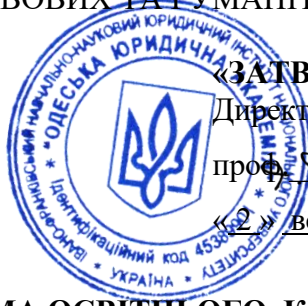
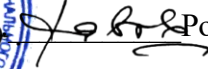


ІВАНО-ФРАНКІВСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ЮРИДИЧНИЙ ІНСТИТУТ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
КАФЕДРА ЗАГАЛЬНОПРАВОВИХ ТА ГУМАНІТАРНИХ ДИСЦИПЛІН



«ЗАТВЕРДЖУЮ»

Директор ІФННЮІ НУ «ОЮА»

проф.  Роман САВЧУК

«2» вересня 2025 р.

РОБОЧА ПРОГРАМА ОСВІТНЬОГО КОМПОНЕНТУ

**КІБЕРБЕЗПЕКА ТА ІНФОРМАЦІЙНО-АНАЛІТИЧНЕ ЗАБЕЗПЕЧЕННЯ
ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ
ОК 13**

рівень вищої освіти	другий (магістерський)
ступінь вищої освіти	магістр
галузь знань	26 Цивільна безпека (К Безпека та оборона)
спеціальність	262 Правоохоронна діяльність (К9 Правоохоронна діяльність)
освітня програма	Правоохоронна діяльність

Розробники програми: Гладенький Юрій Васильович

Затверджено на засіданні кафедри загальноправових та гуманітарних дисциплін
(протокол № 1 від 28.08.2025 р.)

В.о. завідувача кафедри загальноправових
та гуманітарних дисциплін



Лілія КОРИТКО

Керівник навчального відділу



Ірина ЯЦКІВ

Гарант освітньої програми



Ігор МАГНОВСЬКИЙ

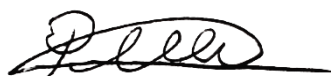
Науково-методична рада (протокол № 1 від 02.09 2025 р.)

Голова науково-методичної
ради



Олександр ФЕЛИК

Заступник директора



Олександр ФЕЛИК

РОБОЧА ПРОГРАМА ОСВІТНЬОГО КОМПОНЕНТА

1. Опис освітнього компонента					
Назва освітнього компонента	<u>Кібербезпека та інформаційно-аналітичне забезпечення правоохоронної діяльності</u> <u>Cybersecurity and information-analytical support for law enforcement activities</u>				
Освітня програма	Освітньо-професійна програма підготовки здобувачів вищої освіти другого (магістерського) рівня вищої освіти галузі знань 26 «Цивільна безпека» за спеціальністю 262 «Правоохоронна діяльність» (галузі знань К «Безпека та оборона» за спеціальністю К9 «Правоохоронна діяльність» – в редакції постанови КМУ від 30.08.2024 р. № 1021 для набору з 2025 року включно)				
Рівень вищої освіти	Форма навчання	Тип	Курс	Семестр	Обсяг, кредит / год
Другий (магістерський) рівень	Денна, заочна форма навчання	О	1	2	денна ф/н – 3/90, заочна ф/н – 3/90
Короткий опис предметної сфери	Навчальна дисципліна «Кібербезпека та інформаційно-аналітичне забезпечення правоохоронної діяльності» спрямована на підготовку висококваліфікованих фахівців здатних ідентифікувати та розв'язувати складні задачі і проблеми у сфері правоохоронної діяльності, що характеризуються невизначеністю умов і вимог, вивчення теоретичних основ та набуття ними базових практичних навичок з організації інформаційної діяльності та використання сучасних інформаційних технологій, роботи з державними реєстрами, відомчими інформаційними системами, сучасними аналітичними програмними продуктами, що використовуються під час інформаційно-аналітичного забезпечення правоохоронної діяльності.				
Викладач освітнього компонента	Гладенький Юрій Васильович асистент кафедри загальноправових та гуманітарних дисциплін ІФННЮІ Національного університету «Одеська юридична академія» Івано-Франківськ, вул. Максимовича, 13 каб. 408				
Мова викладання	українська				
Передумови	«Кримінальний аналіз та стратегічне прогнозування у правоохоронних органах України», «Сучасні практики поліцейської діяльності», «Теорія та практика правоохоронної діяльності»				
Постреквізити	Дисципліна є підґрунтям для подальшого засвоєння та вдосконалення спеціальних (фахових) компетентностей за обраним спрямуванням.				

