Міністерство освіти і науки України
Національний університет водного господарства та природокористування

Навчально-науковий інститут права та гуманітарних наук
Кафедра правових природоохоронних дисциплін

08-03-06М

МЕТОДИЧНІ ВКАЗІВКИ

до практичних занять та самостійної роботи
з навчальної дисципліни
«*Правоохоронна діяльність в інформаційну епоху: глобальні виклики та забезпечення безпеки в умовах цифрових технологій*»
для здобувачів вищої освіти першого (бакалаврського) та другого (магістерського) рівнів
всіх освітньо-професійних програм спеціальностей НУВГП
усіх форм навчання

Схвалено науково-
методичною радою НУВГП
Протокол № 3 від 18.03.2026 р.

Рівне – 2026

Методичні вказівки до практичних занять та самостійної роботи з навчальної дисципліни «*Правоохоронна діяльність в інформаційну епоху: глобальні виклики та забезпечення безпеки в умовах цифрових технологій*» для здобувачів вищої освіти першого (бакалаврського) та другого (магістерського) рівнів всіх освітньо-професійних програм спеціальностей НУВГП усіх форм навчання [Електронне видання] / Садовнік В. П., Багатко А. С. – Рівне : НУВГП, 2026. – 42 с.

Укладачі: Садовнік В. П. доктор філософії з права, доцент кафедри правових природоохоронних дисциплін; Багатко А. С., асистент кафедри інформаційного права та юридичної журналістики.

Відповідальний за випуск: Швець О. М., к.ю.н., доцент, в.о. завідувача кафедри правових придоохоронних дисциплін.

Вчений секретар науково-методичної ради Костюкова Т. А.

ЗМІСТ

Передмова

Шановні студенти!

Ми живемо в час, коли інформаційні технології змінюють усе: від способу спілкування та отримання інформації до механізмів державного управління й методів забезпечення безпеки. Цифровізація суспільства формує нову реальність, у якій більшість соціальних, економічних і правових процесів відбувається в інформаційному просторі. У цих умовах правоохоронна діяльність набуває якісно нових рис та потребує переосмислення традиційних підходів до забезпечення правопорядку.

Правоохоронна діяльність в інформаційну епоху стикається з комплексом нових викликів – кіберзлочинністю, цифровими шахрайствами, незаконним втручанням у роботу інформаційних систем, поширенням дезінформації, загрозами інформаційній безпеці держави та суспільства. Поряд із цим виникають питання правового регулювання використання штучного інтелекту, обігу персональних даних, електронних доказів та цифрової ідентифікації. Разом із викликами відкриваються і нові можливості: застосування сучасних аналітичних інструментів, цифрової криміналістики, автоматизованих інформаційних систем, міжнародної співпраці у сфері кібербезпеки.

Методичні вказівки до практичних занять та самостійної роботи з навчальної дисципліни “Правоохоронна діяльність в інформаційну епоху: глобальні виклики та забезпечення безпеки в умовах цифрових технологій” покликані допомогти вам не лише глибше зрозуміти сучасні тенденції у сфері безпеки, а й сформувати комплекс професійних компетентностей, необхідних для майбутньої практичної діяльності.

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ТА ЇЇ СТРУКТУРА

1.1. Опис навчальної дисципліни

Метою навчальної дисципліни «Правоохоронна діяльність в інформаційну епоху: глобальні виклики та забезпечення безпеки в умовах цифрових технологій» є формування у здобувачів вищої освіти системного уявлення про особливості здійснення правоохоронної діяльності в умовах цифрової трансформації суспільства, оволодіння теоретичними знаннями та практичними навичками щодо виявлення, запобігання, документування й розслідування правопорушень у інформаційному середовищі, а також розвиток професійних компетентностей у сфері забезпечення інформаційної та кібербезпеки.

Основними завданнями дисципліни є формування у здобувачів освіти здатності розв'язувати складні професійні завдання у сфері правоохоронної діяльності в умовах цифрової трансформації суспільства та розвиток навичок абстрактного мислення, аналізу і синтезу під час дослідження правових явищ, пов'язаних із використанням інформаційних технологій. Дисципліна забезпечує ґрунтовне розуміння предметної області, структури правничої професії та ролі правоохоронної діяльності в інформаційному суспільстві. Вона спрямована на формування здатності застосовувати норми національного, міжнародного та європейського права, зокрема стандарти захисту прав людини, у сфері цифрових правовідносин.

У процесі навчання здобувачі набувають практичних навичок збору, аналізу та оцінки інформації з різних джерел, у тому числі електронних доказів, для встановлення юридично значущих фактів. Дисципліна також розвиває вміння здійснювати критичний та системний аналіз

правових проблем, формувати обґрунтовані правові позиції та готувати проєкти актів застосування права.

Особлива увага приділяється формуванню навичок публічної комунікації, ведення професійної дискусії, аргументованого захисту правової позиції та презентації результатів досліджень. Дисципліна виховує повагу до гідності людини, прав і свобод, принципів мультикультурності, професійної етики та цінностей правової держави в умовах інформаційної епохи. Крім того, навчання сприяє розвитку здатності до безперервного професійного розвитку, самонавчання та ефективної адаптації до швидких змін у сфері цифрових технологій і забезпечення безпеки, що дозволяє здобувачам освіти успішно застосовувати набуті знання та навички у практичній діяльності.

Компетентності:

ІК – Здатність розв'язувати складні спеціалізовані задачі у галузі правничої діяльності.

ЗК1 - Здатність до абстрактного мислення, аналізу та синтезу.

ЗК3 - Знання та розуміння предметної області та розуміння професійної діяльності.

ЗК7 – Здатність вчитися і оволодівати сучасними знаннями.

ЗК13 – Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

ЗК14- Цінування та повага різноманітності та мультикультурності.

ЗК18- Здатність володіти навичками публічних виступів, ведення переговорів, професійної та наукової дискусії,

підготовка та демонстрація результатів дослідження.

СК1- Здатність застосовувати знання з основ теорії та філософії права, знання і розуміння структури правничої професії та її ролі у суспільстві.

СК2- Здатність аналізувати ретроспективи розвитку правових явищ та процесів у контексті їх впливу на сучасну правову систему.

СК3- Цінування та повага до гідності людини як найвищої соціальної цінності, розуміння її правової природи.

СК4 - Здатність застосовувати Конвенцію про захист прав людини та основоположних свобод, а також прецедентну практику Європейського суду з прав людини.

СК5 - Здатність застосовувати норми та інститути міжнародного публічного права, а також міжнародного приватного права.

СК6 - Здатність здійснювати порівняльний аналіз окремих правових інститутів права Європейського Союзу та Ради Європи і правової системи України.

СК8 - Здатність застосовувати правові принципи та доктрини

СК10 – Здатність використовувати різноманітні інформаційні джерела для повного та всебічного встановлення певних обставин.

СК11- Здатність визначати належні та прийнятні для юридичного аналізу факти.

СК12 – Здатність аналізувати правові проблеми та обгрунтовувати правові позиції.

СК13 – Здатність до критичного та системного аналізу правових явищ.

СК 17 - Здатність аналізувати правові процеси і явища в історичному контексті.

Програмні результати навчання (ПРН). Результати навчання (РН)

РН2 –Знати та розуміти міжнародні стандарти прав людини, положення Конвенції про захист прав людини та основоположних свобод, а також практику Європейського суду з прав Людини.

