МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

Кафедра інформаційних технологій

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОРГАНІЗАЦІЯ ТА ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ОБ'ЄКТІВ, ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Назва освітньо-професійної програми	Правоохоронна діяльність
Рівень вищої освіти	другий (магістерський)
Галузь знань	26 Цивільна безпека
Спеціальність	262 Правоохоронна діяльність
Вид навчальної дисципліни	обов'язкова
Мова викладання	українська
Рік навчання	перший (денна, заочна)

2024

ЗАТВЕРДЖЕНО
Науково-методичною радою
Дніпровського державного
університету внутрішніх справ

протокол від 30.08.2024 № 17
протокол від 02.09.2024 № 18

СХВАЛЕНО
Вченою радою Навчально-
наукового інституту права та
інноваційної освіти
протокол від 16.08.2024 №12

ПОГОДЖЕНО
Гарант освітньої програми «Правоохоронна діяльність»

Володимир ШАБЛИСТИЙ

Розглянуто на засіданні кафедри інформаційних технологій протокол від 15.08.2024 № 1

Організація та технічні засоби захисту об’єктів, інформації від несанкціонованого доступу. Робоча програма навчальної дисципліни. Дніпро: Дніпровський державний університет внутрішніх справ, 2024 рік. 16 с.

РОЗРОБНИК:
Професор кафедри інформаційних технологій Дніпровського державного університету внутрішніх справ, доктор технічних наук, професор Дісковський Олександр Андрійович.

РЕЦЕНЗЕНТИ:
1. Старший науковий співробітник науково-дослідної лабораторії з підготовки військ, Київський інститут національної гвардії України, доктор юридичних наук, доцент Титаренко Олексій Олексійович;
2. Доцент кафедри системного аналізу та управління Національного технічного університету «Дніпровська політехніка», кандидат технічних наук, доцент Станіна Ольга Дмитрівна.

Лист оновлення та перезатвердження
робочої програми навчальної дисципліни
(додаток 1 до Робочої програми навчальної дисципліни)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	Характеристика навчальної дисципліни	
	денна форма здобуття вищої освіти	заочна форма здобуття вищої освіти
Кількість кредитів ЄКТС	3	3
Загальна кількість годин	90	90
Рік підготовки	1	1
Семестр	2	2
Лекції	4	4
Семінарські	-	2
Практичні	26	2
Самостійна робота	60	82
Індивідуальні завдання (курсова робота)	-	-
Підсумковий семестровий контроль	залік	залік

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Метою вивчення навчальної дисципліни «Організація та технічні засоби захисту об’єктів, інформації від несанкціонованого доступу» є формування у здобувачів вищої освіти знань основних видів інформаційних загроз та вміння впроваджувати новітні методи і заходи та побудови ефективної технології захисту інформації. Використовувати основні теоретичні положення і методи, формування умінь і прищеплення навичок застосування теоретичних знань для вирішення прикладних завдань, а також розвиток нових підходів до забезпечення інформаційної безпеки в сфері економіки. Використовувати комплекс нормативно-правових актів, що регулюють діяльність людей.

Очікувані результати навчання передбачають, що в результаті опанування навчальної дисципліни здобувач вищої освіти матиме ґрунтовні знання та практичні навички у сфері інформаційної безпеки в контексті правоохоронної діяльності. Здобувач повинен знати теоретичні засади організації та технічного забезпечення захисту об’єктів і інформації від несанкціонованого доступу; сучасні інструменти й технології, що застосовуються для захисту інформаційних ресурсів; нормативно-правову базу, яка регулює питання інформаційної безпеки у правоохоронній сфері; специфіку загроз в інформаційному середовищі, а також методи їх виявлення й запобігання; основи використання технічних засобів для захисту даних. Водночас, здобувач має вміти ефективно застосовувати аналітичні інструменти для збору, обробки та інтерпретації інформації; виявляти і аналізувати потенційні правопорушення й загрози за допомогою інформаційно-аналітичних методів, а також своєчасно

реагувати на ризики, забезпечуючи надійний захист інформаційного простору правоохоронної діяльності.

