

**Державна наукова установа
«Інститут інформації, безпеки і права
Національної академії правових наук України»**

ЗАТВЕРДЖЕНО

Директор ДНУ ІІБП НАПрН України

В. Пилипчук

Наказ № 41 від «16» листопада 2026 р.



ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

РОБОЧА НАВЧАЛЬНА ПРОГРАМА

підготовки аспірантів із спеціальності D8 Право

Укладач: Ткачук Т. Ю.,
доктор юридичних наук, професор

Ухвалено Вченою радою
ДНУ ІІБП НАПрН України
Протокол № 6 від 14.10.2026р.

Київ, 2026

АНОТАЦІЯ

Навчальна дисципліна «Правове забезпечення кібербезпеки» формує у здобувачів третього (освітньо-наукового) рівня вищої освіти системне розуміння правового регулювання кібербезпеки, кіберстійкості, кіберзахисту, протидії кіберзлочинності та доказування у цифровому середовищі. Оновлена редакція враховує трансформацію національної системи кібербезпеки України у 2025–2026 роках, євроінтеграційні зобов'язання України, досвід протидії російській кіберагресії, розвиток штучного інтелекту, цифрових доказів та транскордонного доступу до електронних даних, а також сучасні підходи до управління кіберризиками і стійкості критичної інфраструктури.

Особлива увага приділяється ризик-орієнтованому правовому управлінню кібербезпекою, правовим аспектам реагування на кіберінциденти, директивам NIS2 і CER, Регламентам DORA та Cyber Resilience Act, застосуванню AI Act, електронним доказам відповідно до e-Evidence, правовим межах OSINT, протидії deepfake та counter-forensics, безпеці ланцюгів постачання, а також міжнародно-правовій кваліфікації кібероперацій у збройному конфлікті.

Мета дисципліни

Мета дисципліни – сформувати у здобувачів здатність здійснювати поглиблений юридичний аналіз відносин у сфері кібербезпеки, визначати правові ризики та обов'язки суб'єктів, оцінювати правомірність і належність процедур реагування на кіберінциденти та роботи з цифровими доказами, готувати правові висновки й пропозиції щодо вдосконалення законодавства України з урахуванням права Європейського Союзу, міжнародних стандартів та практики кіберпротидії в умовах війни.

Завдання дисципліни

- розуміти сучасну архітектуру національної системи кібербезпеки України, повноваження її суб'єктів та правові механізми координації;
- аналізувати національні, міжнародні та європейські нормативно-правові акти у сфері кібербезпеки, кіберстійкості, критичної інфраструктури та протидії кіберзлочинності;
- застосовувати ризик-орієнтований підхід до юридичної оцінки кіберризиків, кіберінцидентів, вразливостей, ланцюгів постачання та обов'язків з повідомлення про інциденти;
- визначати правові межі застосування OSINT, обробки персональних даних, збереження та використання цифрових доказів, у тому числі у справах про воєнні злочини;
- оцінювати правові наслідки використання штучного інтелекту, генеративних систем, deepfake та автономних/агентних систем у контексті кібербезпеки;
- готувати юридично обґрунтовані локальні акти, правові висновки, матриці відповідності та пропозиції щодо вдосконалення регулювання;
- застосовувати методи порівняльного правознавства і правового прогнозування до нових технологічних викликів, включаючи постквантову криптографію, цифровий суверенітет і безпеку цифрових продуктів.

У результаті вивчення дисципліни здобувач повинен

знати:

- систему чинного законодавства України у сфері кібербезпеки, кіберзахисту та критичної інфраструктури;
- правовий статус, компетенцію та механізми взаємодії основних суб'єктів національної системи кібербезпеки;
- основні положення NIS2, CER, DORA, Cyber Resilience Act, AI Act, e-Evidence та інших релевантних актів ЄС;

- міжнародно-правові механізми протидії кіберзлочинності й транскордонного одержання електронних доказів;
- правові стандарти захисту персональних даних, приватності, конфіденційної та іншої інформації з обмеженим доступом;
- актуальні моделі кіберзагроз 2026 року: DDoS, ransomware, supply-chain attacks, експлуатацію вразливостей, соціальну інженерію з використанням ШІ, deepfake, атаки на хмарні, OT/ICS та AI-системи;
- правові підходи до атрибуції та кваліфікації кібероперацій у збройному конфлікті.

вміти:

- здійснювати доктринальне і порівняльно-правове тлумачення норм у сфері кібербезпеки;
- кваліфікувати юридично значущі обставини кіберінциденту, визначати обов'язки суб'єктів щодо реагування, повідомлення, збереження даних і доказів;
- проводити правовий аудит політик кібербезпеки та кіберстійкості організації, не підміняючи юридичний аналіз технічним аудитом;
- оцінювати законність збирання й обробки відкритих даних, доказову цінність цифрових матеріалів та ризики маніпулювання/контрфорензики;
- здійснювати правову оцінку використання систем ШІ, генеративного контенту і deepfake, включаючи вимоги прозорості, безпеки та захисту основоположних прав;
- готувати правові висновки, compliance-матриці, проєкти локальних нормативних актів і науково обґрунтовані пропозиції щодо змін законодавства.

