
39. Особливості виявлення та розслідування правопорушень у кіберпросторі.
40. Цифрова криміналістика: основні напрями та перспективи розвитку.
41. Кібербезпека інформаційних систем правоохоронних органів.
42. Захист службової інформації в інформаційних системах правоохоронних органів.
43. Захист персональних даних у правоохоронній діяльності.
44. Правові засади оброблення персональних даних правоохоронними органами.
45. Забезпечення конфіденційності, цілісності та доступності правоохоронної інформації.
46. Основні загрози інформаційній безпеці правоохоронних органів.
47. Соціальна інженерія як загроза інформаційним системам правоохоронних органів.
48. Організація розмежування доступу до службових інформаційних ресурсів.
49. Ідентифікація та автентифікація користувачів інформаційних систем.
50. Використання електронного підпису в діяльності правоохоронних органів.

Методи контролю та засоби діагностики якості навчання

Методи організації та здійснення навчально-пізнавальної діяльності:

- словесні методи: пояснення, розповідь, інструктаж, інформаційна і проблемна лекція, лекція-візуалізація, бесіда, робота з нормативно-правовими актами та службовою документацією;
- практичні методи: ситуаційні задачі, кейси, моделювання службових ситуацій, ситуаційно-рольові та навчально-тренувальні вправи;
- методи стимулювання і мотивації: дискусія, полеміка, обмін думками, аналіз практичного досвіду органів і установ виконання покарань.

Методи контролю

1. Поточний контроль: контроль активності здобувачів на семінарських і практичних заняттях, оцінювання самостійної роботи, тестування та модульний контроль.
2. Підсумковий контроль: здійснюється у формі заліку.

ПОРЯДОК ОЦІНЮВАННЯ (Денна/Заочна)

Оцінювання ваших досягнень відбувається за системою відображеною в таблиці

№ теми	Назви розділів і тем	Всього балів	Форма заняття	
			семінарське заняття (у т.ч. самостійна робота)	практичне заняття (у т.ч. самостійна робота)
1	2	3	4	5
2	Види та характеристика засобів інформаційно-комп'ютерної техніки	4/0		4/0
3	Адміністрування операційної системи	4/8	4/8	
4	Створення та обробка службових документів за допомогою текстового процесора.	12/20		12/20
5	Створення та обробка службових документів за допомогою табличного процесора.	12/0		12/0
6	Використання мультимедійних засобів в професійній діяльності	4/0		4/0
7	Комп'ютерні мережі, інформаційна безпека, спільна робота в мережі.	4/0	4/0	
8	Використання мережевих технологій в професійній діяльності	8/20		8/20
Разом		48/48	8/8	40/40
Індивідуальна робота		12		
Залік		40		
Всього		100 балів		

Робота на семінарських (практичних) заняттях оцінюється викладачем із розрахунку балів, зазначених у таблиці. Здобувач може виконати індивідуальну роботу, за визначеною формою та тематикою.

Підсумковий контроль з дисципліни здійснюється у вигляді заліку/екзамену, на якому можете отримати до 40 балів в залежності від повноти та обґрунтованості відповідей.

Якщо під час проходження курсу здобувач набрав 60 балів, він має право не складати залік/екзамен вдовольнившись підсумковою оцінкою відповідно до кількості набраних балів. Схема переведення балів у підсумкову оцінку наведена в таблиці

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою
90 – 100	A	відмінно
82-89	B	добре
75-81	C	
64-74	D	
60-63	E	задовільно
35-59	FX	незадовільно з можливістю повторного складання
0-34	F	незадовільно з обов'язковим повторним вивченням дисципліни

ПЕРЕЛІК ПИТАНЬ ДЛЯ ПІДСУМКОВОГО КОНТРОЛЮ.