2. Структура освітнього компонента		
Види навантаження	Денна форма год.	Заочна форма год.
Кількість кредитів / год	3/90	3/90
Усього годин аудиторної роботи, у т. ч.:	34	16
• лекційні заняття, год.	16	10
• практичні/семінарські заняття, год.	18	6
Усього годин самостійної роботи, у т. ч.:	56	74
• індивідуальне науково-дослідне завдання, год.	17	17
• підготовка до аудиторних занять та контрольних заходів, год.	39	57
Екзамен	+	+
Залік	–	–

3. Мета і завдання освітнього компонента				
Мета навчальної дисципліни		Метою викладання навчальної дисципліни є формування та удосконалення у здобувачів системи знань, умінь і навичок, необхідних для використання сучасних інформаційних технологій у практичній діяльності поліції; удосконалення навичок професійної роботи з комп'ютерними пристроями, комп'ютерними мережами та електронними документами; напрямками використання інформаційних технологій у практиці боротьби із злочинністю, формування знань і вмінь з методів забезпечення кібербезпеки в інформаційних та комунікаційних системах.		
Завдання навчальної дисципліни		Основними завданнями вивчення навчальної дисципліни «Кібербезпека та інформаційно-аналітичне забезпечення правоохоронної діяльності» є: – опанування інформаційними та аналітичними ресурсами правоохоронних органів, сутністю новітніх інформаційних технологій, які використовуються в діяльності поліції; – вивчення основних принципів роботи з інформаційно-аналітичними системами, які використовуються в структурі МВС України та в правоохоронній діяльності; – ознайомлення із різними видами атак на інформаційні та комунікаційні системи; – формування навичок аналізу можливих інформаційних загроз та прийняття рішень щодо захисту від них.		
Результати освітнього компонента				
Сим вол РН	Внаслідок вивчення ОК студент буде здатним продемонструвати такі результати навчання:	Посилання на символ ПРН	Методи викладання і навчання	Методи оцінювання досягнення РН
1.	використовувати сучасні інформаційні технології, бази даних та стандартне і спеціалізоване програмне забезпечення	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
2.	визначати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях

3.	застосовувати методи криптографічного та технічного захисту інформації	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
4.	розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів; технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
5.	користуватися державною системою урядового зв'язку, Національною системою конфіденційного зв'язку, радіочастотним ресурсом України, поштовим зв'язком спеціального призначення, урядовим фельд'єгерським зв'язком	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
6.	узагальнювати та аналізувати державну політику у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, криптографічного та технічного захисту інформації, телекомунікацій	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
7.	здійснювати пошук необхідної інформації в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
8.	аналізувати обстановку, рівень потенційних загроз та викликів, прогнозувати розвиток дій правопорушників, вживати заходів з метою запобігання, виявлення та припинення правопорушень	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях
9.	надавати оцінку проблемам та прогалинам у сфері кібербезпеки та інформаційно-аналітичного забезпечення	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях

	правоохоронної діяльності, пропонувати шляхи їх вирішення та усунення			
10.	аргументовано викладати у процесуальних документах свою правову позицію з питань кібербезпеки та інформаційно-аналітичного забезпечення правоохоронної діяльності, а також логічно та послідовно її відстоювати.	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	Лекції, семінарські заняття, самостійне навчання, консультації, практичні роботи, наукові семінари	Екзамен, поточне оцінювання на семінарських/практичних заняттях