ЗМІСТ

1. Опис навчальної дисципліни
2. Мета та завдання кредитного модуля
3. Структура кредитного модуля
4. Лекційні заняття
5. Практичні заняття
6. Самостійна робота
7. Контрольні заходи
8. Рейтингова система оцінювання результатів навчання
9. Методичні рекомендації
10. Рекомендована література та нормативні джерела
11. Орієнтовні питання до заліку

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Галузь знань, спеціальність, рівень	Загальні показники	Характеристика кредитного модуля
Галузь знань: D Бізнес, адміністрування та право	Назва дисципліни: «Правове забезпечення кібербезпеки»	Форма навчання: заочна
Спеціальність: D8 Право	Кількість кредитів ECTS: 4	Статус: вибіркова компонента
Ступінь вищої освіти: доктор філософії	Загальна кількість годин: 120	Цикл: навчальні дисципліни за напрямом дослідження
	Кількість розділів: 2	Рік підготовки: 2026–2027 н. р.
	Лекції: 18 год.	Семестровий контроль: залік
	Практичні заняття: 18 год.	
	Самостійна робота: 84 год.	
	Мова викладання: українська	

2. МЕТА ТА ЗАВДАННЯ КРЕДИТНОГО МОДУЛЯ

Метою викладання навчальної дисципліни є формування в аспірантів системного, науково обґрунтованого та практично орієнтованого розуміння правових засад кібербезпеки й кіберстійкості, здатності аналізувати національне, міжнародне та європейське регулювання, оцінювати юридичні наслідки кіберінцидентів і новітніх технологій, а також розробляти правові механізми захисту прав, законних інтересів, інформаційних ресурсів та критичної інфраструктури.

Програма виходить із міждисциплінарної природи кібербезпеки, проте для здобувачів спеціальності D8 Право пріоритет надається юридичній кваліфікації, правовому управлінню ризиками, доказуванню, правам людини, комплаєнсу, відповідальності та правотворчим рішенням. Технічні аспекти розглядаються у межах, необхідних для коректного юридичного аналізу.

Програмні компетентності

Інтегральна компетентність (ІК): здатність продукувати нові ідеї, розв'язувати комплексні проблеми професійної та/або дослідницько-інноваційної діяльності у сфері права, застосовувати методологію наукової та педагогічної діяльності, проводити власне наукове дослідження, результати якого мають наукову новизну, теоретичне та практичне значення.

- ЗК01. Здатність генерувати нові ідеї (креативність).
- ЗК02. Здатність розробляти наукові проекти та управляти ними.
- ЗК04. Здатність усно і письмово презентувати результати власного наукового дослідження українською та іноземною мовами, глибоко розуміти іншомовні наукові та професійні тексти за напрямом досліджень.
- СК01. Здатність планувати та виконувати оригінальні дослідження, досягати наукових результатів, які створюють нові знання у галузі права та дотичних міждисциплінарних напрямках.
- СК02. Здатність застосовувати методи правового і міждисциплінарного дослідження, виявляти їх евристичні можливості та межі, використовувати релевантний дослідницький інструментарій.
- СК03. Здатність здійснювати науково-педагогічну діяльність у вищій освіті та проектах правничої освіти у системі освіти дорослих.
- СК04. Здатність виявляти, ставити та вирішувати проблеми дослідницького характеру у сфері права та забезпечувати якість виконуваних досліджень; дотримуватися права інтелектуальної власності та стандартів академічної доброчесності.

- СК05. Здатність моделювати оптимальні варіанти вирішення складних правових проблем, прогнозувати можливі наслідки їх реалізації.
- СК06. Здатність здійснювати експертну діяльність у сфері права.
- СК07. Здатність виявляти нові інституційні та етичні виклики в житті суспільства і пропонувати правові механізми їх розв'язання.

Програмні результати навчання

- ПРН01. Мати передові концептуальні та методологічні знання у сфері права і на межі предметних галузей, а також дослідницькі навички, достатні для проведення наукових і прикладних досліджень, отримання нових знань та здійснення інновацій.
- ПРН03. Застосовувати у фаховій діяльності знання та розуміння системи права, сучасної правової доктрини, основних напрямів і провідних тенденцій розвитку права.
- ПРН04. Формулювати і перевіряти гіпотези; використовувати належні аргументи, наукові джерела й результати прикладних досліджень; аналізувати проблему з урахуванням широкого правового та загальносоціального контекстів.
- ПРН05. Планувати і виконувати теоретичні та прикладні дослідження з права та дотичних міждисциплінарних напрямів з використанням сучасного наукового інструментарію та дотриманням стандартів академічної і професійної етики.
- ПРН06. Розуміти загальні принципи та методи юридичної науки й методологію наукових досліджень, застосовувати їх у власних дослідженнях і викладацькій практиці.
- ПРН07. Застосовувати сучасні інструменти і технології пошуку, оброблення, аналізу й збереження даних та інформації, спеціалізоване програмне забезпечення, бази даних та інформаційні системи у науковій, викладацькій, правотворчій та правозастосовній діяльності.
- ПРН10. Готувати правові висновки, пропозиції та рекомендації за результатами правового дослідження.
- ПРН11. Здійснювати доктринальне тлумачення норм національного, міжнародного та права Європейського Союзу, здійснювати порівняльний аналіз правових явищ і процесів у різних правових системах.