1. Розкрийте поняття інформації та її значення у правоохоронній діяльності.
2. Охарактеризуйте основні властивості інформації, яка використовується правоохоронними органами.
3. Розкрийте поняття, ознаки та структуру інформаційної системи.
4. Наведіть класифікацію інформаційних систем, що використовуються у правоохоронній діяльності.
5. Охарактеризуйте поняття та основні види інформаційних технологій.
6. Визначте основні напрями застосування інформаційних технологій у правоохоронній діяльності.
7. Розкрийте поняття інформаційного забезпечення правоохоронної діяльності.
8. Охарактеризуйте основні етапи збирання, реєстрації, накопичення, оброблення, зберігання та використання інформації.
9. Визначте принципи функціонування інформаційних систем правоохоронних органів.
10. Охарактеризуйте нормативно-правові засади використання інформаційних систем у правоохоронній діяльності.
11. Розкрийте поняття та особливості правового режиму інформації.
12. Охарактеризуйте види інформації за порядком доступу.
13. Розкрийте поняття публічної інформації та порядок доступу до неї.
14. Визначте особливості роботи правоохоронних органів з інформацією з обмеженим доступом.
15. Охарактеризуйте вимоги до оброблення службової та конфіденційної інформації.
16. Розкрийте поняття персональних даних та визначте правові підстави їх оброблення.
17. Охарактеризуйте права суб'єкта персональних даних.
18. Визначте обов'язки правоохоронних органів під час оброблення персональних даних.
19. Розкрийте поняття бази даних та охарактеризуйте її основні складові.
20. Охарактеризуйте основні моделі організації баз даних.
21. Розкрийте поняття автоматизованого обліку та його значення у правоохоронній діяльності.
22. Охарактеризуйте призначення інформаційно-пошукових систем правоохоронних органів.
23. Визначте основні вимоги до формування інформаційно-пошукового запиту.
24. Охарактеризуйте способи пошуку, сортування, фільтрування та аналізу інформації в електронних базах даних.
25. Розкрийте поняття ідентифікації, автентифікації та авторизації користувачів інформаційних систем.
26. Охарактеризуйте порядок розмежування прав доступу до інформаційних ресурсів.
27. Розкрийте поняття електронного документа та назвіть його основні реквізити.
28. Охарактеризуйте юридичну силу електронного документа.
29. Визначте призначення та порядок використання кваліфікованого електронного підпису.
30. Охарактеризуйте особливості електронного документообігу в правоохоронних органах.
31. Розкрийте поняття електронного доказу та назвіть його основні види.
32. Охарактеризуйте порядок виявлення, фіксації, вилучення та збереження електронних доказів.
33. Визначте основні вимоги до забезпечення цілісності й автентичності електронних доказів.
34. Охарактеризуйте поняття цифрової криміналістики та її основні завдання.

35. Розкрийте поняття метаданих та їх значення під час дослідження електронних доказів.
36. Охарактеризуйте призначення Єдиної інформаційної системи Міністерства внутрішніх справ України.
37. Визначте основні складові та завдання інформаційних ресурсів Національної поліції України.
38. Охарактеризуйте призначення інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України».
39. Розкрийте призначення автоматизованих дактилоскопічних інформаційних систем.
40. Охарактеризуйте можливості використання біометричних інформаційних систем у правоохоронній діяльності.
41. Визначте призначення систем автоматизованого розпізнавання облич і номерних знаків транспортних засобів.
42. Охарактеризуйте інформаційні системи та електронні обліки Державної кримінально-виконавчої служби України.
43. Розкрийте призначення Єдиного реєстру засуджених та осіб, узятих під варту.
44. Охарактеризуйте особливості інформаційного забезпечення діяльності установ виконання покарань і слідчих ізоляторів.
45. Визначте основні напрями застосування інформаційних технологій у діяльності органів пробації.
46. Охарактеризуйте порядок міжвідомчого інформаційного обміну у правоохоронній сфері.
47. Розкрийте призначення державних електронних реєстрів та особливості їх використання правоохоронними органами.
48. Охарактеризуйте інформаційні ресурси Інтерполу та напрями їх використання правоохоронними органами України.
49. Визначте основні можливості інформаційної взаємодії правоохоронних органів України з Європолем.
50. Розкрийте поняття OSINT та охарактеризуйте основні напрями використання відкритих джерел інформації.
51. Охарактеризуйте особливості пошуку, перевірки та оцінювання інформації з відкритих джерел.
52. Визначте можливості використання соціальних мереж у правоохоронній діяльності.
53. Розкрийте поняття геоінформаційної системи та охарактеризуйте напрями її застосування правоохоронними органами.
54. Охарактеризуйте використання систем відеоспостереження, нагрудних відеореєстраторів і технологій відеоаналітики.
55. Розкрийте можливості застосування штучного інтелекту та технологій Big Data у правоохоронній діяльності.
56. Охарактеризуйте правові, організаційні та етичні ризики автоматизованого прийняття рішень у правоохоронній сфері.
57. Розкрийте поняття інформаційної та кібербезпеки правоохоронних органів.
58. Охарактеризуйте основні загрози, вразливості та ризики для інформаційних систем правоохоронних органів.
59. Визначте організаційні, програмні й технічні заходи захисту правоохоронної інформації.
- 60.** Охарактеризуйте перспективні напрями розвитку інформаційних систем і технологій у правоохоронній діяльності.