РН3- Проводити збір і інтегрований аналіз матеріалів з різних джерел.

РН5- Давати короткий правовий висновок щодо окремих фактичних обставин з достатньою обгрунтованістю.

РН6- Оцінювати недоліки і переваги певних правових аргументів, аналізуючи відому проблему.

РН18- Застосовувати в професійній діяльності основні сучасні правові доктрини, цінності та принципи функціонування національної правової системи.

РН19- Пояснювати природу та зміст основних правових явищ і процесів.

РН20- Виокремлювати і аналізувати юридично значущі факти і робити обгрунтовані правові висновки.

РН21- Готувати проекти необхідних актів застосування права відповідно до правового висновку зробленого у різних правових ситуаціях.

1.2. Тематика практичних занять

№ п\п	Назва теми	Кількість годин			
		лекції		практичні	
		денна форма	заочна форма	денна форма	заочна форма
МОДУЛЬ 1. Сучасні виклики та інструменти правоохоронної діяльності в цифровому середовищі					
1.	Тема 1. Кіберзлочинність у цифровому суспільстві: види, тенденції та методи протидії	2	2	2	2
2.	Тема 2. Електронні докази та цифрова криміналістика: принципи збору, оцінки та використання	2	2	2	2
3.	Тема 3. Використання штучного інтелекту в правоохоронній	2	2	2	2

	діяльності: можливості та ризики				
4.	Тема 4. Забезпечення інформаційної безпеки держави та суспільства в умовах глобалізації	2	-	2	-
5.	Тема 5. Соціальні мережі та цифрові платформи як інструменти розслідування та джерела загроз	2	2	2	1
6.	Тема 6. Міжнародні стандарти прав людини в цифровому просторі та їх застосування у правоохоронній діяльності	2	2	2	1
	МОДУЛЬ 2. Правові та організаційні аспекти протидії цифровим загрозам у правоохоронній діяльності				
7.	*Тема 7* Етичні та правові аспекти цифрового нагляду та контролю інформаційних потоків.	2	1	1	-
8.	Тема 8. Прогнозування та реагування на цифрові загрози: стратегічний підхід для сучасних правоохоронців	2	1	1	-

1.3. Контрольні заходи та засоби діагностики

Поточний контроль знань здобувачів освіти з освітньої компоненти проводиться у формах:

- усного опитування на практичних заняттях;
- оцінки за написання есе та участь в обговоренні проблемних питань;

- аналіз та складання правових документів;
- оцінка виконання індивідуального науково-дослідного завдання.

1.4. Критерії та шкала оцінювання

Основні критерії, що характеризують рівень компетентності здобувача вищої освіти при оцінюванні результатів поточного та підсумкового контролів з навчальної дисципліни:

- виконання всіх видів навчальної роботи, що передбачені силабусом;
- глибина і характер знань навчального матеріалу за змістом навчальної дисципліни, що міститься в основних та додаткових рекомендованих літературних джерелах;
- вміння аналізувати явища, що вивчаються, у їх взаємозв'язку і розвитку;
- характер відповідей на поставлені питання (чіткість, лаконічність, логічність, послідовність тощо);
- вміння застосовувати теоретичні положення під час розв'язання практичних задач;
- вміння аналізувати достовірність одержаних результатів;
- своєчасність виконання;
- дотримання вимог до оформлення.

Критерії оцінювання практичних завдань (у % від кількості балів, виділених на завдання із заокругленням до цілого числа):
0% – завдання не виконано;
40% – завдання виконано частково та містить суттєві помилки методичного або розрахункового характеру, порушені терміни виконання та вимоги до оформлення;
60% – завдання виконано повністю, але містить суттєві помилки, порушені терміни виконання та вимоги до оформлення;
80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки (висновки, оформлення тощо);
100% – завдання виконано правильно, вчасно і без зауважень.
*у разі колективного виконання завдань передбачається розподіл балів між виконавцями

Критерії оцінювання ситуаційних вправ та інших завдань творчого характеру* (% від кількості балів, виділених на завдання із заокругленням до цілого числа):
0% – завдання не виконано;
40% – завдання виконано частково, висновки не аргументовані і не конкретні, звіт підготовлено недбало, порушені терміни виконання;
60% – завдання виконано повністю, висновки містять окремі недоліки,
судження здобувача вищої освіти недостатньо аргументовані, звіт підготовлено з незначним відхиленням від вимог до термінів та оформлення;
80% – завдання виконано повністю і вчасно, проте містить окремі несуттєві недоліки не системного характеру;
100% – завдання виконано правильно, вчасно і без зауважень.
*у разі колективного виконання завдань передбачається розподіл балів між виконавцями

Підсумкова складова оцінювання передбачає складання двох модульних контролів (та/або іспиту) у тестовій формі на платформі Moodle.

Іспит здається студентом у таких випадках:

- студент не повністю виконав завдання передбачені силабусом дисципліни та не отримав рекомендацію щодо автоматичного зарахування суми поточних балів у якості підсумкової оцінки;
- студент хоче покращити отриману шляхом автоматичного зарахування суми поточних балів підсумкову оцінку.

Тестові завдання включають три рівні складності: достатній рівень (запитання з однією правильною відповіддю із п’яти запропонованих варіантів), вище достатнього (запитання із декількома правильними відповідями із п’яти запропонованих варіантів), високого рівня складності (завдання на співставлення понять, визначення поняття із пропущеним словом).

2. ПЛАНИ ПРАКТИЧНИХ ЗАНЯТЬ

МОДУЛЬ 1. Сучасні виклики та інструменти правоохоронної діяльності в цифровому середовищі

ТЕМА № 1. Кіберзлочинність у цифровому суспільстві: види, тенденції та методи протидії

План лекції:

1.Основні поняття та класифікація кіберзлочинності у цифровому суспільстві.
2.Сучасні види кіберзлочинів: фішинг, шкідливе програмне забезпечення, атаки на критичну інфраструктуру.
3. Тенденції та статистика кіберзлочинності в Україні та світі.
4. Основи кібербезпеки та превентивні заходи для захисту інформаційних систем.
5. Методи розслідування та запобігання кіберзлочинам: цифрова криміналістика та аналітика даних.
6. Міжнародне співробітництво у сфері кібербезпеки та протидії кіберзлочинам.

Питання для семінарського заняття:

1. Що таке кіберзлочинність та які її основні характеристики?
2. Які існують класифікації кіберзлочинів? Назвіть приклади.
3. Поясніть поняття фішингу та його основні методи реалізації.
4. Що таке шкідливе програмне забезпечення (віруси, трояни, ransomware) і як воно використовується для злочинних цілей?
5. Які кіберзагрози існують для критичної інфраструктури України та світу?

6. Проаналізуйте останні тенденції кіберзлочинності в Україні: які види злочинів стають більш поширеними?
7. Які основні методи кібербезпеки можуть запобігати злочинам у цифровому середовищі?
8. Що таке цифрова криміналістика і яку роль вона відіграє у розслідуванні кіберзлочинів?
9. Як аналітика даних допомагає у виявленні та прогнозуванні кіберзлочинів?
10. Які міжнародні організації займаються боротьбою з кіберзлочинністю та як відбувається міжнародне співробітництво?
11. Наведіть приклади успішних міжнародних кейсів протидії кіберзлочинності.
12. Поясніть різницю між превентивними та реактивними заходами кібербезпеки.
13. Як впливають технології штучного інтелекту на методи кіберзлочинності та захисту від них?
14. Які етичні та правові проблеми виникають у сфері цифрової безпеки?
15. Обговоріть роль держави та приватного сектору у запобіганні кіберзлочинам.