3. СТРУКТУРА КРЕДИТНОГО МОДУЛЯ

№	Змістовні модулі	Всього	Лекції	Практичні	Індивід.	Самост.
Розділ 1. ПРАВОВІ ТА ІНСТИТУЦІЙНІ ЗАСАДИ КІБЕРБЕЗПЕКИ ТА КІБЕРСТІЙКОСТІ						
1.1	Національна система кібербезпеки України: правова архітектура, governance та реформа 2025–2026	18	4	2	–	12
1.2	Кіберризики, кіберінциденти та юридична відповідальність: ризик-орієнтоване управління	14	2	2	–	10
1.3	Право ЄС та міжнародно-правові механізми кібербезпеки і протидії кіберзлочинності	16	2	2	–	12
	Всього за розділ 1	48	8	6	–	34
Розділ 2. ПРАВОВЕ РЕГУЛЮВАННЯ СУЧАСНИХ КІБЕРТЕХНОЛОГІЙ І ЦИФРОВОЇ СТІЙКОСТІ						
2.1	OSINT, цифрові докази та e-Evidence: правові межі, верифікація і протидія counter-forensics	22	4	4	–	14
2.2	Штучний інтелект, deepfake і кібербезпека: AI Act, права людини та ризики автономних/агентних систем	18	2	2	–	14
2.3	Кіберстійкість критичної інфраструктури, ланцюгів постачання та продуктів із цифровими елементами	16	2	2	–	12
2.4	Кібероперації під час збройного конфлікту, міжнародна відповідальність і технологічні тренди 2026	16	2	4	–	10
	Всього за розділ 2	72	10	12	–	50
	РАЗОМ	120	18	18	–	84

4. ЛЕКЦІЙНІ ЗАНЯТТЯ

Лекція 1. Національна система кібербезпеки України: правова архітектура, управління та реформа 2025–2026 (4 год.)

Основні питання:

1. Трансформація правового регулювання кібербезпеки України після змін 2025 року: понятійний апарат, система суб'єктів, координація, оцінювання стану кіберзахисту, реагування на кіберінциденти та робота з вразливостями.
2. Повноваження основних суб'єктів національної системи кібербезпеки; роль РНБО, НКЦК, Держспецзв'язку, СБУ, Національної поліції, Міністерства оборони, НБУ та інших суб'єктів.
3. Чинна Стратегія кібербезпеки України та напрями її оновлення. Проєкт Стратегії кібербезпеки України 2026–2031: проактивна кібероборона, кіберстійкість, цифровий суверенітет, державно-приватне партнерство, людський капітал.
4. Ризик-орієнтоване управління кібербезпекою: ISO/IEC 27001:2022, NIST Cybersecurity Framework 2.0 та функція GOVERN як компаративні інструменти правового governance.

Питання для самоперевірки:

1. Які ключові зміни відбулися в правовій архітектурі національної системи кібербезпеки у 2025–2026 роках?
2. Які функції та межі компетенції мають основні суб'єкти національної системи кібербезпеки?
3. Чим відрізняються стратегічні документи, нормативно-правові акти та технічні стандарти у сфері кібербезпеки?
4. Які правові наслідки має перехід від моделі «захисту інформації» до управління кіберризиками та кіберстійкості?

Лекція 2. Кіберризики, кіберінциденти та юридична відповідальність (2 год.)

Основні питання:

1. Актуальний ландшафт загроз: DDoS, ransomware, supply-chain attacks, експлуатація вразливостей, фішинг і соціальна інженерія з використанням ШІ, FIMI та атаки на хмарні/OT/ICS-системи.
2. Юридично значущі ознаки кіберінциденту: кваліфікація, повідомлення, ескалація, документування, збереження даних, взаємодія з компетентними органами.
3. Правова відповідальність та due diligence: цивільно-правові, адміністративні, кримінально-правові й договірні аспекти; відповідальність керівництва та постачальників.
4. Координоване розкриття вразливостей, vulnerability management та правові межі security research.

Питання для самоперевірки:

1. Як правова кваліфікація інциденту впливає на обсяг обов'язків організації?
2. Які докази та журнали подій необхідно зберігати для подальшого правозастосування?
3. Як розмежовуються юридична відповідальність, управлінська відповідальність та технічна відповідальність за кіберризик?
4. Які правові ризики виникають під час дослідження вразливостей?