Зв'язок з програмними результатами навчання	
Шифр програмного РН	Результати навчання цього ОК деталізують такі Програмні результати навчання:
РН 1.	Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію до фахівців і нефаківців; зокрема, під час публічних виступів, дискусій, проведення занять.
РН 4.	Узагальнювати практичні результати роботи і пропонувати нові рішення, з урахуванням цілей, обмежень, правових, соціальних, економічних та етичних аспектів.
РН 5.	Аналізувати умови і причини вчинення правопорушень, визначати шляхи їх усунення.
РН 7.	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.
РН 8.	Забезпечувати законність та правопорядок, захист прав та інтересів особистості, суспільства, держави з використанням ефективних методів й засобів забезпечення публічної безпеки і порядку в межах виконання своїх посадових обов'язків.
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 11.	Розробляти та кваліфіковано застосовувати нормативно-правові акти в різних сферах юридичної діяльності, реалізовувати норми матеріального й процесуального права в професійній діяльності.
РН 12.	Надавати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності.
РН 13.	Відшуковувати необхідну інформацію в спеціальній літературі, базах даних, інших джерелах інформації, аналізувати та об'єктивно оцінювати інформацію.
РН 14.	Розробляти та управляти проектами у сфері правоохоронної діяльності та з дотичних міждисциплінарних напрямів, аналізувати вимоги, визначати цілі, завдання, ресурси, строки, виконавців.
РН 15.	Модифікувати основні методи та засоби забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки та порядку.

РН 16.	Використовувати сучасні методи і засоби системного аналізу, імітаційного моделювання, збирання та оброблення інформації для аналізу варіантів і прийняття рішень при виконанні професійних завдань.
РН 17.	Розуміти основи забезпечення національної безпеки, особливості застосування спеціальних засобів (вогнепальної зброї, спеціальних засобів, засобів фізичної сили); технології захисту даних, методи обробки, накопичення та оцінювання інформації; інформаційно-аналітичної роботи, бази даних (в тому числі міжвідомчі та міжнародні); оперативні та оперативно-технічні засоби, здійснення оперативно-розшукової діяльності).
РН 18.	Мати навички вирішення завдань у складі міжвідомчих органів з проблем забезпечення безпеки та підтримання правопорядку.
РН 19.	Аналізувати обстановку, рівень потенційних загроз та викликів, прогнозувати розвиток дій правопорушників, вживати заходів з метою запобігання, виявлення та припинення правопорушень.

Зв'язок з програмними результатами навчання	
Шифр програмного РН	Результати навчання цього ОК деталізують такі програмні результати навчання:
ІК	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.
ЗК1.	Здатність до абстрактного мислення, аналізу та синтезу.
ЗК2.	Здатність застосовувати знання у практичних ситуаціях.
ЗК4.	Здатність проведення досліджень на відповідному рівні.
ЗК5.	Здатність вчитися і оволодівати сучасними знаннями.
ЗК7.	Здатність до адаптації та дії в новій ситуації.
ЗК8.	Здатність приймати обґрунтовані рішення.
ЗК9.	Здатність генерувати нові ідеї (креативність).
ЗК10.	ЗК10. Здатність оцінювати та забезпечувати якість виконуваних робіт.
СК1.	Здатність брати участь у розробленні та кваліфіковано застосовувати нормативно-правові акти в різних сферах юридичної діяльності, реалізовувати норми матеріального й процесуального права в професійній діяльності.
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.
СК5.	Здатність давати кваліфіковані юридичні висновки й консультації в конкретних сферах юридичної діяльності.
СК9.	Здатність обирати оптимальні методи й засоби забезпечення публічної безпеки і порядку.
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.
СК15.	Здатність вживати заходів з метою запобігання, виявлення та припинення адміністративних і кримінальних правопорушень, заходів, спрямованих на усунення загроз приватним та публічним інтересам людини й держави.