Завдання № 1

Виберіть один реальний кейс кіберзлочину в Україні або світі. Опишіть, який вид злочину було скоєно. Вкажіть, які методи та технології використовували злочинці. Проаналізуйте наслідки злочину для організації або держави. Складіть короткий план превентивних заходів для запобігання подібним злочинам. Врахуйте методи цифрової криміналістики та аналітики даних. Підготуйте висновки щодо ефективності заходів кібербезпеки. Оформіть звіт обсягом 1–2 сторінки або презентацію на 5–7 слайдів.

Завдання № 2

Проаналізуйте статистичні дані щодо кількості та видів кіберзлочинів за останні три роки. Визначте найбільш поширені методи злочинців для атак на інформаційні системи. Поясніть, як фішинг та шкідливе ПЗ використовуються для отримання несанкціонованого доступу. Розгляньте приклади атак на критичну інфраструктуру та їх наслідки. Складіть список заходів кібербезпеки, які можна застосувати для захисту організацій. Опишіть роль аналітики даних у виявленні потенційних загроз. Оцініть ефективність превентивних та захисних заходів.

ТЕМА № 2. Електронні докази та цифрова криміналістика: принципи збору, оцінки та використання

План лекції:

1. Електронні докази та цифрова криміналістика: основи, значення та джерела інформації
2. Основні правила збору електронних доказів: забезпечення цілісності та дотримання ланцюга зберігання
3. Сучасні методи цифрової криміналістики: відновлення даних, аналіз логів та мережевих потоків
4. Оцінка та тлумачення електронних доказів: визначення достовірності та класифікація інформації
5. Застосування електронних доказів у слідстві та судочинстві: підготовка експертних висновків та розбір практичних кейсів.

Питання для семінарського заняття:

1. Що розуміють під електронними доказами та які види інформаційних ресурсів можуть їх становити?
2. Яке значення цифрової криміналістики у сучасній правоохоронній діяльності?
3. Які принципи збору електронних доказів забезпечують їхню цілісність та допустимість у суді?
4. Що таке ланцюг зберігання доказів і чому його дотримання важливе?
5. Які сучасні методи цифрової криміналістики застосовують для відновлення видалених файлів і аналізу логів?
6. Як визначити достовірність електронних доказів та класифікувати інформацію за доказовою значимістю?
7. Які кроки включає підготовка експертного висновку з електронних доказів для суду?
8. Наведіть приклади практичних кейсів використання цифрових доказів у слідчих та судових процесах.
9. Які типові помилки трапляються при зборі та використанні електронних доказів, і як їх уникнути?
10. Як забезпечується баланс між ефективністю збору цифрових доказів та дотриманням прав людини?

Завдання № 1

Уявіть ситуацію, коли потрібно отримати електронні докази з комп'ютера та мобільного пристрою підозрюваного. Опишіть, які принципи слід дотримуватися під час збору доказів, щоб гарантувати їхню цілісність, достовірність і допустимість у суді. Зверніть увагу на важливість дотримання ланцюга зберігання доказів та використання сертифікованих інструментів і методик. Складіть покроковий план дій для збору та первинного аналізу інформації з обох пристроїв, враховуючи необхідність захисту даних від несанкціонованого доступу або втрати.

Поясніть, як ви будете оцінювати достовірність отриманих даних, визначати їхню доказову силу та документувати всі етапи процесу. Окремо опишіть методи цифрової криміналістики, які можуть бути використані для відновлення видалених файлів, аналізу мережевих логів, перегляду історії доступу та відстеження електронних слідів користувача. Зробіть акцент на практичних інструментах та програмному забезпеченні, які забезпечують ефективний збір і обробку доказів. Поясніть, як результати аналізу можуть бути представлені у суді та яким чином вони підвищують ефективність розслідування. Обговоріть можливі труднощі та ризики під час роботи з цифровими доказами та способи їх мінімізації.

Завдання № 2

Уявіть, що під час розслідування правоохоронці отримали доступ до серверу організації, де зберігаються важливі електронні дані, пов'язані з можливим правопорушенням. Ваше завдання – визначити, які дії необхідно здійснити для збору доказів так, щоб вони залишалися достовірними та допустимими у суді. Опишіть покроково процес збору та фіксації інформації з сервера, включаючи методи захисту даних від зміни або втрати. Поясніть, які інструменти цифрової криміналістики ви б застосували для аналізу журналів подій, мережевого трафіку та відновлення видалених файлів. Додатково обґрунтуйте, як ви будете оцінювати достовірність отриманих доказів, класифікувати їх за значимістю та підготувати до представлення у суді.

ТЕМА № 3. Використання штучного інтелекту в правоохоронній діяльності: можливості та ризики

План лекції:

1. Основи та значення штучного інтелекту у

правоохоронній діяльності

2. Ризики та етичні аспекти застосування штучного інтелекту
3. Практичні кейси використання ШІ у слідчій та судовій діяльності
4. Використання алгоритмів машинного навчання для аналізу тенденцій і профілактики правопорушень
5. Технології розпізнавання облич і аналізу великих даних у роботі правоохоронних органів
6. Контроль та мінімізація ризиків при використанні ШІ у правоохоронній діяльності

Питання для семінарського заняття:

- Що таке штучний інтелект і які основні принципи його роботи у правоохоронній діяльності?
- Яке значення ШІ у сучасних правоохоронних органах і які його основні можливості?
- Які ризики можуть виникати при застосуванні ШІ у слідчій та судовій практиці?
- Як забезпечити етичне та правомірне використання ШІ у роботі правоохоронних органів?
- Наведіть приклади практичного застосування ШІ у слідчих або судових процесах.
- Як алгоритми машинного навчання можуть допомогти прогнозувати злочинність та запобігати правопорушенням?
- У чому полягають переваги та обмеження технологій розпізнавання облич і аналізу великих даних у правоохоронній діяльності?
- Які заходи контролю та методи мінімізації ризиків слід застосовувати при використанні ШІ?
- Яким чином результати аналізу ШІ можуть впливати на рішення слідчих та судові висновки?
- Обговоріть можливі помилки або упередження, які можуть виникати при роботі алгоритмів ШІ, і як їх уникнути.

Завдання № 1

Ви отримали завдання оцінити ефективність застосування штучного інтелекту для аналізу даних про правопорушення в місті. Опишіть, які типи даних і джерела інформації слід використати для навчання алгоритмів ШІ. Визначте потенційні ризики та обмеження при застосуванні технологій ШІ у цьому випадку. Складіть план дій, який включає підготовку даних, перевірку достовірності результатів та заходи контролю за алгоритмами, щоб мінімізувати помилки і упередження. Поясніть, яким чином результати аналізу можуть допомогти слідчим у прийнятті рішень та які етичні аспекти слід враховувати під час використання ШІ.

Завдання № 2

Муніципальна поліція планує впровадити систему штучного інтелекту для аналізу повідомлень про правопорушення та прогнозування районів підвищеного ризику злочинності.