Лекція 3. Право ЄС та міжнародно-правові механізми кібербезпеки і протидії кіберзлочинності (2 год.)

Основні питання:

1. NIS2, CER, DORA та Cyber Resilience Act: предмет регулювання, адресати, вимоги до ризик-менеджменту, стійкості, ланцюгів постачання та повідомлення про інциденти.

2. Євроінтеграційний вимір: наближення українського законодавства і практик до acquis ЄС у сфері кібербезпеки.
3. Будапештська конвенція про кіберзлочинність та Другий додатковий протокол: міжнародне співробітництво та електронні докази.
4. Конвенція ООН проти кіберзлочинності 2024 року: предмет, статус і значення для майбутньої системи міжнародного співробітництва.

Питання для самоперевірки:

1. Які відмінності між NIS2, CER, DORA та CRA за предметом і колом адресатів?
2. Яке значення мають строки та порядок повідомлення про значні інциденти за NIS2?
3. Які механізми транскордонного отримання електронних доказів передбачає сучасне міжнародне регулювання?
4. Які положення актів ЄС доцільно враховувати під час подальшого розвитку законодавства України?

Лекція 4. OSINT, цифрові докази та e-Evidence: правові межі, верифікація і протидія counter-forensics (4 год.)

Основні питання:

1. Правові підстави і межі OSINT: публічність інформації, приватність, персональні дані, інтелектуальна власність, законність автоматизованого збирання даних.
2. Цифровий доказ як юридична категорія: походження (provenance), автентичність, цілісність, фіксація часу, хешування, журналювання, chain of custody та відтворюваність дослідження.
3. Регламент ЄС e-Evidence: Європейські ордери на надання та збереження електронних доказів; транскордонна взаємодія з провайдерами.
4. OSINT у документуванні воєнних злочинів. Deepfake, синтетичний контент, counter-forensics та методи юридичного забезпечення достовірності цифрових матеріалів.
5. Сучасний інструментарій OSINT: пошукові оператори, архівування вебконтенту, Shodan/Censys, Maltego, Meta Content Library/API (за наявності правомірного доступу), перевірка метаданих та геолокації.

Питання для самоперевірки:

1. Коли відкрите джерело не означає автоматично правомірне використання інформації?
2. Які елементи процесу збирання необхідно документувати для забезпечення доказової придатності OSINT-матеріалу?
3. Які юридичні ризики виникають при використанні автоматизованих OSINT-інструментів?
4. Як counter-forensics та генеративний ШІ впливають на оцінку автентичності цифрових доказів?

Лекція 5. Штучний інтелект, deepfake і кібербезпека: AI Act, права людини та ризики автономних/агентних систем (2 год.)

Основні питання:

1. AI Act у 2026 році: ризик-орієнтована модель, заборонені практики, обов'язки щодо GPAI, вимоги прозорості для взаємодії з ШІ та маркування deepfake/синтетичного контенту.
2. ШІ як інструмент і об'єкт кібератак: AI-enhanced phishing, генерація шкідливого коду, adversarial machine learning, prompt injection, data poisoning, model theft та ризики агентних систем.
3. Кібербезпека GPAI і систем із системним ризиком; співвідношення AI Act з вимогами захисту персональних даних, авторського права та основоположних прав.
4. Юридичні проблеми використання ШІ у секторі безпеки і оборони, автономних системах та під час збройного конфлікту.

Питання для самоперевірки:

1. Які вимоги AI Act стали особливо актуальними у 2026 році?
2. Які юридичні наслідки має використання deepfake у доказуванні, інформаційних операціях та комунікаціях?
3. Як розподіляються обов'язки між provider, deployer та іншими суб'єктами життєвого циклу AI-системи?
4. Які правові ризики створюють автономні/агентні системи для кібербезпеки?

Лекція 6. Кіберстійкість критичної інфраструктури, ланцюгів постачання та цифрових продуктів (2 год.)

Основні питання:

1. Правове регулювання критичної інфраструктури і критичної інформаційної інфраструктури в Україні. Секторальна відповідальність і безперервність надання життєво важливих послуг.
2. CER і NIS2 як взаємопов'язані моделі стійкості критичних суб'єктів. OT/ICS, хмарні послуги, MSP/MSSP та залежність від зовнішніх постачальників.
3. Cyber Resilience Act: secure-by-design, vulnerability handling, обов'язки виробників та інших економічних операторів щодо продуктів із цифровими елементами.
4. Управління ланцюгами постачання: правові вимоги до договорів, закупівель, SBOM, vulnerability disclosure, резервного копіювання та recovery.

Питання для самоперевірки:

1. Чим кіберстійкість відрізняється від кіберзахисту?
2. Які ризики третіх сторін мають бути враховані в договорах і політиках закупівель?
3. Як CRA змінює підхід до відповідальності за безпеку цифрових продуктів?
4. Які елементи має містити локальний акт про кіберстійкість критичного суб'єкта?

Лекція 7. Кібероперації під час збройного конфлікту, міжнародна відповідальність і технологічні тренди 2026 (2 год.)