Вивчення дисципліни забезпечує формування компетентностей за освітньою програмою:

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:

ЗК1 – здатність до абстрактного мислення, аналізу та синтезу.

ЗК2 – здатність застосовувати знання у практичних ситуаціях.

ЗК4 – здатність проведення досліджень на відповідному рівні.

ЗК8 – здатність приймати обґрунтовані рішення.

ЗК10 – здатність оцінювати та забезпечувати якість виконуваних робіт.

Спеціальні компетентності:

СК2 – здатність забезпечувати законність та правопорядок, безпеку особистості, суспільства, держави в межах виконання своїх посадових обов'язків.

СК3 – здатність виявляти та аналізувати причини та умови, що сприяють вчиненню кримінальних та адміністративних правопорушень, вживати заходи для їх усунення.

СК10 – здатність аналізувати, оцінювати й застосовувати сучасні інформаційні технології під час рішення професійних завдань.

СК12 – 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.

СК16 – здатність знаходити, перевіряти й аналізувати інформацію з відкритих джерел та ухвалювати обґрунтовані рішення у сфері безпеки та розслідувань.

Пререквізити та постреквізити дисципліни:

Пререквізити: «Інформаційні технології», «Інформаційно-аналітичне забезпечення правоохоронної діяльності».

Постреквізити: «Виробнича практика».

Здобувачі вищої освіти повинні продемонструвати такі **результати навчання**:

РН4 – узагальнювати практичні результати роботи і пропонувати нові

рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.

РН5 – аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення.

РН7 – оцінювати та забезпечувати якість виконуваних робіт у процесі управління правоохоронним підрозділом в різних умовах обстановки, а також розробляти відповідні аналітичні та інформаційні матеріали, робити усні та письмові звіти та доповіді.

РН9 – використовувати у професійній діяльності сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення.

РН10 – 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.

ПРН13 – відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію.

ПРН16 – використовувати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань

ПРН20 – вміти працювати із джерелами відкритої інформації з метою ухвалення обґрунтованих рішень у сфері правоохоронної діяльності.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМА 1. ОСНОВНІ ПОНЯТТЯ ЗАХИСТУ ОБ'ЄКТІВ. ІНФОРМАЦІЙНА БЕЗПЕКА.

Поняття та загальна класифікація інформаційної безпеки ресурсів. Види інформаційних ресурсів. Національний реєстр електронних інформаційних ресурсів. Загрози об'єктам та інформаційним ресурсам. Встановлення режим доступу до інформації та визначення ступеня секретності інформації. Становлення інституту державних експертів з питань таємниць, функції та повноваження державних експертів з питань таємниць в сучасній Україні. Організація захисту об'єктів та інформаційних ресурсів.

ТЕМА 2. МЕТОДИКИ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Аналіз усіх загроз, які діють на інформаційну систему, і вразливостей, через які можлива реалізація загроз. Побудова моделі загроз і вразливостей, актуальних для інформаційної системи компанії. На основі отриманої моделі проводиться аналіз ймовірності реалізації загроз інформаційній безпеці на кожен ресурс та проводиться розрахунок ризиків. Вибір ефективних і

економічно виправданих захисних заходів і засобів для зменшення або нейтралізації ризиків.

ТЕМА 3. ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ СИСТЕМ.

Організація внутрішньо-об'єктного режиму і охорони приміщень. Фізичний захист об'єктів ІБ. Організація режиму секретності в установах і на підприємствах. Виявлення атак і розпізнавання вторгнень. Локалізація та усунення наслідків. Ідентифікація нападника (або джерела розповсюдження шкідливих програм). Оцінка і подальший аналіз процесу нападу. Регламентація виробничої діяльності і взаємин виконавців на нормативній основі. Організаційні заходи для створення надійного механізму захисту інформації, та запобігання несанкціонованого використання конфіденційних відомостей. Організація роботи з співробітниками, навчання правилам роботи з конфіденційною інформацією, ознайомлення з мірою відповідальності за порушенням правил захисту інформації.

ТЕМА 4. ЗАХИСТ ДОКУМЕНТІВ MS OFFICE, PDF ТА ІНШИХ.

