

Силабус освітнього компоненту

Захист інформації з обмеженим доступом

Рівень вищої освіти – **перший (бакалаврський) рівень**
Освітньо-професійна програма – **Правоохоронна діяльність**
Рік навчання: **2025–2026**, Семестр: **2**
Кількість кредитів: **денна ф/н - 3, заочна ф/н - 3**
Обсяг годин: **денна ф/н - 90, заочна ф/н - 90**
Мова викладання: **українська**
Підсумковий контроль – **залік**
Форма проведення занять – **лекції, семінарські заняття**

Назва освітнього компоненту	<u>Захист інформації з обмеженим доступом</u> <u>Protection of restricted information</u>
Викладач	Коропецька Сніжана Орестівна Доцент кафедри кримінального процесу та криміналістики Івано-Франківського навчально-наукового юридичного інституту Національного університету «Одеська юридична академія», кандидат юридичних наук, доцент Івано-Франківськ, вул. Максимовича, 13 каб. 208
E-mail:	snigana.koropetska@gmail.com
Консультації викладача	Ср.14.00-16.00

1. Коротка анотація до курсу:

Навчальна дисципліна «Захист інформації з обмеженим доступом» є обов'язковою навчальною дисципліною, яка спрямована на формування у здобувачів вищої освіти системи теоретичних знань та практичних навичок у сфері забезпечення інформаційної безпеки, організації та здійснення захисту інформації з обмеженим доступом у діяльності правоохоронних органів.

Вивчення навчальної дисципліни передбачає ознайомлення із правовими засадами інформаційних відносин, класифікацією інформації з обмеженим доступом, особливостями правового режиму конфіденційної, службової та таємної інформації відповідно до чинного законодавства України. Значна увага приділяється аналізу нормативно-правових актів, що регулюють захист інформації, зокрема законодавства у сфері інформації, державної таємниці, захисту персональних даних та інформаційно-комунікаційних систем.

Систему дисципліни становлять теми, що розкривають поняття та види інформації з обмеженим доступом, принципи її захисту, суб'єктів забезпечення інформаційної безпеки, порядок організації режиму доступу до інформації, а також особливості роботи з матеріальними носіями інформації.

Окрема увага приділяється технічному, програмному та криптографічному захисту інформації, виявленню каналів витоку інформації, методам протидії несанкціонованому доступу, а також створенню та функціонуванню комплексної системи захисту інформації в інформаційно-комунікаційних системах.

Вивчення навчальної дисципліни передбачає формування у здобувачів освіти вмінь здійснювати аналіз загроз інформаційній безпеці, оцінювати ризики, обирати та

застосовувати відповідні засоби і методи захисту інформації, забезпечувати дотримання режиму обмеженого доступу та організувати захист інформації у професійній діяльності.

Знання, отримані під час вивчення навчальної дисципліни, сприятимуть формуванню у здобувачів освіти правової культури, відповідальності, дотримання принципів законності, доброчесності та захисту інформаційних прав особи.

Вивчення навчальної дисципліни спрямоване на підготовку здобувачів освіти до професійної діяльності у правоохоронних органах та інших державних установах, діяльність яких пов'язана із забезпеченням захисту інформації та інформаційної безпеки.

Основна мета вивчення навчальної дисципліни полягає у формуванні у здобувачів вищої освіти поглибленого теоретичного та практичного розуміння механізмів захисту інформації з обмеженим доступом, а також набутті знань, умінь і навичок, необхідних для їх ефективного застосування у професійній діяльності.

2. Формат курсу: Очний та/або змішаний.

3. Компетентності, які мають бути сформовані у результаті опанування навчальної дисципліни:

Інтегральні компетентності: Здатність вирішувати складні спеціалізовані задачі та практичні проблеми у сфері правоохоронної діяльності.

Загальні компетентності:

ЗК1. Здатність застосовувати знання у практичних ситуаціях.

ЗК2. Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК4. Здатність використовувати інформаційні та комунікаційні технології.

ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

ЗК8. Здатність приймати обґрунтовані рішення.

Спеціальні компетентності:

СК2. Здатність здійснювати нагляд (контроль) за додержанням вимог законодавства у сфері правоохоронної діяльності.

СК4. Здатність самостійно збирати та критично опрацьовувати, аналізувати та узагальнювати правову інформацію з різних джерел.

СК8. Здатність ефективно застосовувати сучасну техніку та інформаційні технології, використовувати технічні засоби, спеціалізовані інформаційно-пошукові системи, бази та банки даних, а також відповідне програмне забезпечення для захисту прав і свобод людини, власності, суспільних відносин від протиправних посягань.

СК16. Здатність забезпечувати кібербезпеку, економічну та інформаційну безпеку держави, об'єктів критичної інфраструктури.