Основні питання:

1. Міжнародно-правова кваліфікація кібероперацій: суверенітет, невтручання, застосування сили, державна відповідальність, атрибуція та контрзаходи.
2. Міжнародне гуманітарне право та кібероперації у збройному конфлікті: принципи розрізнення, пропорційності та запобіжних заходів; дискусійні питання щодо даних як об'єкта нападу.
3. Tallinn Manual 2.0 як доктринальне, не обов'язкове джерело та межі його використання у правовій аргументації.
4. Технологічні тренди 2026 року: постквантова міграція, AI-native security, цифровий суверенітет, кіберрезерв, колективна кібероборона, безпека космічних і супутникових систем.

Питання для самоперевірки:

1. Які критерії використовуються для міжнародно-правової оцінки кібератаки?
2. Чим технічна атрибуція відрізняється від юридичної та політичної?
3. Які норми міжнародного гуманітарного права можуть застосовуватися до кібероперацій у війні?
4. Які правові наслідки для держави та організацій має перехід до постквантової криптографії?

5. ПРАКТИЧНІ ЗАНЯТТЯ

Практичне заняття 1. Правова карта національної системи кібербезпеки (2 год.)

Завдання:

Побудувати актуальну карту нормативно-правових актів та компетенцій органів у сфері кібербезпеки України станом на дату виконання. Окремо проаналізувати зміни, пов'язані із

Законом України № 4336-IX, та підготувати короткий legal memo щодо розподілу відповідальності за умовного значного кіберінциденту в державній установі.

Завдання на самостійну роботу:

Порівняти підхід українського законодавства до governance кіберризиків з функцією GOVERN NIST CSF 2.0 та вимогами ISO/IEC 27001:2022. Результат – матриця «норма/вимога – суб'єкт – обов'язок – доказ виконання».

Практичне заняття 2. Кейс реагування на ransomware / supply-chain incident (2 год.)

Завдання:

На основі змодельованого інциденту визначити юридично значущі факти, кваліфікувати інцидент, сформулювати перелік невідкладних юридичних дій, адресатів повідомлення, правил збереження журналів та цифрових доказів, договірних і регуляторних ризиків. Окремо проаналізувати порівняльні строки повідомлення за NIS2.

Завдання на самостійну роботу:

Підготувати односторінковий incident legal checklist для керівника організації.

Практичне заняття 3. Європейський кіберкомплаєнс (2 год.)

Завдання:

Скласти порівняльну compliance-матрицю NIS2, CER, DORA і CRA для одного обраного суб'єкта (оператор критичної послуги, фінансова установа, хмарний провайдер або виробник продукту з цифровими елементами). Визначити, які положення можуть бути релевантними для адаптації українського законодавства.

Завдання на самостійну роботу:

Підготувати 2–3 сторінки правового висновку з конкретними пропозиціями щодо приведення внутрішньої політики організації у відповідність до обраної моделі регулювання.

Практичне заняття 4. OSINT та цифрові докази (2 год.)

Завдання:

Виконати документований OSINT-мінікейс виключно з правомірно доступних відкритих джерел. Для кожного матеріалу зафіксувати URL/ідентифікатор, час доступу, спосіб отримання, контекст, хеш (за наявності файлу), метадані та обмеження достовірності. Скласти chain-of-custody log та оцінити правові підстави обробки персональних даних.

Завдання на самостійну роботу:

Порівняти можливості e-Evidence, Другого додаткового протоколу до Будапештської конвенції та традиційної міжнародної правової допомоги для умовного транскордонного запиту про електронні докази.

Практичне заняття 5. AI Act, deepfake та політика безпечного використання генеративного ШІ (2 год.)

Завдання:

Проаналізувати кейс використання генеративного ШІ для створення/модифікації аудіо- або відеоконтенту. Визначити застосовні вимоги AI Act щодо прозорості, ризику для приватності, авторського права, доказування і кібербезпеки. Розмежувати факт використання ШІ та юридичну оцінку наслідків.

Завдання на самостійну роботу:

Розробити проєкт короткої внутрішньої політики використання генеративного ШІ для юридичного або кібербезпекового підрозділу: класифікація даних, заборонені сценарії, human oversight, журналювання, перевірка результатів, інцидент-репортинг.

Практичне заняття 6. Локальний акт про кіберстійкість критичного суб'єкта (2 год.)

Завдання:

Розробити проєкт локального нормативного акта про кіберстійкість умовного об'єкта критичної інфраструктури. Документ має охоплювати governance, ролі й відповідальність, управління ризиками, third-party/supply-chain risk, vulnerability management, резервування та відновлення, реагування на інциденти, журналювання, захист цифрових доказів, хмарні та AI-сервіси.

Завдання на самостійну роботу:

Підготувати таблицю відповідності проєкту українському законодавству та релевантним вимогам NIS2/CER/CRA.

Практичне заняття 7. Moot court: правова оцінка державної кібероперації (4 год.)