ПОЛІТИКА АКАДЕМІЧНОЇ ДОБРОЧЕСНОСТІ

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу (принципи описані у Законі України «Про академічну доброчесність» від 18 грудня 2025 року №4742ІХ (<https://zakon.rada.gov.ua/laws/show/4742-20#Text>) та Кодексі академічної доброчесності Пенітенціарної академії України від 30 березня 2026 року №132/ОД (<https://pau.edu.ua/higher-education-quality-assurance-sector/academic-integrity/>).

Списування під час підсумкового контролю, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

РЕКОМЕНДОВАНА ЛІТЕРАТУРА:

Основна:

1. A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement: Workforce Development / A. K. Nag et al. International Journal of Smart Education and Urban Society. 2022. Vol. 13, no. 1. P. 1–14. URL: <https://www.igi-global.com/article/a-conceptual-learning-framework-of-cybersecurity-education-for-military-and-law-enforcement/309953> (date of access: 17.08.2026).
2. Koteliukh M. Cooperation of Law Enforcement Agencies with Other Departments in the Fight Against Criminal Offences at Critical Infrastructure. Journal of Discipline and Security. 2025. P. 110–121. URL: <https://dialnet.unirioja.es/descarga/articulo/10092804.pdf> (date of access: 17.08.2026).
3. Hoofnagle C. J., Richard III G. G. Cybersecurity in Context: Technology, Policy, and Law. Hoboken : John Wiley & Sons, Inc., 2025. URL: <https://repository.lsu.edu/facultybooks/602/> (date of access: 17.08.2026).
4. Pokryshen D. Artificial Intelligence in Education: Cases of Using ChatGPT 3.5. Фізико-математична освіта. 2024. Т. 39, № 1. С. 56–63. DOI: <https://doi.org/10.31110/fmo2024.v39i1-08>.
5. Davydenko V. The Role of Operational Units of the National Police in Preventing Cybercrime in the Context of Economic Globalisation and Existential Challenges. Baltic Journal of Economic Studies. 2025. Vol. 11, no. 3. P. 84–91. URL: <http://www.baltijapublishing.lv/index.php/issue/article/download/2967/2944/> (date of access: 17.08.2026).
6. Гончарова І. П. Кібербезпека в цифровому освітньому середовищі закладів професійної освіти : електронний навчальний курс. Біла Церква : БІНПО ДЗВО «УМО» НАПН України, 2022. 80 с.
7. Ліпкан В. А. Кібербезпека та інформаційний захист : підручник. Київ : Юрінком Інтер, 2022. 432 с.
8. Кривоніс О. І. Кібербезпека: правові та організаційні аспекти : навч. посіб. Київ : Центр навчальної літератури, 2022. 310 с.
9. Горулько В. В. Основні напрями удосконалення законодавства України з інформаційної безпеки в умовах війни. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 90. С. 364–369.
10. Покришень Д. А. Цифровізація в системі пробації: сучасні технології та інноваційні підходи до управління процесами. Пробація: 10 років змін та досягнень : колективна

монографія / за ред. С. К. Гречанюка. Чернігів : Пенітенціарна академія України, 2025. С. 187–200.