СК17. Здатність забезпечувати охорону державної таємниці та працювати з носіями інформації з обмеженим доступом.

4. Програмні результати навчання:

РН3. Розуміти та професійно застосовувати понятійний апарат права та правоохоронної діяльності.

РН4. Формулювати і перевіряти гіпотези, виокремлювати юридично значущі факти, виявляти причинно-наслідкові зв'язки в діях і явищах для прийняття оптимального рішення в конкретних ситуаціях.

РН8. Здійснювати пошук інформації у доступних джерелах, аналізувати і оцінювати її для повного та всебічного встановлення обставин, необхідних для виконання професійних завдань.

РН9. Використовувати інформаційно-комунікаційні системи та інші інформаційні ресурси, у тому числі ті, що мають технічний та криптографічний захист, поштовий зв'язок

спеціального призначення, фельд'єгерський зв'язок, системи цифрового зв'язку суб'єктів сектору безпеки і оборони з метою виконання професійних завдань у сфері правоохоронної діяльності.

РН10. Виокремлювати юридично значущі факти і формувати обґрунтовані правові висновки.

РН21. Організовувати та здійснювати заходи щодо дотримання режиму секретності та захисту інформації.

5. Обсяг курсу

Вид заняття	Загальна кількість годин (ДФ)	Загальна кількість годин (ЗФ)
Лекції	18	8
семінарські заняття	20	6
індивідуальна робота	15	15
самостійна робота	37	61
Всього	90	90

6. Технічне й програмне забезпечення/обладнання – доступ до мережі Internet за умови змішаного формату курсу, конспект лекцій, система мультимедійних презентацій та засоби інтерактивного навчання, мультимедійне забезпечення в порталі ZOOM, Moodle.

7. Зміст освітнього компонента:

Лекційні заняття			
	Опис змісту навчання (теми)	ДФ год.	ЗФ Год
Тема 1.	Загальні положення та класифікація інформації з обмеженим доступом.	2	2
Тема 2.	Поняття та види інформації з обмеженим доступом.	2	2
Тема 3.	Правовий режим інформації з обмеженим доступом.	2	-
Тема 4.	Носії інформації з обмеженим доступом та порядок роботи з ними.	2	-
Тема 5.	Суб'єкти забезпечення захисту інформації в Україні.	2	2
Тема 6.	Нормативно-правове забезпечення технічного захисту інформації.	2	2
Тема 7.	Основні положення щодо організації системи захисту інформації.	2	-
Тема 8.	Класифікація технічних каналів витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів.	2	-
Тема 9.	Засоби та методи захисту інформації. Створення комплексів технічного захисту інформації, комплексної системи захисту інформації.	2	-
Всього		18	8

Семінарські, практичні заняття			
	Опис змісту навчання (теми)	ДФ год.	ЗФ год.
Тема 1.	Загальні положення та класифікація інформації з обмеженим доступом.	2	2
Тема 2.	Поняття та види інформації з обмеженим доступом.	2	2
Тема 3.	Правовий режим інформації з обмеженим доступом.	2	-

Тема 4.	Носії інформації з обмеженим доступом та порядок роботи з ними.	2	-
Тема 5.	Суб'єкти забезпечення захисту інформації в Україні.	2	2
Тема 6.	Нормативно-правове забезпечення технічного захисту інформації.	2	-
Тема 7.	Основні положення щодо організації системи захисту інформації.	2	-
Тема 8.	Класифікація технічних каналів витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів.	2	-
Тема 9.	Засоби та методи захисту інформації. Створення комплексів технічного захисту інформації, комплексної системи захисту інформації.	4	-
Всього		20	6

Самостійна робота			
	Опис змісту навчання (наприклад, теми або види навчальної активності)	ДФ год.	ЗФ год.
Тема 1.	Загальні положення та класифікація інформації з обмеженим доступом.	3	6
Тема 2.	Поняття та види інформації з обмеженим доступом.	3	6
Тема 3.	Правовий режим інформації з обмеженим доступом.	3	6
Тема 4.	Носії інформації з обмеженим доступом та порядок роботи з ними.	3	6
Тема 5.	Суб'єкти забезпечення захисту інформації в Україні.	3	6
Тема 6.	Нормативно-правове забезпечення технічного захисту інформації.	4	6
Тема 7.	Основні положення щодо організації системи захисту інформації.	4	6
Тема 8.	Класифікація технічних каналів витоку інформації. Способи несанкціонованого зняття інформації з технічних каналів.	4	6
Тема 9.	Засоби та методи захисту інформації. Створення комплексів технічного захисту інформації, комплексної системи захисту інформації.	4	7
Підготовка до семестрового контролю		6	6
Всього		37	61

Індивідуальні завдання			
	Опис змісту індивідуального завдання	ДФ год.	ЗФ год.
	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.	8	8
	Аналітичний (критичний) огляд наукових публікацій за заданою тематикою та підготовка доповіді, у якій дається зведена	7	7

характеристика певного питання, проблеми, теми, що базується на інформації, здобутій із документів.		
Всього	15	15

8. Система оцінювання

Оцінювання проводиться за 100-бальною шкалою.