Завдання:

У групах проаналізувати змодельовану кібероперацію проти критичної інфраструктури під час міжнародного збройного конфлікту. Окремо оцінити фактичну базу атрибуції, суверенітет, невтручання, можливе застосування сили, норми міжнародного гуманітарного права, державну відповідальність та допустимі заходи реагування. Позиції сторін повинні спиратися на норми міжнародного права і чітко відділяти lex lata від доктринальних підходів.

Завдання на самостійну роботу:

Підготувати policy brief (до 2 сторінок) на одну з тем: «Правове забезпечення постквантової міграції», «Цифровий суверенітет і технологічні залежності», «Кіберрезерв і правовий статус залучених фахівців», «Кібербезпека супутникових сервісів».

6. САМОСТІЙНА РОБОТА

Самостійна робота аспіранта спрямована на поглиблене опрацювання першоджерел, судової та правозастосовної практики, документів ЄС, міжнародних договорів, технічних стандартів у тій частині, у якій вони мають юридичне значення, а також на підготовку власних аргументованих правових висновків. Пріоритет надається офіційним текстам актів і документам компетентних органів; вторинні джерела мають використовуватися критично.

1. Порівняльний аналіз Закону України «Про основні засади забезпечення кібербезпеки України» у чинній редакції та змін 2025 року; визначення нових/змінених інститутів кіберзахисту.
2. Порівняння ISO/IEC 27001:2022 та NIST CSF 2.0 з точки зору їх можливого використання як орієнтирів юридичного governance і доказу належної обачності.
3. Підготовка таблиці правових обов'язків за NIS2 (управління ризиками, governance, incident reporting, supply-chain security) та аналіз можливостей їх імплементації в Україні.
4. Аналіз CER, DORA та CRA із визначенням відмінностей між організаційною стійкістю, цифровою операційною стійкістю та безпекою продуктів із цифровими елементами.
5. Підготовка короткого дослідження щодо e-Evidence та Другого додаткового протоколу до Будапештської конвенції: гарантії прав людини, юрисдикційні конфлікти та взаємодія з провайдерами.
6. Розроблення протоколу верифікації OSINT-матеріалів і цифрових доказів із урахуванням deepfake та counter-forensics.
7. Правовий аналіз застосування AI Act до генеративних систем: прозорість, deepfake, GPAI, кібербезпека, права людини та авторське право.

8. Аналіз одного публічно документованого кіберінциденту проти критичної інфраструктури України за останні три роки: факти, правова кваліфікація, інституційна реакція, lessons learned.
9. Наукова записка щодо одного тренду 2026 року: agentic AI, post-quantum transition, digital sovereignty, software supply-chain security, SBOM, space cybersecurity або collective cyber defence.

7. КОНТРОЛЬНІ ЗАХОДИ

Замість тестів, орієнтованих переважно на запам'ятовування базових технічних термінів, контроль здійснюється через юридичні кейси, аналітичні записки та аргументовані правові висновки. Така форма відповідає третьому (освітньо-науковому) рівню та дозволяє оцінювати не лише знання нормативного матеріалу, а й здатність кваліфікувати факти, працювати з джерелами, будувати юридичну аргументацію і прогнозувати наслідки.

Передбачаються два модульні контрольні заходи:

- за результатами розділу 1 – письмовий case brief / legal memo щодо кіберінциденту та регуляторних обов'язків суб'єкта;
- за результатами розділу 2 – письмовий аналітичний висновок щодо цифрового доказу, AI/deepfake, критичної інфраструктури або міжнародно-правової кваліфікації кібероперації.

Під час виконання контрольних робіт здобувач повинен чітко посилаючись на первинні джерела, розрізняти чинне право (lex lata), проекти нормативних/стратегічних актів, рекомендаційні стандарти та доктринальні позиції.

8. РЕЙТИНГОВА СИСТЕМА ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Рейтингова шкала дисципліни становить 100 балів: $R = RC + RE = 40 + 60 = 100$ балів.

Стартова складова RC (до 40 балів):

- виконання семи практичних кейсів – до 28 балів (по 4 бали);
- інтегрований research/legal memo – до 8 балів;
- аргументована участь у фахових обговореннях із посиланням на первинні джерела – до 4 балів.

Залікова складова RE (до 60 балів):

- вирішення комплексного юридичного кейсу – до 30 балів;
- порівняльно-правовий / доктринальний аналіз – до 20 балів;
- якість роботи з джерелами, коректність правової аргументації та висновків – до 10 балів.

Рейтинг, бали	ECTS	Традиційна оцінка	Залікова оцінка
95–100	A	Відмінно	Зараховано
85–94	B	Дуже добре	Зараховано
75–84	C	Добре	Зараховано
65–74	D	Задовільно	Зараховано
60–64	E	Достатньо	Зараховано
<60	FX/F	Незадовільно	Незараховано / недопущено за правилами закладу

9. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

1. Викладання будується на поєднанні нормативного аналізу, case method, comparative law, problem-based learning та елементів tabletop exercise. У кожній темі здобувач має відділяти технічний опис події від її юридично значущих ознак.