Технологія навчання	Змішане навчання (аудиторне навчання, поєднане із частковим застосуванням електронного навчання і дистанційних технологій)
---------------------	--

4. Програма та тематичний план освітнього компонента	
Програма освітнього компонента	<u>Кібербезпека та інформаційно-аналітичне забезпечення правоохоронної діяльності</u>
	<u>Cybersecurity and information-analytical support for law enforcement activities</u>

Лекційні заняття				
Символ одиниці змісту	Опис змісту навчання (теми)	Посилання на РН дисципліни	ДФ год.	ЗФ год.
Тема 1.	Формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19	2	2
Тема 2.	Основні відомості про кібербезпеку. Пасивний збір інформації. Шкідливе програмне забезпечення.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19	2	2
Тема 3.	Безпека в операційних системах. Безпека в безпроводних мережах.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 14, 15, 17, 18, 19	2	2
Тема 4.	Здійснення оперативно-розшукових заходів у мережі Інтернет. Аналіз соціальних мереж та відкритих джерел інформації під час розслідування злочинів.	ПРН 1, 4, 5, 7, 8, 9, 11, 12, 14, 15, 16, 17, 18, 19	2	—
Тема 5.	Використання новітніх інформаційних технологій в діяльності Національної поліції України. Загальна характеристика і проблеми інформаційно-аналітичного забезпечення правоохоронної діяльності.	ПРН 1, 4, 7, 9, 11, 12, 13, 16, 17, 19	2	2
Тема 6.	Створення шаблонів юридичних документів. Аналіз, вибірка та візуалізація даних в середовищі MS Excel.	ПРН 1, 4, 7, 9, 16, 17	2	—
Тема 7.	Інформаційно-аналітичні системи та юридичні довідкові ресурси. Інформаційні системи міжнародних організацій з протидії злочинності.	ПРН 1, 4, 7, 9, 10, 13, 16, 17	2	2
Тема 8.	Функціонування державної системи урядового зв'язку, Національна система конфіденційного зв'язку (Держспецзв'язок).	ПРН 1, 4, 7, 9, 10, 11, 12	2	—
Всього			16	10

Практичні, семінарські, лабораторні заняття				
Символ одиниці змісту	Опис змісту навчання (теми)	Посилання на РН дисципліни	ДФ год.	ЗФ год.
Тема 1.	Формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19	2	2
Тема 2.	Основні відомості про кібербезпеку. Пасивний збір інформації. Шкідливе програмне забезпечення.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19	2	2
Тема 3.	Безпека в операційних системах. Безпека в безпроводних мережах.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 14, 15, 17, 18, 19	2	—

Тема 4.	Здійснення оперативно-розшукових заходів у мережі Інтернет. Аналіз соціальних мереж та відкритих джерел інформації під час розслідування злочинів.	ПРН 1, 4, 5, 7, 8, 9, 11, 12, 14, 15, 16, 17, 18, 19	4	—
Тема 5.	Використання новітніх інформаційних технологій в діяльності Національної поліції України. Загальна характеристика і проблеми інформаційно-аналітичного забезпечення правоохоронної діяльності.	ПРН 1, 4, 7, 9, 11, 12, 13, 16, 17, 19	2	2
Тема 6.	Створення шаблонів юридичних документів. Аналіз, вибірка та візуалізація даних в середовищі MS Excel.	ПРН 1, 4, 7, 9, 16, 17	2	—
Тема 7.	Інформаційно-аналітичні системи та юридичні довідкові ресурси. Інформаційні системи міжнародних організацій з протидії злочинності.	ПРН 1, 4, 7, 9, 10, 13, 16, 17	2	—
Тема 8.	Функціонування державної системи урядового зв'язку, Національна система конфіденційного зв'язку (Держспецзв'язок).	ПРН 1, 4, 7, 9, 10, 11, 12	2	—
Всього			18	6