Завдання**:**

1. Складіть перелік типів даних, які можна використовувати для навчання алгоритмів (наприклад, історія правопорушень, соціальні мережі, камери спостереження).
2. Визначте потенційні ризики застосування ШІ та запропонуйте способи їх мінімізації (помилки алгоритмів, упереджені дані, порушення приватності).
3. Обговоріть, як результати прогнозування можуть допомогти у плануванні патрулів і профілактичній роботі, та які етичні аспекти слід враховувати.
4. Складіть покроковий план перевірки результатів системи та контролю за алгоритмами.
5. Презентуйте свої висновки групі, аргументуючи практичну користь та обмеження впровадження ШІ.

ТЕМА № 4. Забезпечення інформаційної безпеки держави та суспільства в умовах глобалізації

План лекції:

1. Поняття, принципи, структура інформаційної безпеки. Інформаційний суверенітет та національні інтереси.
2. Вплив цифрових платформ, транснаціональних медіа та глобальних інформаційних потоків на державну політику.
3. Інформаційні операції, дезінформація, психологічний вплив, кібератаки на критичну інфраструктуру.
4. Нормативно-правове регулювання інформаційної безпеки
5. Інституційна система забезпечення інформаційної безпеки
6. Захист державних інформаційних ресурсів, реагування на інциденти, кіберстійкість.

Питання для семінарського заняття:

1. У чому полягає співвідношення понять «інформаційна безпека», «кібербезпека» та «національна безпека»?
2. Чи можна вважати інформаційний суверенітет складовою державного суверенітету? Обґрунтуйте свою позицію.
3. Яким чином глобальні цифрові платформи впливають на формування громадської думки та державну політику?
4. У чому особливості інформаційних операцій як інструменту гібридної війни?
5. Які механізми протидії дезінформації є найбільш ефективними в демократичному суспільстві?
6. Охарактеризуйте основні загрози для об’єктів критичної інфраструктури в умовах кібервійни.
7. Які основні нормативно-правові акти України регулюють сферу інформаційної безпеки?

8. Яку роль відіграє Рада національної безпеки і оборони України у формуванні державної політики у сфері інформаційної безпеки?
9. У чому полягають повноваження Служба безпеки України у сфері захисту інформаційного простору?
10. Які функції виконує Державна служба спеціального зв'язку та захисту інформації України у сфері кіберзахисту?
11. Яким чином міжнародне співробітництво (зокрема в межах Європейський Союз та НАТО) впливає на розвиток системи інформаційної безпеки України?
12. Що означає поняття «кіберстійкість» держави та які фактори забезпечують її формування?

Завдання № 1

У період проведення важливих політичних рішень в Україні в інформаційному просторі різко зростає кількість публікацій у соціальних мережах та онлайн-медіа, які містять ознаки маніпуляції, перекручення фактів та поширення недостовірної інформації. Одночасно фіксуються кібератаки на офіційні державні сайти та спроби несанкціонованого доступу до інформаційних ресурсів органів влади.

Завдання:

1. Визначте, які види загроз інформаційній безпеці мають місце у наведеній ситуації.
2. Охарактеризуйте можливі наслідки для держави та суспільства.
3. Запропонуйте алгоритм дій державних органів щодо реагування на такі загрози.
4. Вкажіть, які органи державної влади повинні бути залучені до вирішення ситуації (з урахуванням повноважень Рада національної безпеки і оборони України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації України).
5. Обґрунтуйте, яким чином у цій ситуації має бути забезпечений баланс між свободою слова та захистом національної безпеки.

Завдання № 2

Проаналізуйте чинну систему нормативно-правового забезпечення інформаційної безпеки України.

Завдання**:**

1. Визначте основні нормативно-правові акти, що регулюють сферу інформаційної безпеки (закони, стратегії, підзаконні акти).
2. Проаналізуйте, які повноваження у сфері інформаційної безпеки мають:
   - Рада національної безпеки і оборони України;
   - Служба безпеки України;
   - Державна служба спеціального зв'язку та захисту інформації України.
3. Оцініть ефективність існуючої моделі координації між цими органами.
4. Визначте можливі прогалини або проблемні аспекти у правовому регулюванні.
5. Запропонуйте власні рекомендації щодо вдосконалення законодавства з урахуванням європейських стандартів (підходи Європейський Союз та практики держав — членів НАТО).

ТЕМА № 5. Соціальні мережі та цифрові платформи як інструменти розслідування та джерела загроз

План лекції:

1. Правова природа, функції та алгоритмічні механізми формування контенту.
2. Поняття цифрового сліду, методи збору та верифікації інформації з соціальних мереж.
3. Особливості фіксації, збереження та оцінки доказів у кримінальному процесі.
4. Соціальні мережі як інструмент протиправної діяльності.
5. Моніторинг платформ, аналітика зв'язків, дотримання прав людини.
6. Національне законодавство та підходи Європейський Союз до регулювання онлайн-сервісів.

7. Захист персональних даних та право на приватність у соціальних мережах.

Питання для семінарського заняття:

1. Які основні функції соціальних мереж та цифрових платформ у сучасному суспільстві?
2. Що таке цифровий слід, і чому він є важливим для розслідувань?
3. Які методи збору та верифікації інформації з соціальних мереж вважаються ефективними та законними?
4. У чому полягають особливості фіксації, збереження та оцінки електронних доказів у кримінальному процесі?
5. Які види протиправної діяльності найчастіше відбуваються через соціальні мережі?
6. Яким чином правоохоронні органи здійснюють моніторинг платформ та аналітику зв'язків користувачів?
7. Які ризики виникають при порушенні прав людини під час моніторингу соціальних мереж?
8. Як національне законодавство України регулює діяльність онлайн-платформ та збір електронних доказів?
9. Які підходи застосовує Європейський Союз до регулювання онлайн-сервісів і чому вони важливі для України?
10. Як забезпечується захист персональних даних та право на приватність користувачів соціальних мереж?
11. Яким чином можна забезпечити баланс між ефективністю розслідувань та правами людини у цифровому просторі?
12. Чи можна використати штучний інтелект для моніторингу контенту у соціальних мережах без порушення законодавства?

Завдання № 1

Студентська група отримала завдання проаналізувати інформаційну кампанію у соціальній мережі, яка активно

поширює певну подію чи тему (наприклад, захід, суспільну ініціативу або політичну подію). Частина інформації є достовірною, частина – маніпулятивною.

Завдання:

1. Визначте основні джерела інформації та типи контенту (тексти, зображення, відео, коментарі).
2. Проаналізуйте, які повідомлення мають ознаки дезінформації або маніпуляції.
3. Вкажіть, який цифровий слід залишають користувачі та як його можна використати у розслідуванні (з дотриманням закону).
4. Запропонуйте методи перевірки достовірності інформації.
5. Визначте ризики для користувачів та суспільства у цій інформаційній кампанії.
6. Розробіть рекомендації для державних органів або організаторів платформи щодо протидії поширенню шкідливого контенту.

Завдання № 2

У соціальній мережі виявлено групу користувачів, які поширюють недостовірну інформацію про роботу державних органів та організовують флешмоби, що можуть дестабілізувати ситуацію у місті. Одночасно відбуваються спроби несанкціонованого доступу до акаунтів користувачів та адміністрування платформ.