Допоміжна:

1. Антонюк Н. М. Використання штучного інтелекту у забезпеченні кібербезпеки. Інформаційна безпека України. 2023. № 2. С. 39–47.
2. Григоренко О. Ю. Алгоритми реагування на кіберінциденти в контексті державної безпеки. Вісник Національної академії правових наук України. 2023. Т. 31, № 2. С. 97–108.
3. Григоренко О. Ю. Проблеми забезпечення кібербезпеки та захисту персональних даних в умовах цифровізації. Вісник Національної академії правових наук України. 2023. Т. 31, № 1. С. 84–95.
4. Збірник завдань з Microsoft Office 2010 : посібник для вивчення та практичної роботи / Д. А. Покришень, Ю. О. Крепкий, І. Й. Сподаренко та ін. Чернігів : ТОВ НВП «Інтерсервіс», 2013. 136 с. Рекомендовано листом Міністерства освіти і науки України від 11.11.2013 р. № 1/9-792.
5. Ліпкан В. А. Штучний інтелект у кібербезпеці: перспективи та загрози. Київ : Юрінком Інтер, 2023. 410 с.
6. Ткаченко О. В. Виклики для кібербезпеки в умовах цифрової трансформації. Юридична Україна. 2022. № 5. С. 18–27.

Інформаційні ресурси

1. Архітектура комп'ютера. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Архітектура_комп'ютера (дата звернення: 17.08.2026).
2. Базові завдання зі створення презентації PowerPoint. Служба підтримки Microsoft. URL: <https://support.office.com/uk-ua/article/97-PowerPoint-efbbc1cd-c5f1-4264-b48e-c8a7b0334e36> (дата звернення: 17.08.2026).
3. Будова та принцип роботи комп'ютера. Програмування по-українськи. URL: <http://programming.in.ua/other-files/hardware/294-structure-and-working-process-of-computers.html> (дата звернення: 17.08.2026).
4. Покришень Д. А. Цифровізація освіти. Розвиток творчої дитини. URL: <https://tvorchistd.blogspot.com> (дата звернення: 17.08.2026).
5. Марченко А. В. Архітектура персонального комп'ютера. Навчальні ресурси Сумського державного університету. URL: http://elearning.sumdu.edu.ua/free_content/lectured:1a259358378153792bb8645df287e86d790fc40d/20150323193201/content-20150323193201.pdf (дата звернення: 17.08.2026).
6. Основні завдання у програмі Excel 2013. Служба підтримки Microsoft. URL: <https://support.office.com/uk-ua/article/Excel-2013-363600c5-55be-4d6e-82cf-b0a41e294054> (дата звернення: 17.08.2026).
7. Основні прийоми створення презентацій. Презентації PowerPoint. URL: <http://teachua.com/uroky-powerpoint/659-osnovni-priyomy-stvorennja-prezentaci> (дата звернення: 17.08.2026).
8. Основні режими роботи текстового процесора Word. Навчальні матеріали онлайн. URL: http://pidruchniki.com/15941024/informatika/osnovni_rezhimi_roboti_tekstovogo_protseora_word (дата звернення: 17.08.2026).
9. Поняття про архітектуру і принципи функціонування комп'ютера. Школа сучасних знань. 2013. URL: http://www.zhu.edu.ua/mk_school/mod/page/view.php?id=5551&lang=ru (дата звернення: 17.08.2026).

10. Різновиди програмного забезпечення. Електронний підручник з інформатики. URL: http://informatic-10.at.ua/index/riznovidi_programnogo_zabezpechennja/0-51 (дата звернення: 17.08.2026).

11. Технічна підтримка Microsoft. Microsoft. URL: <https://support.microsoft.com/uk-ua> (дата звернення: 17.08.2026).