Загальні відомості про захист документів. Захист документів MS Word, MS Excel. Захист pdf документів засобами програми Adobe Acrobat. Використання програми iLove PDF Desktop. Безпека документів Google Docs. Архивація документів. Захист архівів. Програми архівації.

ТЕМА 5. КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ.

Основні положення та визначення криптографії. Традиційні і сучасні криптосистеми. Методи шифрування даних. Характеристика алгоритмів шифрування. Основні криптографічні алгоритми. Абонентське і пакетне шифрування. Взаємне підтвердження автентичності (аутентифікація) абонентів і об'єктів мережі. Забезпечення цілісності інформації на основі електронного цифрового підпису.

ТЕМА 6. АНТИВІРУСНИЙ ЗАХИСТ ДАНИХ.

Поняття комп’ютерного вірусу. Класифікація комп’ютерних вірусів. Структура вірусів. Деструктивні дії комп’ютерних вірусів. Розповсюдження комп’ютерних вірусів. Попередження заражень комп'ютерними вірусами. Програмні засоби захисту від комп’ютерних вірусів. Дія користувача при виявленні факту зараження комп'ютерним вірусом.

ТЕМА 7. ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ.

Визначення персональних даних. Види персональних даних. Законодавство про персональні дані. Законодавство ЄС про захист персональних даних. Наслідки крадіжок персональних даних. Попередження

крадіжки та розповсюдження персональних даних. Засоби захисту персональних даних. Організаційні, правові та програмні методи захисту персональних даних. Захист персональних даних під час використання браузерів. Поняття попередження крадіжки особистості (identity theft).

4. СТРУКТУРА ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ДЕННА ФОРМА НАВЧАННЯ

Теми та план лекційних занять

Назва теми лекційного заняття	План лекційного заняття	Кількість годин
Тема 1. Основні поняття захисту об’єктів. Інформаційна безпека.	1. Поняття та загальна класифікація інформаційної безпеки. 2. Загрози інформаційній безпеці. Встановлення режим доступу до інформації та визначення ступеня секретності інформації. 3. Організація захисту об’єктів та інформаційних ресурсів. Інформаційна безпека.	4

Теми практичних занять

Назва теми практичного заняття	Кількість годин
Тема 1. Основні поняття захисту об’єктів. Інформаційна безпека.	4
Тема 2. Методики оцінки ризиків інформаційної безпеки.	4
Тема 3. Організаційні заходи забезпечення безпеки комп'ютерних інформаційних систем.	4
Тема 4. Захист документів MS Office, pdf та інших.	4
Тема 5. Криптографічні методи захисту інформації.	4
Тема 6. Антивірусний захист даних.	4
Тема 7. Захист персональних даних.	2

Теми для самостійної роботи

Назва теми самостійної роботи	Кількість годин
Тема 1. Основні поняття захисту об’єктів. Інформаційна безпека.	12
Тема 2. Методики оцінки ризиків інформаційної безпеки.	8
Тема 3. Організаційні заходи забезпечення безпеки комп'ютерних інформаційних систем.	12
Тема 4. Захист документів MS Office, pdf та інших.	8
Тема 5. Криптографічні методи захисту інформації.	8
Тема 6. Антивірусний захист даних.	8
Тема 7. Захист персональних даних.	4

ЗАОЧНА ФОРМА НАВЧАННЯ

Теми та план лекційних занять

Назва теми лекційного заняття	План лекційного заняття	Кількість годин
Тема 1. Основні поняття захисту об’єктів. Інформаційна безпека.	1. Поняття та загальна класифікація інформаційної безпеки. 2. Загрози інформаційній безпеці. Встановлення режим доступу до інформації та визначення ступеня секретності інформації. 3. Організація захисту об’єктів та інформаційних ресурсів. Інформаційна безпека.	4

Теми практичних занять

Назва теми практичного заняття	Кількість годин
Тема 2. Методики оцінки ризиків інформаційної безпеки.	2

Теми семінарських занять

Назва теми семінарського заняття	Кількість годин
Тема 7. Захист персональних даних.	2