Завдання:

1. Група 1 – аналізує інформаційний простір, визначає джерела загроз і пропонує алгоритм реагування.
2. Група 2 – оцінює механізми модерації контенту, алгоритми блокування фейків і дезінформації, взаємодію з державними органами.
3. Група 3 – перевіряє достовірність інформації, досліджує цифровий слід та оцінює потенційний вплив на суспільну думку.
4. Група 4– оцінює ризики для приватності, права на свободу слова та пропонує механізми самозахисту.

Завдання:

- Визначити види загроз, що виникають у цій ситуації (дезінформація, кібератаки, маніпуляції).
- Розробити план дій для кожної групи з урахуванням законодавства та етичних норм.

- Обґрунтувати баланс між безпекою, правом на приватність і свободою слова.
- Презентувати результати в групах та обговорити можливі рішення для державних та приватних структур.

ТЕМА № 6. Міжнародні стандарти прав людини в цифровому просторі та їх застосування у правоохоронній діяльності

План лекції

1. Сутність цифрових прав, основні ризики та виклики для користувачів онлайн.
2. Міжнародні стандарти та документи з прав людини
3. Ключові права людини в інтернеті та цифровому просторі
4. Збір електронних доказів, моніторинг соцмереж, баланс між безпекою та правами громадян.
5. Виклики та перспективи розвитку цифрових прав людини

Питання для семінарського заняття:

1. Що таке цифрові права людини і чим вони відрізняються від традиційних прав людини?
2. Які основні ризики та загрози для користувачів цифрового простору існують сьогодні?
3. Які міжнародні документи регулюють права людини в інтернеті та цифровому середовищі?
4. Як принципи міжнародних стандартів прав людини можна застосувати у діяльності правоохоронних органів?
5. Які права людини найбільше порушуються під час моніторингу соціальних мереж та цифрових платформ?
6. Які етичні та правові обмеження слід враховувати під час збору електронних доказів?
7. Як забезпечити баланс між національною безпекою та правами громадян у цифровому просторі?
8. Які перспективи розвитку цифрових прав людини на міжнародному рівні існують і як вони впливають на українське законодавство?

9. Чи можна використати сучасні технології, наприклад штучний інтелект, для захисту цифрових прав людини?
10. Які проблеми виникають при імплементації міжнародних стандартів у національне право та правоохоронну практику?

Завдання № 1

Правоохоронні органи отримали повідомлення про групу користувачів у соціальних мережах, які поширюють заклики до порушення закону. Водночас частина інформації є недостовірною або маніпулятивною. Планується збір електронних доказів та аналіз активності користувачів із використанням спеціальних цифрових інструментів.

Завдання**:**

1. Визначте, які права людини можуть бути порушені під час моніторингу соціальних мереж та збору електронних доказів.
2. Проаналізуйте, які міжнародні стандарти прав людини слід врахувати під час розслідування.
3. Запропонуйте план дій правоохоронних органів, який забезпечує дотримання балансу між безпекою суспільства та правами громадян.
4. Вкажіть, які технологічні та правові засоби можна використати для захисту персональних даних під час розслідування.
5. Розробіть короткі рекомендації для контролю за законністю дій правоохоронців у цифровому середовищі.

Завдання № 2

Влада планує розслідування діяльності групи користувачів у соціальних мережах, які поширюють інформацію, що потенційно загрожує національній безпеці. При цьому деякі користувачі можуть постраждати через порушення їхніх цифрових прав (право на приватність, свободу слова, захист персональних даних).

1. Група 1 – збирають і аналізують цифрові докази, складають план реагування на загрозу.
2. Група 2 – контролюють дотримання прав людини та міжнародних стандартів під час розслідування.

3. Група 3– оцінюють механізми модерації контенту та блокування шкідливих матеріалів.
4. Група 4– відстоюють право на приватність і свободу слова, аналізують потенційні ризики для суспільства.

Завдання:

1. Визначити основні права людини, що можуть бути порушені під час розслідування.
2. Розробити план дій для своєї групи з урахуванням законодавства та етичних норм.
3. Скласти алгоритм співпраці між групами для забезпечення балансу між безпекою та правами користувачів.
4. Обговорити можливі ризики використання технологій (AI, автоматизовані системи) у розслідуванні.
5. Презентувати результати групового аналізу та запропоновані рішення для забезпечення цифрових прав людини.

ТЕМА № 7. Етичні та правові аспекти цифрового нагляду та контролю інформаційних потоків

План лекції

1. Сутність цифрового нагляду, основні види інформаційних потоків та методи їх контролю.
2. Принципи етичного моніторингу, ризики порушення прав людини, баланс між безпекою та свободою громадян.
3. Національне законодавство України, міжнародні стандарти та рекомендації щодо цифрового контролю.
4. Збір електронних доказів, аналітика інформаційних потоків, обмеження на доступ до персональних даних.
5. Порушення приватності, надмірна централізація даних, проблеми ефективності та безпеки технологій.
6. Технології для прозорого контролю, міжнародні тенденції, використання AI з дотриманням прав людини.

Питання для семінарського заняття:

1. Що таке цифровий нагляд і як він відрізняється від традиційного контролю інформаційних потоків?
2. Які основні види інформаційних потоків підлягають контролю у цифровому просторі?
3. Які принципи етичного моніторингу слід враховувати під час цифрового нагляду?
4. Які права людини можуть бути порушені при надмірному цифровому контролі?
5. Як забезпечити баланс між безпекою суспільства та свободою громадян?
6. Які положення національного законодавства України регулюють цифровий нагляд?
7. Які міжнародні стандарти та рекомендації впливають на практику цифрового контролю?
8. Які особливості збору електронних доказів у цифровому середовищі слід враховувати?
9. Які ризики створює надмірна централізація даних та автоматизація цифрового нагляду?
10. Які технології можна використовувати для прозорого та етичного контролю інформаційних потоків?
11. Як штучний інтелект може допомогти або нашкодити дотриманню прав людини під час цифрового нагляду?
12. Які приклади порушень приватності у цифровому просторі можна навести з міжнародної практики?
13. Як організації можуть запровадити внутрішні механізми контролю для дотримання етичних та правових норм?
14. Які наслідки для суспільства можуть виникнути через неетичний або незаконний цифровий нагляд?
15. Як державні органи та громадськість можуть співпрацювати для прозорого та законного цифрового контролю?

Завдання № 1

Місцеві правоохоронні органи запровадили систему моніторингу цифрових каналів комунікацій у місті для запобігання поширенню дезінформації та кібератак. Водночас частина даних,

що збираються, стосується особистої інформації громадян (переписки, поведінкові патерни, геолокація). Є ризик порушення права на приватність та свободи слова.

Завдання:

1. Визначте основні етичні та правові ризики, що виникають у цій ситуації.
2. Проаналізуйте, які права людини можуть бути порушені під час цифрового нагляду.
3. Складіть план дій для правоохоронних органів, який забезпечує баланс між безпекою та захистом прав громадян.
4. Вкажіть, які міжнародні стандарти та національні норми слід враховувати під час збору та обробки даних.
5. Розробіть рекомендації для прозорого використання технологій моніторингу, включно з AI, щоб уникнути порушень прав людини.

Завдання № 2

Ви – консультанти з етики та прав людини у міжнародній організації з цифрового нагляду. Вас запрошено для оцінки нового проєкту уряду, який планує використовувати AI для моніторингу соціальних мереж та месенджерів з метою виявлення фейкових новин та запобігання кібератакам.