2. Основними джерелами є офіційні тексти законодавства України, акти ЄС, міжнародні договори, документи компетентних органів і стандарти. Наукові публікації використовуються для доктринального аналізу, але не підміняють первинні джерела.
3. У темах, пов'язаних із OSINT та цифровими доказами, обов'язковими є вимоги законності, мінімізації втручання у приватність, відтворюваності дій, фіксації provenance та chain of custody. Практичні завдання не повинні передбачати несанкціонований доступ, обхід захисту або інше втручання в інформаційні системи.
4. У темах AI/deepfake необхідно розрізняти технічну ймовірність того, що контент згенеровано ШІ, юридичний стандарт доказування та вимоги конкретного регуляторного режиму. Висновки про автентичність не можуть ґрунтуватися лише на одному автоматизованому детекторі.
5. Проєкт Стратегії кібербезпеки України 2026–2031 використовується як матеріал для правового прогнозування та аналізу державної політики; до моменту офіційного затвердження його не слід цитувати як чинний нормативно-правовий акт.
6. Під час роботи з актами ЄС здобувачі мають перевіряти актуальну редакцію, дату застосування та перехідні положення. Особливо це стосується AI Act та Cyber Resilience Act, де окремі вимоги набувають чинності поетапно.
7. Для аспірантів пріоритетними є завдання, що завершуються юридичним продуктом: legal memo, policy brief, compliance matrix, проєкт локального акта, висновок щодо доказів або науково обґрунтована пропозиція до законодавства.

10. РЕКОМЕНДОВАНА ЛІТЕРАТУРА ТА НОРМАТИВНІ ДЖЕРЕЛА

Нормативні акти України та офіційні стратегічні документи

1. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII (у чинній редакції). URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
3. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27.03.2025 № 4336-IX. URL: <https://zakon.rada.gov.ua/laws/show/4336-20#Text>
4. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX (у чинній редакції). URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>
5. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
6. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
7. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
8. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
9. Кримінальний кодекс України від 05.04.2001 № 2341-III (у чинній редакції). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>
10. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI (у чинній редакції). URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>
11. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013>

13. Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури: постанова Кабінету Міністрів України від 19.06.2019 № 518 (у чинній редакції). URL: <https://zakon.rada.gov.ua/laws/show/518-2019-п#Text>
14. Рада національної безпеки і оборони України. Стратегія кібербезпеки України 3.0: курс на кіберстійкість, цифровий суверенітет та проактивну кібероборону. 12.06.2026 (матеріал щодо проєкту Стратегії). URL: <https://www.rnbo.gov.ua/ua/Diialnist/7637.html>
15. Рада національної безпеки і оборони України. НКЦК: розповідаємо про функції, склад та проєкти. 16.09.2026. URL: <https://rnbo.gov.ua/ua/Diialnist/7801.html>

Право Європейського Союзу та міжнародні документи

1. Convention on Cybercrime (ETS No. 185), Budapest, 23.11.2001. Council of Europe. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>
2. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Council of Europe. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224>
3. United Nations Convention against Cybercrime, adopted by the UN General Assembly on 24.12.2024 (status and materials). URL: <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>
4. Directive (EU) 2022/2555 (NIS2) on measures for a high common level of cybersecurity across the Union. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
5. Directive (EU) 2022/2557 on the resilience of critical entities (CER). URL: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>
6. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA). URL: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
7. Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
8. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
9. European Commission. The enforcement framework of the AI Act (updated 24.08.2026). URL: <https://digital-strategy.ec.europa.eu/en/policies/enforcement-ai-act>
10. Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings. URL: <https://eur-lex.europa.eu/eli/reg/2023/1543/oj>
11. Directive (EU) 2023/1544 laying down harmonised rules on designated establishments and legal representatives for gathering electronic evidence. URL: <https://eur-lex.europa.eu/eli/dir/2023/1544/oj>
12. Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union. URL: <https://eur-lex.europa.eu/eli/reg/2023/2841/oj>
13. Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Стандарти, методичні та аналітичні джерела

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Edition 3; Amendment 1:2024). URL: <https://www.iso.org/standard/27001>
2. NIST. The Cybersecurity Framework (CSF) 2.0. 2024. URL: <https://www.nist.gov/cyberframework>
3. ENISA. ENISA Threat Landscape 2025. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
4. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / gen. ed. Michael N. Schmitt. Cambridge University Press, 2017 (доктринальне, не обов'язкове джерело).
5. Ткачук Т. Ю., Н. І. Ткачук, І. М. Ничитайло, А. І. Старосек. Технологія OSINT: інструменти та методи для захисту інформаційної безпеки: практичний посібник. Київ: НА СБУ, 2023. 180 с.