Накопичувальна. Оцінювання проводиться за 100-бальною шкалою.

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.

Рубіжний 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 рубіжного контролю: контрольна робота, колоквиум.

Індивідуальне завдання.

Підготовка есе, реферату (тез доповіді) або презентації в межах питань, що розглядаються на лекційних та практичних заняттях. Аналіз законодавства та судової практики. Здобувач вищої освіти самостійно обирає об'єкт та предмет дослідження.

Підсумковий контроль.

Проводиться у формі екзамену

9. Шкала оцінювання

Сума балів за 100-бальною шкалою	Оцінка в ЄКТС	Значення оцінки ЄКТС	Критерії оцінювання	Оцінка за національною шкалою	
				Екзамен	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 справи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.	добре	
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.		

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	
60-63	E	достатньо	Здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні.		
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	Незадовільний з обов'язковим повторним вивченням залікового кредиту	Здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів.		

10. Політика оцінювання

Політика щодо дедлайнів та перескладання: Завдання, які виконуються із порушенням термінів без поважних причин, оцінюються на нижчу оцінку (половина балів з максимально можливих). Перескладання модулів відбувається із дозволу Директора за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: визначається Законами України «Про освіту», «Про вищу освіту», «Про академічну доброчесність», Положенням «Про дотримання академічної доброчесності в Івано-Франківському інституті «ОЮА»». Дотримання академічної доброчесності передбачає:

самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання (для осіб з особливими освітніми потребами ця вимога застосовується з урахуванням їхніх індивідуальних потреб і можливостей);

посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;

дотримання норм законодавства про авторське право і суміжні права;

надання достовірної інформації про результати власної навчальної (наукової, творчої) діяльності, використанні методики досліджень і джерела інформації.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання.

Вимоги до семінарських занять	Семінарське/практичне заняття передбачає підготовку студента шляхом опрацювання рекомендованих джерел, включно з нормативно-правовими актами, підручниками, посібниками та науковими працями, для засвоєння необхідного категоріального апарату та формування теоретичних знань і професійних компетентностей. На семінарському занятті студент бере участь в обговоренні ключових питань теми, аналізі нормативно-правової бази, проведенні дискусій, усному та письмовому опитуванні, виокремленні актуальних проблем
--------------------------------------	--

	<p>правозастосування та виробленні практично обґрунтованих рекомендацій.</p> <p>На практичному занятті студент застосовує набуті знання та вміння для виконання практичних завдань, кейсів, розв'язання ситуаційних або процесуальних проблем, моделювання професійної діяльності та обговорення результатів виконаної роботи.</p>
Вимоги до індивідуальної роботи	<p>Індивідуальна робота має виконуватись самостійно, творчо з використанням усього арсеналу методологічного інструментарію, який набутий здобувачем вищої освіти протягом навчального процесу. У процесі виконання індивідуальної роботи здобувач вищої освіти має опрацювати не менше п'яти літературних джерел з посиланнями на використання певної інформації з них по тексту роботи. Робота має носити практичну направленість та бути спрямованою на вирішення певної проблеми чи висловлення особистого погляду автору роботи на питання, яке розглядається в роботі, і має включати такі компоненти: титульна сторінка; зміст; вступ; основна частина; висновок; список використаної літератури; додатки до індивідуального завдання (при необхідності). Обсяг має становити 10-15 сторінок формату А4.</p>
Вимоги до самостійної роботи	<p>Самостійна робота здобувача вищої освіти повинна бути виконаною ним особисто або групою студентів, де кожен її член самостійно виконує свою частку колективної роботи, являти собою закінчену розробку (чи її етап), де розкриваються й аналізуються актуальні проблеми з певної теми або її окремих аспектів, демонструвати достатню компетентність автора (авторів) у розкритті питань, що досліджуються, а також мати навчальну, наукову й (або) практичну спрямованість і значимість, містити певні елементи новизни (при виконанні науково-дослідної роботи). Виконання самостійної роботи оцінюється під час проведення семінарського/практичного заняття у вигляді опитування.</p>
Умови підсумкового контролю	<p>Підсумкове оцінювання знань здобувачів вищої освіти здійснюється за результатами поточного контролю, екзамену</p>

11. Рекомендована література

11.1. Основна:

Нормативно-правові акти:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>
2. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14>
3. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17>
4. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12>
5. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17>
6. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17>
7. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12>
8. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>

9. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. URL: <https://zakon.rada.gov.ua/laws/show/580-19>

10. Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII. URL: <https://zakon.rada.gov.ua/laws/show/2229-12>

11. Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». URL: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF>

12. Постанова Кабінету Міністрів України від 08.10.1997 № 1126 «Про затвердження Концепції технічного захисту інформації в Україні». URL: <https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF>

13. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 19.07.2023 № 366 «Про затвердження переліку документів нормативно-правової бази у сфері криптографічного та технічного захисту інформації». URL: <https://zakon.rada.gov.ua/laws/show/v0633523-23>

14. НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу». URL: <https://tzi.com.ua/downloads/1.1-002-99.pdf>

15. НД ТЗІ 3.7-003-05 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-комунікаційній системі». URL: <https://tzi.com.ua/downloads/3.7-003-2005.pdf>

Підручники, посібники, наукові праці:

1. Антонов І. Є., Олійников А. М. та ін. Системи технічного захисту інформації: навч. посіб. Харків: ХНУРЕ, 2019. 216 с.

2. Гребніков В. В. Історія криптології та секретного зв'язку. Київ: КНТ, 2023. 800 с.

3. Домарєв В. В. Системи захисту інформації в інформаційно-комунікаційних системах. Київ, 2021.

4. Кухаренко С. В. Комплексна оцінка рівня захищеності автоматизованих систем // Сучасна спеціальна техніка. 2021. № 2. С. 28–34.

5. Лаптев О. А., Савченко В. А., Шуклін Г. В. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності: навч. посіб. Київ: Державний університет телекомунікацій, 2020. 126 с.

6. Коропецька С.О. Забезпечення режиму секретності в діяльності органів і підрозділів національної поліції України. Право.ua. 2026. № 1. С.397-403. URL: chrome-extension://efaidnbmninnkjkpcjgclcfndmkaj/https://pravo.unesco-socio.in.ua/wp-content/uploads/archive/Pravo-ua-2026-1/Pravo_ua_2026_1_397.pdf

7. Методи та засоби технічного захисту інформації: навч. посіб. / уклад. В. М. Луценко, Д. О. Прогонов. Київ: КПП ім. Ігоря Сікорського, 2021. 289 с.

8. Самойленко О. А. Основи розслідування злочинів, вчинених у кіберпросторі: монографія. Одеса: ТЕС, 2020. 372 с.

9. Супруненко А. М. та ін. Організація охорони державної таємниці в Україні: навч. посіб. Ірпінь: УДФСУ, 2020. 370 с.

11.2. Допоміжна:

1. Домарєв В. В., Кухаренко С. В., Тимков В. Ф. Підходи щодо створення автоматизованих систем з комплексним захистом інформації // Сучасна спеціальна техніка. 2021. № 1(64). С. 37–44.

2. Задерейко О. В., Трофименко О. Г., Прокоп Ю. В., Логінова Н. І., Кухаренко С. В. Аналіз витоків даних в інформаційних системах // Сучасна спеціальна техніка. 2021. № 3(66). С. 16–30.

3. Задерейко О. В., Трофименко О. О., Прокоп Ю. В., Логінова Н. І., Дука А., Кухаренко С. В. Дослідження потенційних витоків даних в інформаційно-комунікаційних системах // *Radioelectronics and Computer Systems*. 2022. № 4. С. 64–84.

4. Кухаренко С. В. Комплексна оцінка рівня захищеності автоматизованих систем // *Сучасна спеціальна техніка*. 2021. № 2(65). С. 28–34.

5. Ликов В. В., Антипов І. Є., Олійников А. М. Засоби та системи технічного захисту інформації: навч. посіб. Харків: ХНУРЕ, 2019. 216 с.

6. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі: монографія / за ред. А. Ф. Волобуєва. Одеса: ТЕС, 2020. 372 с.

11.3. Інформаційні ресурси в Інтернеті:

1. <https://zakon.rada.gov.ua> — Верховна Рада України (нормативно-правова база законодавства).

2. <https://www.kmu.gov.ua> — Кабінет Міністрів України (постанови та підзаконні акти).

3. <https://cip.gov.ua> — Державна служба спеціального зв'язку та захисту інформації України.

4. <https://www.niss.gov.ua> — Національний інститут стратегічних досліджень.

5. <https://www.nbuv.gov.ua> — Національна бібліотека України імені В. І. Вернадського.

6. <https://ombudsman.gov.ua> — Уповноважений Верховної Ради України з прав людини (захист персональних даних, інформаційні права).

7. <https://tzi.com.ua> — Бібліотека нормативних документів з технічного захисту інформації.

Доцент кафедри кримінального
процесу та криміналістики



Сніжана КОРОПЕЦЬКА