Під час тестового запуску системи було виявлено, що алгоритм автоматично виділяє “підозрілі” повідомлення, але водночас збирає особисті дані користувачів та їхні політичні вподобання.

Завдання:

1. Визначте три головні етичні проблеми та ризики порушення прав людини у цій ситуації.
2. Складіть короткий “кодекс цифрового етикету” для урядового проєкту, який мінімізує порушення приватності.
3. Розробіть креативну стратегію прозорого використання AI: як можна повідомляти громадянам, що їхні дані збираються, і як забезпечити безпеку та анонімність.
4. Створіть міні-сценарій (5–6 речень) того, як могла б виглядати “добра практика” цифрового нагляду, що поважає права людини.

ТЕМА № 8. Прогнозування та реагування на цифрові загрози: стратегічний підхід для сучасних правоохоронців

План лекції

1. Сутність цифрових загроз та їх класифікація (кіберзлочинність, дезінформація, витоки даних, атаки на критичну інфраструктуру).
2. Основні джерела інформації для прогнозування: відкриті дані, соціальні мережі, внутрішні системи правоохоронних органів.
3. Аналітичні методи прогнозування: трендовий аналіз, моделювання сценаріїв, використання AI та машинного навчання.
4. Інструменти раннього попередження та оцінки ризиків цифрових загроз.
5. Етичні та правові аспекти збору та обробки даних для прогнозування загроз.

Питання для семінарського заняття:

1. Що таке цифрові загрози і чим вони відрізняються від традиційних загроз?
2. Які основні види цифрових загроз існують: кіберзлочинність, дезінформація, витоки даних, атаки на критичну інфраструктуру?
3. Як класифікація цифрових загроз допомагає правоохоронним органам у плануванні стратегій реагування?
4. Які джерела інформації можна використовувати для прогнозування цифрових загроз?
5. Які переваги та обмеження мають відкриті джерела інформації (Open Source Intelligence) для прогнозування кібератак?
6. Як соціальні мережі можуть слугувати джерелом даних для аналізу та прогнозування цифрових загроз?
7. Які внутрішні системи правоохоронних органів допомагають збирати дані про кіберзлочинність та інші цифрові загрози?
8. Що таке трендовий аналіз у прогнозуванні загроз і як його застосовують на практиці?
9. Як моделювання сценаріїв допомагає оцінювати потенційні наслідки цифрових атак?

10. Які можливості та ризики використання AI та машинного навчання для прогнозування цифрових загроз?
11. Які інструменти раннього попередження використовують для зменшення ризиків кіберінцидентів?
12. Як оцінюється рівень ризику цифрової загрози та пріоритетність реагування?
13. Які етичні аспекти необхідно враховувати при зборі та обробці даних для прогнозування цифрових загроз?
14. Які правові норми обмежують збір та обробку персональних даних у правоохоронній діяльності?
15. Як забезпечити баланс між ефективністю прогнозування цифрових загроз та захистом прав людини?

Завдання № 1

Ви – аналітики кібербезпеки в міському Центрі цифрового реагування. Нещодавно у місті зросла кількість повідомлень про підозрілі онлайн-активності: фейкові новини про аварії на транспорті, масові спроби фішингу на місцеві банки та підозрілі атаки на енергетичну мережу.

Завдання:

1. Проаналізуйте отриману інформацію та класифікуйте цифрові загрози за видами: кіберзлочинність, дезінформація, витоки даних, атаки на критичну інфраструктуру.
2. Визначте джерела даних, які допоможуть прогнозувати наступні кібератаки (врахуйте соцмережі, відкриті джерела, внутрішні системи правоохоронних органів).
3. Складіть короткий прогноз на найближчий тиждень: які загрози можуть посилитися, та які сценарії розвитку подій можливі.
4. Пропишіть рекомендації щодо дій для правоохоронних органів та операторів критичної інфраструктури, щоб мінімізувати шкоду від цих загроз.
5. Додатково: намалюйте “Щит цифрової безпеки”, який відображає ваші стратегічні кроки для захисту міста.

Завдання № 2

Ви – члени спеціальної групи “Кіберщит”, що відповідає за захист міста від цифрових загроз. Сьогодні до вашого відділу

надходить тривожна інформація: кілька анонімних акаунтів у соціальних мережах почали поширювати неправдиві повідомлення про вибухи на транспорті, паралельно реєструються підозрілі спроби доступу до систем водопостачання та електромережі.

Завдання:

1. Визначте, які типи цифрових загроз одночасно проявляються (дезінформація, кібератаки, витоки даних).
2. Пропишіть стратегічний план дій у форматі “Місія Кіберщит” з трьома рівнями:
   - Рівень 1 – негайне реагування: що зробити в перші 30 хвилин.
   - Рівень 2 – контроль ситуації: як стабілізувати інфраструктуру та зменшити паніку.
   - Рівень 3 – запобігання: які дії слід запровадити, щоб уникнути повторних атак.
3. Придумайте інноваційний інструмент або технологію (реальний або фантастичний AI), який допоможе вашій команді ефективніше відстежувати загрози та захищати дані.
4. Створіть короткий “документ безпеки для громадян”, який пояснює, як держава реагує на цифрові загрози та як громадяни можуть себе захистити.
5. Для креативності: намалюйте або опишіть емблему команди “Кіберщит” і поясніть, що символізує кожен елемент

3. САМОСТІЙНА РОБОТА ЗДОБУВАЧІВ ОСВІТИ

Підготовка до семінарських занять допомагає глибше вивчити основні теми освітньої компоненти "*Правоохоронна діяльність в інформаційну епоху: глобальні виклики та забезпечення безпеки в умовах цифрових технологій*", а самостійна робота сприяє кращому засвоєнню матеріалу, є формування у студентів цілісного уявлення про місце та роль прокуратури в механізмі державної влади й системі забезпечення правопорядку, засвоєння теоретичних і практичних засад організації та здійснення прокурорської діяльності. Дисципліна спрямована на оволодіння знаннями щодо:

- сучасних видів кіберзлочинності та методів їх протидії;
- збору, оцінки та використання електронних доказів у слідчій та судовій практиці;
- застосування штучного інтелекту у правоохоронній діяльності та управлінні ризиками;
- забезпечення інформаційної безпеки держави та суспільства в умовах глобалізації;
- прав людини в цифровому середовищі та їх дотримання під час правоохоронної діяльності;
- етичних та правових аспектів цифрового нагляду та контролю інформаційних потоків.

Самостійна робота здійснюється у таких формах:

1. Вивчення та аналіз навчальної літератури, наукових статей і нормативно-правових актів, що дозволяє студентам поглибити розуміння основних понять та принципів правоохоронної діяльності в цифровому середовищі.
2. Виконання практичних завдань, кейсів і дослідницьких робіт, що сприяє застосуванню теоретичних знань на практиці та розвитку навичок аналітичного мислення.
3. Підготовка та захист презентацій і звітів, яка формує навички публічного виступу, аргументованого обґрунтування та структурованого викладу матеріалу.
4. Проведення самостійного аналізу статистичних даних та тенденцій кіберзлочинності, що допомагає студентам

зрозуміти сучасні виклики в інформаційній сфері та механізми їх оцінки.