Теми для самостійної роботи

Назва теми самостійної роботи	Кількість годин
Тема 1. Основні поняття захисту об’єктів. Інформаційна безпека.	12
Тема 2. Методики оцінки ризиків інформаційної безпеки.	12
Тема 3. Організаційні заходи забезпечення безпеки комп'ютерних інформаційних систем.	12
Тема 4. Захист документів MS Office, pdf та інших.	12
Тема 5. Криптографічні методи захисту інформації.	12
Тема 6. Антивірусний захист даних.	12
Тема 7. Захист персональних даних.	10

5. ПЕРЕЛІК ПИТАНЬ ТА ЗАВДАНЬ, ЩО ВИНОСЯТЬСЯ НА ПІДСУМКОВИЙ КОНТРОЛЬ

1. Що таке несанкціонований доступ та які ризики він несе для інформаційної безпеки?
2. Які існують основні методи захисту об'єктів від несанкціонованого доступу?
3. Як впровадження багаторівневого доступу сприяє захисту інформації?
4. Які технічні засоби використовуються для захисту інформаційних систем?
5. Як працює криптографія для захисту конфіденційної інформації?
6. Що таке система контролю доступу (СКД) і як вона допомагає захисту об'єктів?

7. Які особливості має захист від внутрішніх загроз у інформаційній безпеці?
8. Як захистити інформацію в локальних мережах від несанкціонованого доступу?
9. Які заходи можна вжити для захисту фізичних об'єктів (серверних кімнат, дата-центрів)?
10. Як впливає біометрична аутентифікація на підвищення безпеки доступу?
11. Які є основні методи захисту інформації при передачі по мережі?
12. Які вимоги до технічних засобів захисту інформації регулюють законодавчі акти?
13. Як працює система двофакторної аутентифікації і чому вона є ефективною?
14. Які типи брандмауерів існують та які функції вони виконують?
15. Що таке політика інформаційної безпеки і чому вона важлива?
16. Які є основні технології виявлення вторгнень (IDS/IPS) і як вони працюють?
17. Які ризики виникають при використанні хмарних сервісів для зберігання даних?
18. Як організувати захист об’єктів з використанням відеоспостереження?
19. Які функції виконує мережевий екран (файрвол) для захисту інформаційних ресурсів?
20. Що таке шифрування даних і як воно забезпечує захист інформації?
21. Як здійснюється захист від DDoS-атак на інформаційні ресурси?
22. Які технології використовуються для забезпечення безпечної віддаленої роботи?
23. Які є етапи впровадження системи захисту об'єкта від несанкціонованого доступу?
24. Як працюють системи відеоаналітики для забезпечення безпеки об’єктів?
25. Які є методи захисту бездротових мереж від несанкціонованого доступу?
26. Як побудувати надійну систему резервного копіювання для захисту даних?
27. Які стандарти та протоколи забезпечують безпеку передачі даних у мережах?
28. Що таке токенізація даних та як вона сприяє захисту конфіденційної інформації?
29. Як захистити інформацію при використанні мобільних пристроїв у корпоративній мережі?
30. Які методи управління правами доступу застосовуються для захисту інформації в організації?

6. КРИТЕРІЇ ТА ЗАСОБИ ОЦІНЮВАННЯ УСПІШНОСТІ НАВЧАННЯ

ДЛЯ ДЕННОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		**Підсумковий контроль**
Аудиторна робота	Самостійна робота	Залік (З)
≤ 40	≤ 10	
≤ 50		≤ 50
Підсумкова оцінка у випадку заліку (П) = ПК + З ≤ 100		

ДЛЯ ЗАОЧНОЇ ФОРМИ НАВЧАННЯ		
Поточний контроль (ПК)		**Підсумковий контроль**
Аудиторна робота	Самостійна робота	Залік (З)
≤ 20	≤ 30	
≤ 50		≤ 50
Підсумкова оцінка у випадку заліку (П) = ПК + З ≤ 100		

Критерієм успішного проходження здобувачем підсумкового оцінювання може бути досягнення ним мінімальних порогових рівнів оцінок за кожним запланованим результатом навчання навчальної дисципліни.

Мінімальний пороговий рівень оцінки визначається за допомогою якісних критеріїв і трансформується в мінімальну позитивну оцінку використовуваної числової (рейтингової) шкали.