Самостійна робота				
Символ одиниці змісту	Опис змісту навчання (теми)	Посилання на РН дисципліни	ДФН	ЗФН
Тема 1.	Формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації..	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19	4	7
Тема 2.	Основні відомості про кібербезпеку. Пасивний збір інформації. Шкідливе програмне забезпечення.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19	4	6
Тема 3.	Безпека в операційних системах. Безпека в безпроводних мережах.	ПРН 1, 4, 5, 8, 9, 10, 11, 12, 14, 15, 17, 18, 19	4	6
Тема 4.	Здійснення оперативно-розшукових заходів у мережі Інтернет. Аналіз соціальних мереж та відкритих джерел інформації під час розслідування злочинів.	ПРН 1, 4, 5, 7, 8, 9, 11, 12, 14, 15, 16, 17, 18, 19	5	7
Тема 5.	Використання новітніх інформаційних технологій в діяльності Національної поліції України. Загальна характеристика і проблеми інформаційно-аналітичного забезпечення правоохоронної діяльності.	ПРН 1, 4, 7, 9, 11, 12, 13, 16, 17, 19	4	7
Тема 6.	Створення шаблонів юридичних документів. Аналіз, вибірка та візуалізація даних в середовищі MS Excel.	ПРН 1, 4, 7, 9, 16, 17	4	6
Тема 7.	Інформаційно-аналітичні системи та юридичні довідкові ресурси. Інформаційні системи міжнародних організацій з протидії злочинності.	ПРН 1, 4, 7, 9, 10, 13, 16, 17	4	6
Тема 8.	Функціонування державної системи урядового зв'язку, Національна система конфіденційного зв'язку (Держспецзв'язок).	ПРН 1, 4, 7, 9, 10, 11, 12	4	6
Підготовка до семестрового контролю		ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	6	6
Всього			39	57

Індивідуальні завдання				
Символ одиниці змісту	Опис змісту індивідуального завдання	Посилання на РН ОК	ДФ год.	ЗФ год.
1.	Підготовка есе, реферату (тез доповіді) або презентації в межах питань, що розглядаються на лекційних та практичних заняттях. Есе та/або реферат (доповідь) являє собою інформаційне повідомлення, результат індивідуальної думки та враження з поглибленого дослідження індивідуально обраної здобувачем теми (окремих питань навчальної дисципліни) та має бути підкріпленим науково-літературною базою та/або прикладами із практики.	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	6	6
2.	Аналіз міжнародно-правових актів, національного законодавства та судової практики у сфері кібербезпеки та інформаційно-аналітичного забезпечення правоохоронної діяльності.	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	6	6
3.	Демонстрація навичок користування інформаційно-аналітичними системами та юридичними довідковими ресурсами, а також вмінь здійснювати вибірку та візуалізацію даних за допомогою інформаційних технологій.	ПРН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19	5	5
Всього			17	17

5. Ресурси для навчання	
Список основних джерел	1. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник / В.Л. Бурячок, Г.М. Гулак, В.Б. Толубко. – Львів: «Магнолія, 2006». 2024. 448 с 2. Виганяйло С. М. Інформаційне забезпечення професійної діяльності: навч. посіб. / С.М. Виганяйло. Харків: ХНУВС, 2021. 108 с. 3. Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник. Київ : Видавництво НА СБ України, 2020. 256 с. 4. Інформаційне та обліково-аналітичне забезпечення економічної безпеки підприємства: навч. посіб. / О.М. Левченко, Н.С. Шалімова, Т.І. Грінка, О.В. Сторожук, Кропивницький: ЦНТУ, 2022. 190 с 5. Когут Ю.І. Цифрова трансформація економіки та проблеми кібербезпеки: практичний посібник. Київ: Консалтингова компанія «СІДКОН»; ВД «ДАКОР», 2023. 368 с. 6. Манжай О.В., Манжай І.А. Правові засади захисту інформації: підручник/ вид. друге, переробл. та доповн. Харків: Промарт, 2020. 162 с. 7. Методичний посібник для тренерів з питань кібергігієни у рамках спеціальної професійної (сертифікованої) програми підвищення кваліфікації: практикум / О.В. Манжай, В.В. Носов. К.: ВАІТЕ, 2021. 106 с. 9. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с. 10. Остапов С.Є., Євсєєв С.П., Король О.Г. Технології захисту інформації. Львів: «Новий світ-2000», 2024. 678 с. 11. Павлиш Т.Г., Цуркан О.П. Інформаційне забезпечення професійної діяльності: навч. посіб. Кривий Ріг: ДонДУВС, 2021. 87 с. 12. Присяжнюк М.М. Організаційно-правові основи забезпечення кібербезпеки: підручник. Київ: Видавництво Ліра-К, 2023. 320 с. 13. Смірнов О.А., Коноплицька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. Вступ до кібербезпеки: навч. посіб. – Кропивницький : ЦНТУ, 2022. 967 с.