5. Складання алгоритмів реагування на інциденти у цифровому середовищі, що розвиває вміння планувати заходи з кібербезпеки та оцінювати ефективність запобіжних дій.
6. Виконання практичних завдань з цифрової криміналістики, включаючи збір, обробку та оцінку електронних доказів для забезпечення їх достовірності та допустимості у суді.
7. Моделювання реальних кейсів правопорушень та аналіз дій правоохоронних органів, що дозволяє розвивати навички прийняття рішень у складних професійних ситуаціях.
8. Оцінка етичних і правових аспектів використання технологій, включно зі штучним інтелектом, що формує усвідомлення ризиків і відповідальності при роботі в цифровому середовищі.
9. Робота з нормативно-правовими документами та міжнародними стандартами, що забезпечує розуміння застосування законодавства та міжнародного досвіду у сфері інформаційної безпеки та прав людини.
10. Самостійне вивчення сучасних інструментів моніторингу та аналізу інформаційних потоків, що розвиває практичні навички контролю, оцінки загроз та підготовки рекомендацій для забезпечення безпеки у цифровому середовищі.

4. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Однією з форм організації навчального процесу в умовах кредитно-модульної системи є індивідуальна робота здобувачів освіти.

Індивідуальна робота студентів з навчальної дисципліни "*Правоохоронна діяльність в інформаційну епоху: глобальні виклики та забезпечення безпеки в умовах цифрових технологій"* може включати:

- написання наукових статей, тез наукових доповідей, рефератів та їх презентація на семінарських заняттях;
- участь у студентських конференціях, конкурсах, олімпіадах, наукових засіданнях, науково-практичних семінарах, колоквіумах тощо;
- аналіз наукової та навчальної літератури, нормативно-правових актів і практичних кейсів для глибшого розуміння теми;
- підготовка індивідуальних завдань, практичних вправ та кейс-стаді з використанням цифрових технологій і методів кібербезпеки;
- розробка алгоритмів реагування на інформаційні загрози та кібератаки у теоретичних і практичних завданнях;
- вивчення методів цифрової криміналістики, збору, обробки та оцінки електронних доказів;
- оцінка етичних і правових аспектів застосування сучасних технологій у правоохоронній діяльності;
- аналіз статистичних даних та тенденцій кіберзлочинності, прогнозування потенційних ризиків;
- самостійне опанування сучасних інструментів моніторингу та аналізу інформаційних потоків, формування рекомендацій для забезпечення безпеки в цифровому середовищі;
- підготовка презентацій і звітів за результатами самостійної роботи та їх обговорення на практичних;

- ознайомлення з міжнародними стандартами та практиками у сфері цифрових прав людини та інформаційної безпеки, застосування їх у національному контексті.

Вибір видів індивідуальної роботи здійснюється студентом за власними інтересами та попереднім узгодженням з викладачем. Тематику та форму індивідуальної роботи студент отримує на початку навчального року і здає роботу у визначені строки. Організацію, контроль та оцінювання якості виконання індивідуальної роботи студентів здійснює науковий керівник. Індивідуальна робота подається на кафедру для перевірки до початку екзаменаційної сесії.

Теми для написання рефератів

(есе, наукових статей, тез наукових доповідей, презентацій)

1. Кіберзлочинність у цифровому суспільстві: види та сучасні тенденції.
2. Методи протидії фішингу та соціальній інженерії.
3. Шкідливе програмне забезпечення: віруси, трояни, ransomware і способи захисту.
4. Атаки на критичну інфраструктуру: механізми, наслідки та профілактика.
5. Цифрова криміналістика: основи та практичне застосування у слідстві.
6. Збір, збереження та оцінка електронних доказів.
7. Використання штучного інтелекту у правоохоронній діяльності: перспективи та ризики.
8. Машинне навчання для прогнозування злочинності та профілактики правопорушень.
9. Технології розпізнавання облич та аналіз великих даних у роботі правоохоронних органів.
10. Етичні та правові аспекти застосування ШІ у кримінальному процесі.
11. Інформаційна безпека держави: поняття, принципи та структура.
12. Інформаційний суверенітет та національні інтереси України в цифрову епоху.
13. Вплив цифрових платформ та глобальних медіа на формування громадської думки.
14. Інформаційні операції, дезінформація та психологічний вплив на суспільство.
15. Нормативно-правове регулювання кібербезпеки в Україні.
16. Інституційна система забезпечення інформаційної безпеки держави.
17. Захист державних інформаційних ресурсів та кіберстійкість.
18. Соціальні мережі та цифрові платформи як інструменти розслідувань.

19. Цифровий слід: методи збору та верифікації інформації з онлайн-платформ.
20. Соціальні мережі як інструмент протиправної діяльності.
21. Захист персональних даних та право на приватність у цифровому середовищі.
22. Міжнародні стандарти прав людини в цифровому просторі.
23. Баланс між національною безпекою та цифровими правами громадян.
24. Збір електронних доказів та моніторинг соціальних мереж із дотриманням прав людини.
25. Цифровий нагляд та контроль інформаційних потоків: етичні та правові аспекти.
26. Технології прозорого контролю та використання AI для етичного моніторингу.
27. Надмірна централізація даних та ризики порушення приватності.
28. Превентивні заходи кібербезпеки для організацій та держави.
29. Міжнародне співробітництво у сфері кібербезпеки: приклади та ефективність.
30. Використання цифрових слідів і аналітики даних для розслідування злочинів та прогнозування загроз.

Вимоги до оформлення тез доповідей. Обсяг тез – від 3 до 6 сторінок формату А-4 (включно із рисунками, таблицями, фотографіями, переліком літератури). Технічні параметри: Формат файлу – *.doc, *.docx або *.rtf. Шрифт – гарнітура Times New Roman, кегль 14 пт, інтервал 1,5 пт. Поля (усі) – 20 мм. Назва доповіді – напівжирний шрифт, кегль 14 пт. Прізвища авторів – нежирний шрифт, кегль 14 пт. Посада, місце роботи, назва організації, місто – курсив, 14 пт. Основний Текст – нежирний, кегль 14 пт. Порядок оформлення таблиць, формул, підписів всередині рисунків: Шрифт – гарнітура Times New Roman, кегль 12 пт, курсив. Підписи таблиць – ставляться над таблицею, вирівнювання по правому краю.Формули – набирати у редакторі формул MS Equation або Mathtype.

5. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Гулак Г. М., Гринь А. К., Мельник С. В. Методологія захисту інформації : навч.-метод. посіб. Київ : Вид-во НА СБ України, 2015. 251 с.
3. Вавіленкова А. І. Методи і моделі протидії кібератакам : навч. посіб. Київ, 2023. 142 с.
4. Кобозева А. А., Мачалін І. О., Хорошко В. О. Аналіз захищеності інформаційних систем : підручник. Київ : ДУІКТ, 2010. 316 с.
5. Конахович Г. Ф., Корченко О. Г., Юдін О. К. Захист інформації в мережах передачі даних : підручник. Київ : ТОВ НВП «Інтерсервіс», 2009. 714 с.
6. Гайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. Київ : BHV, 2009. 608 с.
7. Богуш В. М., Юдін О. К. Інформаційна безпека держави. Київ : МК-Прес, 2005. 432 с.
8. Андрєєв В. І. та ін. Основи інформаційної безпеки : підручник. Київ : ДУІКТ, 2009. 292 с.
9. Основи кіберпростору, кібербезпеки та кіберзахисту : навч. посіб. / В. М. Богуш та ін. Київ : Ліра-К, 2021. 554 с.
10. Луценко В. М., Прогонов Д. О. Методи та засоби технічного захисту інформації : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2021. 289 с.
11. Організаційно-правові основи забезпечення кібербезпеки : підручник / за заг. ред. М. М. Присяжнюка. Київ : Ліра-К, 2023. 320 с.
12. Бурячок В. Л. та ін. Технології забезпечення безпеки мережевої інфраструктури. Київ : КУБГ, 2019. 218 с.
13. Харченко В. С., Яковлев С. В. та ін. Забезпечення функціональної безпеки критичних інформаційно-керуючих систем : монографія. Харків : Константа, 2019. 272 с.