Здобувач допускається до складання підсумкового контролю, якщо ним виконані всі передбачені РПНД поточні завдання та сума балів поточного контролю не менше ніж 34. Якщо сума балів поточного контролю менше ніж 34, здобувач не допускається до підсумкового контролю і зобов'язаний доопрацювати завдання та набрати необхідну кількість балів.

За результатами аудиторної роботи здобувач денної форми навчання має отримати максимальну кількість 40 балів (кожне заняття оцінюється за п'ятибальною шкалою); за результатами самостійної роботи – 10 балів. Таким чином бали за поточний контроль (34-50 балів).

За результатами аудиторної роботи здобувач заочної форми навчання має отримати максимальну кількість 20 балів (кожне заняття оцінюється за п'ятибальною шкалою); за результатами самостійної роботи – 30 балів. Таким чином бали за поточний контроль (34-50 балів).

Розрахунок підсумкової оцінки з навчальної дисципліни «Організація та технічні засоби захисту об'єктів, інформації від несанкціонованого доступу» здійснюється відповідно до формули:

$$\mathbf{П=ПК+З\leq 100,}$$

де ПК – бали за поточний контроль (34-50 балів),

З – бали за результатами складання заліку

Критерії оцінювання аудиторної роботи здобувачів вищої освіти (денна та заочна форми навчання)

БАЛИ	ПОЯСНЕННЯ
5	**Високий рівень** компетентностей. Питання по практичним роботам, винесені на розгляд, засвоєні у повному обсязі; на високому рівні сформовані необхідні практичні навички та вміння; всі навчальні завдання, передбачені планом заняття, виконані в повному обсязі. Під час заняття продемонстрована стабільна активність та ініціативність. Відповіді на теоретичні питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань ґрунтується на глибокому знанні навчального матеріалу дисципліни.
4	**Невисокий рівень** компетентностей. Питання по практичним роботам, винесені на розгляд, засвоєні у повному обсязі; в основному сформовані необхідні практичні навички та вміння; всі передбачені планом заняття навчальні завдання виконані в повному обсязі з неістотними неточностями. Під час заняття продемонстрована ініціативність. Відповіді на питання, розв'язання практичних завдань, висловлення власної думки стосовно дискусійних питань переважно ґрунтується на знанні навчального матеріалу дисципліни.
3	**Достатній рівень** компетентностей. Питання по практичним роботам, винесені на розгляд, у цілому засвоєні; практичні навички та вміння мають поверхневий характер, потребують подальшого напрацювання та закріплення; навчальні завдання, передбачені планом заняття, виконані, деякі види завдань виконані з помилками.
2	**Недостатній рівень** компетентностей. Питання по практичним роботам, винесені на розгляд, **засвоєні частково**, **прогалини** у знаннях **не носять істотного характеру**; практичні навички та вміння **сформовані недостатньо**; **більшість** навчальних завдань **виконано, деякі** з виконаних завдань **містять істотні помилки,** які потребують подальшого усунення.
1	**Мінімальний рівень** компетентностей. Здобувач не готовий до заняття, не знає більшої частини програмного матеріалу, з труднощами виконує завдання, невпевнено відтворює терміни і поняття, що розглядалися під час заняття, допускає змістовні помилки, не володіє відповідними вміннями і навичками, необхідними для розв'язання професійних завдань.
0	**Незадовільний рівень** компетентностей. Відсутність на занятті.

Для навчальної дисципліни «Організація та технічні засоби захисту об'єктів, інформації від несанкціонованого доступу» засобами діагностики знань (успішності навчання) виступають: стандартизовані тести, тези, есе, презентації результатів виконаних завдань та досліджень, презентації та виступи на наукових заходах, інші види індивідуальних та групових завдань.

Критерії оцінювання самостійної роботи (денна форма навчання)

Пропонується наступне оцінювання самостійної роботи здобувачів вищої освіти: виконання одного завдання, обраного здобувачем за погодженням із викладачем:

1. Написання та участь у конкурсі творчих та/або наукових робіт серед здобувачів (МОН, ДДУВС): написання робіт, есе, доповідей, творчих публікацій, візуалізацій або відеороликів — **10 балів**.