14. Управління інформаційною безпекою / КПП ім. Ігоря Сікорського; уклад.: С.О. Носок, О.М. Фаль, В.М. Ткач. Київ : КПП ім. Ігоря Сікорського, 2021. 258 с.

Нормативні акти:

1. Про електронні комунікації. Закон України від 16.12.2020 № 1089-IX. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>.

2. Про захист інформації в інформаційно-комунікаційних системах. Закон України від 05.07.2014 № 80/94-ВР. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.

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

4. Про Національну програму інформатизації. Закон України від 04.02.1998 № 74/98-ВР. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text>.

5. Деякі питання державної реєстрації та функціонування єдиних та державних реєстрів, держателем яких є Міністерство юстиції, в умовах воєнного стану. Постанова Кабінету Міністрів України від 06.03.2022 № 209. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/209-2022-п#Text>.

6. Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану. Постанова Кабінету Міністрів України від 12.03.2022 № 263. Урядовий портал. Єдиний веб-портал органів виконавчої влади. URL: <https://www.kmu.gov.ua/npas/deyaki-pitannya-zabezpechennya-funkcionuvannya-informacijno-komunikacijnih-sistem-elektronnih-komunikacijnih-sistem-publichnih-elektronnih-reyestriv-v-umovah-voyennogo-stanu-263>.

7. Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС. Наказ МВС України від 20.10.2017 № 870. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/z1433-17#Text>.

8. Положення про єдину інформаційну систему Міністерства внутрішніх справ та переліку її пріоритетних інформаційних ресурсів. Постанова Кабінету Міністрів України від 14.11.2018 № 1024. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF#Text>.

9. Положення про інформаційно-комунікаційну систему «Інформаційний портал Національної поліції України». Наказ МВС України від 03.08.2017 № 676. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/z1059-17#Text>.

10. Про внесення змін до деяких законів України щодо заборони виготовлення та поширення інформаційної продукції, спрямованої на пропагування дій держави-агресора. Закон України від 03.03.2022 № 2109-IX. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2109-20#Text>.

11. Про внесення змін до деяких законодавчих актів України щодо посилення кримінальної відповідальності за виготовлення та поширення забороненої інформаційної продукції. Закон України від 03.03.2022 № 2110-IX. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2110-20#Text>.

12. Про внесення змін до Кримінального кодексу України щодо підвищення боротьби з кіберзлочинністю в умовах дії воєнного стану. Закон України від 24.03.2022 № 2149-IX. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2149-20#Text>.

13. Про внесення змін до Кримінального процесуального кодексу України та Закону України «Про електронні комунікації» щодо підвищення ефективності досудового розслідування «за гарячими слідами» та протидії кібератакам. Закон України від 15.03.2022 № 2137-IX. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2137-20#Text>.

14. Про електронні довірчі послуги. Закон України від 05.10.2017 № 2155-VII. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>.

	15. Про електронні документи та електронний документообіг. Закон України від 22.05.2003 № 851-IV. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text. 16. Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 № 2163-VIII. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text. 17. Стратегія кібербезпеки України. Указ Президента України від 26.08.2021 року № 447/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n7 18. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text 19. Закон України «Про Національну поліцію». URL: https://zakon.rada.gov.ua/laws/show/580-19#Text 20. Про затвердження Інструкції з формування та ведення інформаційної підсистеми «Єдиний облік» інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України». URL: http://search.ligazakon.ua/l_doc2.nsf/link1/RE33710.html 21. Вимоги до створення і впровадження єдиної системи електронного документообігу в Міністерстві внутрішніх справ України та центральних органах виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України (Шифр – СЕД системи MBC). URL: https://mvs.gov.ua/upload/file/vimogi_do_sed_sistemi_mvs_363.pdf
--	---