6. Пилипчук В. Г., Брижко В. М., Доронін І. М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху: монографія / за заг. ред. В. Г. Пилипчука. Київ–Одеса: Фенікс, 2020. 260 с.
7. Тарасюк А. В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи. Одеса: Фенікс, 2020. 404 с.
8. Ткачук Т. Ю., Оніщенко В. Г. Забезпечення достовірності цифрових доказів воєнних злочинів: механізми протидії counter forensics. Аналітично-порівняльне правознавство. 2025. Вип. 4, ч. 3. С. 310–317. DOI: 10.24144/2788-6018.2025.04.3.44.
9. Довгань О. Д., Ткачук Т. Ю. Протидія counter-forensics як складова цифрової безпеки критичної інфраструктури України. Інформація і право. 2025. № 2(53). С. 115–125. DOI: 10.37750/2616-6798.2025.2(53).334135.
10. Довгань О. Д., Ткачук Т. Ю., Тарасюк А. В. Counter forensics як загроза інформаційній безпеці України: проблематика судової експертизи цифрових доказів у реаліях війни. Науковий вісник Ужгородського національного університету. Серія: Право. 2025. Вип. 89, ч. 2. С. 402–409. DOI: 10.24144/2307-3322.2025.89.2.61.

11. ОРІЄНТОВНІ ПИТАННЯ ДО ЗАЛІКУ

1. Поняття, принципи та система правового забезпечення кібербезпеки України.
2. Національна система кібербезпеки України: склад, повноваження і координація суб'єктів.
3. Законодавчі зміни 2025 року у сфері захисту інформації та кіберзахисту: зміст і правове значення.
4. Чинна Стратегія кібербезпеки України та напрями, закладені у проєкті Стратегії 2026–2031 років.
5. Поняття кіберризиків, кіберінциденту, кібератаки, кіберзагрози та вразливості: юридичне значення.
6. Ризик-орієнтоване управління кібербезпекою: роль governance, ISO/IEC 27001:2022 та NIST CSF 2.0.
7. Правові обов'язки суб'єктів під час кіберінциденту: реагування, повідомлення, документування та збереження доказів.
8. Юридична відповідальність у сфері кібербезпеки: види, підстави та проблеми розмежування відповідальності.
9. NIS2: сфера дії, governance, управління ризиками, supply-chain security та incident reporting.
10. CER: правова модель стійкості критичних суб'єктів та її співвідношення з NIS2.
11. DORA: цифрова операційна стійкість фінансового сектору.
12. Cyber Resilience Act: вимоги до продуктів із цифровими елементами, secure-by-design та vulnerability handling.
13. Правове регулювання критичної інфраструктури та критичної інформаційної інфраструктури України.
14. Правові проблеми кібербезпеки ланцюгів постачання, хмарних послуг та зовнішніх постачальників.
15. Будапештська конвенція про кіберзлочинність: значення та основні механізми міжнародного співробітництва.
16. Другий додатковий протокол до Будапештської конвенції: електронні докази та співробітництво з провайдерами.
17. Конвенція ООН проти кіберзлочинності 2024 року: предмет, статус і потенційне значення.
18. Правові межі OSINT: відкриті дані, персональні дані, приватність, інтелектуальна власність.
19. Цифрові докази: автентичність, цілісність, provenance, chain of custody та відтворюваність.
20. e-Evidence: Європейські ордери на надання та збереження електронних доказів.
21. OSINT та цифрові докази у документуванні воєнних злочинів.

22. Counter-forensics як загроза достовірності цифрових доказів: правові та експертні проблеми.
23. Deepfake та синтетичний контент: правові ризики для доказування, приватності та інформаційної безпеки.
24. AI Act: ризик-орієнтована модель регулювання та її значення для кібербезпеки.
25. Вимоги прозорості AI Act щодо взаємодії з ШІ, deepfake та синтетичного контенту.
26. GPAI, системний ризик і кібербезпека моделей загального призначення.
27. ШІ як інструмент кібератак: AI-enhanced phishing, генерація шкідливого коду, adversarial ML та agentic AI.
28. Захист персональних даних і основоположних прав у системах ШІ та кібербезпеки.
29. Правове регулювання використання ШІ у секторі безпеки і оборони.
30. Міжнародно-правова атрибуція кібероперацій: технічний, юридичний та політичний виміри.
31. Суверенітет, принцип невторчання та заборона застосування сили у контексті кібероперацій.
32. Міжнародне гуманітарне право і кібероперації під час збройного конфлікту.
33. Державна відповідальність і допустимі заходи реагування на міжнародно-протиправні кібероперації.
34. Tallinn Manual 2.0: правова природа, значення і межі використання.
35. Кібербезпека і цифровий суверенітет: правові проблеми технологічної залежності.
36. Постквантова криптографія як майбутній правовий і організаційний виклик.
37. Кіберрезерв, державно-приватне партнерство та колективна кібероборона.
38. Правові аспекти кібербезпеки космічних і супутникових систем.
39. Актуальні тренди кіберзагроз 2026 року та їх вплив на розвиток права.
40. Напрями подальшої адаптації законодавства України до acquis ЄС у сфері кібербезпеки.