2. Підготовка презентації-доповіді для участі в роботі наукового студентського гуртка кафедри (необхідно надати презентацію та фото виступу) — **10 балів**.

3. Підготовка тез доповіді на міжнародну або всеукраїнську науково-практичну конференцію за умови надання скриншоту перевірки на плагіат із результатом не менше ніж 70 % оригінального тексту. Тези мають бути підготовлені відповідно до «Методичних вказівок з написання тез» — **10 балів**.

4. Отримання сертифіката після проходження онлайн-курсу **«Аналітик із кібербезпеки»** на освітній платформі **Дія: Освіта** (https://osvita.diia.gov.ua/courses/cybersecurity-analyst) — **10 балів**.

5. Підготовка презентації в редакторі Google Презентації (завантаження та надання посилання в коментарях у СУДН «Moodle») за темою зі списку у додатковому файлі «Методичні вказівки до виконання презентації у редакторі Google Презентації» — **10 балів**.

6. Виконання індивідуальної роботи згідно із завданням викладача (до **10 балів**: кросворд — **3 бали**, реферат — **3 бали**, есе — **4 бали**).

7. Проходження тесту з самостійної роботи (40 питань) — **10 балів**.

Критерії оцінювання самостійної роботи (заочна форма навчання)

Пропонується наступне оцінювання самостійної роботи здобувачів вищої освіти: виконання одного завдання, обраного здобувачем за погодженням із викладачем, для отримання максимальної кількості балів — **30**:

1. Написання та участь у конкурсі творчих та/або наукових робіт серед здобувачів (МОН, ДДУВС): написання робіт, есе, доповідей, творчих публікацій, візуалізацій або відеороликів — **30 балів**.

2. Підготовка презентації-доповіді для участі в роботі наукового студентського гуртка кафедри (необхідно надати презентацію та фото виступу) — **10 балів**.

3. Підготовка тез доповіді на міжнародну або всеукраїнську науково-практичну конференцію за умови надання скриншоту (PrintScreen) перевірки на плагіат із результатом не менше ніж 70 % оригінального тексту. Тези мають бути підготовлені відповідно до «Методичних вказівок з написання тез» — **10 балів**.

4. Отримання сертифіката після проходження онлайн-тесту **«Цифрограм 2.0 для громадян»** на освітній платформі **Дія: Освіта** (https://osvita.diia.gov.ua/digigram) — **30 балів**.

5. Підготовка презентації в редакторі Google Презентації (завантаження та надання посилання в коментарях у СУДН «Moodle») за темою зі списку у

додатковому файлі «Методичні вказівки до виконання презентації у редакторі Google Презентації» — **10 балів**.

6. Проходження тесту із самостійної роботи (40 питань) — **30 балів**.

Шкала оцінювання: національна та ECTS

Оцінка в балах	Оцінка за національною шкалою		Оцінка за шкалою ECTS	
	Залік	Екзамен/ диференційований залік	Оцінка	Пояснення
90-100	зараховано	Відмінно	A	«**Відмінно**» - теоретичний зміст курсу засвоєний у повному обсязі; сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані в повному обсязі.
83-89		Добре	B	«**Дуже добре**» - теоретичний зміст курсу засвоєний в повному обсязі; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання більшості з них оцінена кількістю балів, близько до максимальної.
75-82			C	«**Добре**» - теоретичний зміст курсу засвоєний цілком; в основному сформовані практичні навички роботи із засвоєним матеріалом; всі навчальні завдання, передбачені РПНД, виконані, якість виконання жодного з них не оцінена мінімальною кількістю балів, деякі види завдань виконані з помилками.
68-74		Задовільно	D	«**Задовільно**» - теоретичний зміст курсу засвоєний не повністю; але прогалини не носять істотного характеру; в основному сформовані необхідні практичні навички роботи із засвоєним матеріалом; більшість передбачених РПНД навчальних завдань виконано, деякі з виконаних завдань містять помилки.
60-67			E	«**Достатньо**» - теоретичний зміст курсу засвоєний частково; не сформовано деякі практичні навички роботи; частина передбачених РПНД навчальних завдань не виконані або якість виконання деяких з них оцінено числом балів, близьким до мінімального.
35-59	не зараховано	Не задовільно	FX	«**Умовно незадовільно**» - теоретичний зміст курсу засвоєний частково; не сформовані необхідні практичні навички роботи; більшість навчальних завдань не виконано або якість їх виконання оцінено кількістю балів, близько до мінімальної; при додатковій самостійній роботі над матеріалом курсу можливе підвищення якості виконання навчальних завдань (з можливістю