Список допоміжних джерел	1. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с. 2. Бурячок В.Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В.Л. Бурячок, Р.В. Киричок, П.М. Складанний. К, 2018. 320 с. 3. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. [Видання друге, перероб. та доп.]. Одеса.: ОНАЗ ім. О.С. Попова, 2019. 320 с. 4. Задерейко О.В., Трофименко О.Г., Логінова Н.І., Прокоп Ю.В., Кухаренко С.В., Дика А.І. Захист даних користувачів в інформаційних системах // Сучасна спеціальна техніка, наук.-пр. журн. / Держ. н.-д. ін-т МВС України, Київ. 2022. № 1(68), С. 23-33. 5. Інформаційно-аналітичне забезпечення правоохоронної діяльності: навчально-методичні матеріали /уклад. Г.В. Форос, О.А. Балтовський. Одеса: ОДУВС, 2022. 26 с. 6. Лісовська Ю.П. Кібербезпека: ризики та заходи: навч. посібник. К.: Видавничий дім «Кондор», 2019. 272 с. 7. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с. 8. Організація правоохоронної діяльності Національної поліції України [Електронне видання]: навчально-методичний посібник з навчальної дисципліни «Організація правоохоронної діяльності Національної поліції України» (галузь знань 26 «Цивільна безпека», другий (магістерський) рівень, спеціальність 262 «Правоохоронна діяльність») для студентів I курсу магістратури заочної форми навчання / Н.М. Бакаянова, А.В. Кубаєнко, О.Г. Свіда. Одеса: Фенікс, 2020. 218 с. 9. Судові та правоохоронні органи України: навчальний посібник / М.А. Макаров, А.С. Симчук, М.Й. Кулик, Ю.В. Терещенко, С.В. Харченко. Київ: Нац. акад. внутр. справ, 2022. 656 с. 10. Tulinov Valentyn S., Bilykh Iryna V., Merdova Olga M., Volobuieva Olena O., Veselov Mykola Y. (2022). Activities of Law Enforcement Agencies in the Context of the Introduction of Innovative Technologies (Comparative Legal Aspect). Cuestiones Políticas, 40/72: P. 145–163.
---------------------------------	---

	11. Zadereyko O., Trofymenko O., Prokop Y., Loginova N., Dyka A., Kukharensko S. Research of potential data leaks in information and communication systems. Radioelectronic and Computer Systems. 2022. No 4. P.64-84.
--	--

Інформаційні ресурси в Інтернеті	1. http://www.nbu.gov.ua – Бібліотека ім. Вернадського. 2. https://nlu.org.ua – Парламентська бібліотека. 3. https://www.gp.gov.ua/ua/index.html – Офіс Генерального прокурора. 4. https://mvs.gov.ua/uk – МВС України. 5. https://www.npu.gov.ua – Національна поліція України. 6. https://ssu.gov.ua – Служба безпеки України. 7. https://supreme.court.gov.ua/supreme/gromadyanam/perelik_sprav – Верховний суд. 8. https://unba.org.ua – Національна асоціація адвокатів України. 9. https://esbu.gov.ua/ – Бюро економічної безпеки. 10. https://dbr.gov.ua – Державне бюро розслідування. 11. https://nabu.gov.ua – Національне антикорупційного бюро України. 12. https://www.mon.gov.ua – Міністерство освіти і науки України. 13. https://www.president.gov.ua – Президент України. 14. https://zakon.rada.gov.ua – Верховна Рада України. 15. https://www.reyestr.court.gov.ua – Єдиний державний реєстр судових рішень. 16. https://www.echr.coe.int/echr – Європейський суд з прав людини. 17. http://dspace.onua.edu.ua – eNUOLAIR – депозитарій (архів) НУ «ОЮА». 18. https://tzi.com.ua – Бібліотека «Технічний захист інформації». 19. https://cip.gov.ua/ua/news/perelik-aktiv-zakonodavstva-u-sferi-tekhnichnogozakhistu-informaciyi – Державна служба спеціального зв'язку та захисту (перелік актів законодавства у сфері технічного захисту інформації). 20. https://www.coe.int/uk/web/kyiv – Офіс Ради Європи в Україні. 21. https://pravojustice.eu/ua – Проект ЄС «Підтримка реформ у сфері юстиції».
---	---