14. Богуш В. М., Бровко В. Д., Настрадін В. П. Кіберпростір: основи кібербезпеки та кіберзахисту. Ч. 3. Київ : Нац. акад. СБУ, 2020. 272 с.
15. Левченко О. Система забезпечення інформаційної безпеки держави у воєнній сфері : монографія. Житомир : Євро-Волинь, 2021. 172 с.
16. Когут Ю. І. Кібервійна та безпека об'єктів критичної інфраструктури : практ. посіб. Київ : Сідкон, 2021. 332 с.
17. Самойленко О. А. Діяльність правоохоронних органів у протидії кіберзлочинності : навч.-метод. посіб. Одеса, 2020. 133 с.
18. Хахановський В. Г., Корнейко О. В. Актуальні питання інформаційного права : навч. посіб. Київ : НАВС, 2024. 258 с.
19. Корнейко О. В. та ін. Сучасні інформаційні технології в юридичній діяльності : навч. посіб. Київ : НАВС, 2024. 205 с.
20. Комаров М. Ю. Методи та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах критичної інфраструктури : дис. ... канд. техн. наук. Київ, 2021. 171 с.
21. Садовнік В. П., Багатко А. С. Застосування штучного інтелекту в розслідуванні транснаціональної злочинності: роль прокуратури та міжнародно-правові стандарти. *Наукові інновації та передові технології. Серія «Право».* 2026. № 2 (54). С. 33–55.
22. Цимбалюк В. І., Багатко А. С. Правове регулювання кібербезпеки в Україні: сучасні виклики та перспективи розвитку. *Український політико-правовий дискурс*. 2025. № 18. С. 1–17.
23. Цимбалюк В. І., Багатко А. С. Міжнародне співробітництво у сфері кібербезпеки: роль України в умовах гібридної війни. *Науковий вісник УжНУ. Серія «Право».* Вип. 92. С. 34–42.
24. Цимбалюк В. І., Багатко А. С. Кібербезпека об'єктів критичної інфраструктури України: актуальні проблеми

та шляхи вирішення. *Наукові інновації та передові технології. Серія «Право».* 2026. № 2 (54). С. 3490–3498.

Допоміжна:

1. Кудінов В. А., Яровий К. В. Інформаційне забезпечення правоохоронної діяльності : навч.-практ. посіб. Київ : Нац. акад. внутр. справ, 2024. 120 с.
2. Інформаційно-аналітичне забезпечення правоохоронної діяльності : навч. посіб. / Е. В. Рижков, Ю. П. Синиціна, С. О. Прокопов та ін. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2024. 180 с.
3. Використання сучасних інформаційних технологій у діяльності Національної поліції України : матеріали Всеукр. наук.-практ. семінару (28 листоп. 2019 р., м. Дніпро). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. 124 с.
4. Інформаційне забезпечення юридичної діяльності : підручник / кол. авт. ; за ред. В. Б. Вишні. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 245 с.
5. Бондар В. С., Рибалкін А. О. Інформаційне забезпечення досудового розслідування колабораційної діяльності. *Науковий вісник Ужгородського університету. Серія «Право».* 2023. Т. 2, вип. 79. С. 225–231.
6. Вареник О. С. Тенденції міжнародного співробітництва у сфері кібербезпеки. *Юридичний науковий електронний журнал*. 2024. № 11. С. 591–593.
7. Кононенко В. П. Інформаційна безпека як стан. *Науковий вісник Ужгородського університету.* 2023. Т. 2, вип. 76. С. 244–250.
8. Поляков О. М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. *Інформація і право*. 2021. № 2 (37). С. 129–138.
9. Тарасюк А. В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі.

Прикарпатський юридичний вісник. 2020. Вип. 1. С. 133–136.
10. Тєтєвін М. С. Досвід України у сфері міжнародного співробітництва в галузі кібербезпеки. *Науковий вісник Ужгородського національного університету.* 2024. Вип. 82, ч. 3. С. 263–266.
11. Черниш Р. В. Міжнародний організаційний досвід у сфері забезпечення кібербезпеки. *Вісник кримінального правосуддя.* 2023. № 3–4. С. 112–121.
12. Бєлкін Л. М., Юринець Ю. Л., Бєлкін М. Л., Криволап Є. В. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law».* 2022. № 3 (64). С. 78–86.
13. Колосовський Є. Ю. Сучасний стан кібербезпеки в Україні в умовах воєнного періоду. *Юридичний науковий електронний журнал*. 2023. № 12. С. 402–405.
14. Ширяєв Д. О. Кібербезпека та сучасний світ. *Актуальні проблеми сучасної науки в дослідженнях молодих учених, курсантів та студентів.* 2023. С. 600–602.
15. Синиціна Ю. Актуальні питання підготовки фахівців у галузі інформаційних технологій для органів Національної поліції України. *Сучасні інформаційні технології в діяльності Національної поліції* : матеріали Всеукр. наук.-практ. конф. (м. Дніпро, 02 листоп. 2023 р.). Дніпро : ДДУВС, 2024. С. 171–174.
16. Биков І. О. Інформаційно-аналітичне забезпечення діяльності слідчих та оперативних підрозділів у боротьбі з економічними злочинами. *Право і суспільство*. 2024. № 1, т. 2. С. 392–396.
17. Старостін О. Ю. Забезпечення інформаційної безпеки як складової національної безпеки України. *Вісник кримінологічної асоціації України.* 2024. № 1 (31). С. 446–474.
18. Паращук Л. Я., Паращук С. М. Рекомендації щодо використання інформаційних систем для покращення

ситуаційної обізнаності органів військового управління. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2025. № 1. С. 46–54.
19. Зоренко Д. До питання процедури фіксації результатів OSINT у контексті розслідування воєнних злочинів. *Сучасні реалії протидії воєнним злочинам: набутий досвід та погляд у майбутнє* : матеріали панел. дискусії VII Харківського міжнар. юрид. форуму (25 верес. 2023 р.). Київ : Алерта, 2023. 146 с.
20. Латковська Т., Марущак А. Інтеграція штучного інтелекту у діяльність правоохоронних органів: ризики в контексті кібербезпеки. *Право та державне управління*. 2025. № 1. С. 355–361.
21. Глиняний І. В., Марчук В. В. Електронні сервіси в правоохоронній діяльності як елемент протидії корупції. *Правові новели*. 2025. № 25. С. 206–212.
22. Інформаційна безпека : навч. вид. / за ред. Ю. Я. Бобала, І. В. Горбатого. Львів : Вид-во Львівської політехніки, 2019. 590 с.
23. Присяжнюк М. М. Інформаційна безпека та кібербезпека держави. Київ : Ліра-К, 2024. 224 с.