				повторного складання).
1-34			F	«**Безумовно незадовільно**» - теоретичний зміст курсу не засвоєний; не сформовані необхідні практичні навички роботи; всі виконані навчальні завдання містять грубі помилки або не виконані взагалі; додаткова самостійна робота над матеріалом курсу не призведе до значного підвищення якості виконання навчальних завдань.

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧЕНО НАВЧАЛЬНОЮ ДИСЦИПЛІНОЮ

1. Комп'ютерна техніка, відповідне програмне забезпечення.
2. Наявність доступу до Інтернет.
3. Мультимедійне обладнання.

8. ІНФОРМАЦІЙНЕ ТА МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ (рекомендовані джерела інформації)

Основні нормативні акти:

- закони:

1. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

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

- постанови, інші рішення, роз'яснення суддів (Конституційного, Верховного):

1. Питання забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних система: Постанова КМУ від 8 лютого 2021 року № 92. URL: https://zakon.rada.gov.ua/laws/show/92-2021-%D0%BF#Text;

Підручники:

1. Інформаційні системи та технології: підруч. / кол. авт. ; за заг. ред. доктора технічних наук, проф. В.Б. Вишні. Дніпро: Дніпроп. держ. ун-т внутр. справ, 2021. 280 с. URI: https://er.dduvs.in.ua/handle/123456789/7110;

2. Інформаційні технології: підруч. / В.Б. Вишня, К.Ю. Ісмайлов, І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков. Дніпро: Дніп-роп. держ. ун-т внутр.справ, 2021. 492с. URI: http://er.dduvs.in.ua/handle/123456789/6820

Монографії та інші наукові видання:

1. Благута Р. І., Мовчан А. В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: Львівський державний університет внутрішніх справ, 2020. 256 с.
2. Габорець О. А., Лунгол О. М. Основи кібербезпеки: методичні рекомендації до практичних занять. Кропивницький: Book Creator, 2023. 76 с. URL:https://read.bookcreator.com/fQ6a2RCUdGO8pRylJCh2iAlj1bt2/v0qCTrYoRnGfe3g3qIgfHQ/axo1DK1pTdutlxaUM4L81Q
3. Лунгол О. М., Габорець О. А. OSINT-технології в правоохоронній діяльності: навчальний посібник. Мультимедійне видання. Кропивницький: Book Creator, 2023. 107 с. URL: https://read.bookcreator.com/fQ6a2RCUdGO8pRylJCh2iAlj1bt2/sWY11xVJRKymMSKpkHe4TQ/izsvJPMuS4uLPTsQxI8LvQ
4. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: Львівський державний університет внутрішніх справ, 2017. 244 с.

Інтернет-ресурси:

1. Офіційний сайт Президента України: www.president.gov.ua
2. Офіційний сайт Верховної Ради України: www.kmu.gov.ua
3. Офіційний сайт Кабінету Міністрів України: www.kmu.gov.ua
4. Офіційний сайт Верховного Суду: https://supreme.court.gov.ua/supreme/
5. Офіційний сайт Міністерства внутрішніх справ України: https://mvs.gov.ua/
6. Офіційний сайт Національної поліції України: https://www.npu.gov.ua/
7. Головне управління державної служби України: http://www.guds.gov.ua
8. Сайт Ради національної безпеки і оборони України: http://www.raibow.gov.ua
9. OSINT Framework: https://osintframework.com/
10. Національна бібліотека України імені В.І. Вернадського: www.nbuv.gov.ua

Додаток 1 до Робочої програми навчальної дисципліни

Лист оновлення та перезатвердження робочої програми навчальної дисципліни

Навчальний рік	Протокол та дата засідання кафедри	Зміст змін	Підпис завідувача кафедри