6. Контрольні заходи	
Методи діагностики знань (контролю)	Поточний контроль знань здійснюється під час проведення практичних занять і має на меті перевірку рівня знань студентів. Методи поточного контролю: Усне опитування здобувачів вищої освіти, вирішення практичних завдань, тестові завдання, проектний метод (складання типових документів); кейс-метод, ситуаційні завдання, ділові ігри. Проміжний контроль. Проводиться після вивчення відповідних тем або блоку тем з метою з'ясування ступеню засвоєності здобувачами вищої освіти відповідного об'єму опрацьованого та вивчення матеріалу та подальшої оцінки рівня отриманих знань. Форми проведення проміжного контролю: контрольна робота, колоквіум. Індивідуальне завдання. Підготовка есе, реферату (тез доповіді) або презентації з питань, що розглядаються на лекційних та практичних заняттях. Аналіз законодавства та судової практики. Здобувач освіти самостійно обирає об'єкт та предмет дослідження. Підсумковий контроль. Проводиться у формі екзамену.

Схема нарахування балів (складові оцінювання результатів навчання)			
Пункт оцінки	% підсумкової оцінки або максимальна оцінка в балах	Групове чи індивідуальне оцінювання	Посилання на РН
Поточний контроль, разом, у т.ч.:	60		
• усне опитування	30	Групове та індивідуальне	РН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
• індивідуальні завдання	15	Індивідуальне	РН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
• вирішення практичних завдань	15	Індивідуальне	РН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Підсумковий контроль, разом, у т.ч.:	40		
• письмова компонента	20	Індивідуальне	РН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
• усна компонента	20	Індивідуальне	РН 1, 4, 5, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19
Разом за дисципліну	100		

Шкала та критерії оцінювання

Сума балів за 100-бальною шкалою	Оцінка в ECTS	Значення оцінки ECTS	Критерії оцінювання	Оцінка за національною шкалою	
				Іспит	Залік
90-100	A	відмінно	Здобувач вищої має глибокі і системні знання, вміє узагальнювати теоретичний матеріал, співвідносити загальні знання з конкретними ситуаціями; засвідчив уміння критично оцінювати варіантні підходи щодо сутності норм та уявлень; оволодів навиками аналізувати, моделювати та адекватно оцінювати ситуацію; обізнаний з науковими працями вітчизняних та зарубіжних спеціалістів в даній галузі; матеріал викладає логічно, послідовно та переконливо; самостійно розкриває власні обдарування і нахили.	відмінно	зараховано
82-89	B	дуже добре	Здобувач вищої освіти вільно володіє вивченим обсягом матеріалу, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.	добре	зараховано
74-81	C	добре	Здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача; в цілому самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, серед яких є суттєві, добирати аргументи для підтвердження думок.	добре	зараховано

64-73	D	задовільно	Здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень; з допомогою викладача може аналізувати навчальний матеріал, виправляти помилки, серед яких є значна кількість суттєвих.	задовільно	зараховано
60-63	E	достатньо	Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.	задовільно	зараховано
35-59	FX	незадовільно з можливістю повторного складання семестрового контролю	Здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу.	незадовільно	не зараховано
0-34	F	Незадовільно з обов'язковим повторним вивченням залікового кредиту	Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.	незадовільно	не зараховано

7. Інші застереження щодо вивчення освітнього компонента

Вимоги викладача:	Регулярне відвідування лекційних та практичних занять, самостійна робота та опрацювання рекомендованої літератури і матеріалів є необхідною умовою. Користування електронними пристроями (телефони, планшетні ПК тощо) під час аудиторної роботи дозволяється тільки з дозволу викладача та у відповідних до навчального курсу цілях.
--------------------------	---

Припущення основних проблем, пов'язаних з реалізацією курсу	Великий обсяг законодавчої бази та літератури, необхідної для засвоєння, динамічність внесення змін та доповнень до нормативно-правових актів. Наявність значного різноманіття наукових поглядів з приводу питань, що вивчаються в межах курсу. Можливе певне ускладнення у зв'язку з появою нових кіберзагроз та необхідністю розробки інноваційних методів боротьби з ними, а також постійним удосконаленням і оновленням інформаційно-аналітичного забезпечення правоохоронної діяльності. Також передбачаються деякі труднощі в роботі з новітньою літературою та матеріалами іноземною мовою у студентів з низьким рівнем відповідного мовного знання.
--	--