МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра права
Кафедра системного аналізу та інформаційних технологій

ЗАТВЕРДЖЕНО:
протокол засідання кафедри
«29» серпня 2025 року № 1

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «СУЧАСНЕ ПРАВОВЕ РЕГУЛЮВАННЯ В СФЕРІ ІТ»

Освітньо-професійна програма: Кібербезпека
Спеціальність: 125 Кібербезпека
Факультет: Економіко-правовий
2025 – 2026 навчальний рік

Київ, 2025-2026 рр.

Робоча програма навчальної дисципліни «Сучасне правове регулювання в сфері ІТ» для здобувачів вищої освіти першого (бакалаврського) рівня ОПП «Кібербезпека» спеціальності 125 «Кібербезпека» (галузь знань – 12 «Інформаційні технології»).

Розробник:
Волік Вячеслав Вікторович, професор кафедри права МДУ, доктор юридичних наук, професор

Контактна інформація:
Електронна адреса: v.volik@mdu.edu.ua
Консультації: онлайн через Viber, Telegram, WhatsApp; офлайн за попередньою домовленістю

1.Опис навчальної дисципліни

Показник	Денна форма	Заочна форма
Кількість кредитів	3 кредити ECTS	3 кредити ECTS
Загальна кількість годин	90 годин	90 годин
Рівень вищої освіти	Перший (бакалаврський)	Перший (бакалаврський)
Спеціальність	125 Кібербезпека	125 Кібербезпека
Освітньо-професійна програма	Кібербезпека	Кібербезпека
Статус дисципліни	Обов'язкова	Обов'язкова
Семестр	3-й (для бакалаврів 1-го року навчання)	3-й (для бакалаврів 1-го року навчання)
Аудиторні години	Лекції: 12 год. Семінарські: 12 год.	Лекції: 8 год. Семінарські: 8 год.
Самостійна робота	66 год. (включаючи 12 год. на індивідуальні завдання)	74 год. (включаючи 12 год. на індивідуальні завдання)
Індивідуальні завдання	Реферат, есе, кейсові завдання	Реферат, есе, кейсові завдання
Форма контролю	Залік	Залік
Співвідношення годин	Аудиторні: 24 год. (26,7%) Самостійна та індивідуальна робота: 66 год. (73,3%)	Аудиторні: 16 год. (17,8%) Самостійна та індивідуальна робота: 74 год. (82,2%)
Передумови для вивчення	Знання з дисциплін: «Основи права», «Основи інформаційної безпеки», «Інформатика та комп'ютерні технології»	Знання з дисциплін: «Основи права», «Основи інформаційної безпеки», «Інформатика та комп'ютерні технології»

Місце дисципліни в освітній програмі:

Дисципліна є обов'язковою складовою циклу професійної підготовки бакалаврів кібербезпеки, спрямована на формування правових знань і навичок щодо сучасного регулювання IT-сфери, включаючи цифрові технології, інтелектуальну власність, контракти та етичні аспекти в IT. Вона взаємопов'язана з дисциплінами «Основи права», «Основи інформаційних технологій» та «Інформатика та комп'ютерні технології».

2. Мета, завдання, компетентності та результати навчання

Мета навчальної дисципліни:

Формування у здобувачів вищої освіти бакалаврського рівня знань і практичних навичок щодо сучасного правового регулювання в сфері інформаційних технологій, включаючи національне законодавство України, міжнародні стандарти, правові механізми регулювання цифрових технологій, інтелектуальної власності, контрактів в IT та етичних аспектів у цифровій економіці. Дисципліна спрямована на підготовку фахівців, здатних аналізувати правові аспекти IT-проектів, розробляти заходи регулювання, реагувати на правові виклики в IT та прогнозувати їх наслідки в професійній діяльності.

Завдання навчальної дисципліни:

1. Ознайомлення з основними аспектами сучасного правового регулювання в сфері IT, включаючи:
    - аналіз національного законодавства України у сфері цифрових технологій;
    - вивчення міжнародних стандартів і конвенцій (наприклад, EU Digital Services Act, WIPO treaties);
    - правові механізми регулювання інтелектуальної власності в IT;
    - регулювання IT в умовах цифрової трансформації;
    - правові та етичні аспекти використання AI, блокчейн та інших технологій в IT;
    - захист даних, контракти в IT та відповідальність за порушення.
2. Формування навичок аналізу нормативно-правових актів, судової практики та міжнародних стандартів у сфері IT.
3. Розвиток умінь розробляти правові заходи для IT-проектів, реагувати на правові інциденти та прогнозувати їх наслідки.
4. Виховання професійної етики та відповідальності за дотримання принципів регулювання в IT.

Компетентності та результати навчання:

Тип компетентності	Опис
Інтегральна компетентність (ІК)	Здатність розв'язувати складні спеціалізовані задачі та практичні проблеми в галузі кібербезпеки з використанням нормативно-правових актів, міжнародних стандартів і методів інформаційної безпеки в умовах невизначеності.
Загальні компетентності (ЗК)	ЗК1. Здатність до абстрактного мислення, аналізу та синтезу (для аналізу нормативно-правових актів). ЗК2. Здатність застосовувати знання у практичних ситуаціях (для розробки заходів захисту інформації). ЗК5. Усвідомлення необхідності дотримання етичних принципів і норм професійної діяльності (для етичного підходу до кібербезпеки).
Фахові компетентності (ФК)	ФК2. Здатність застосовувати нормативно-правові акти та стандарти у сфері кібербезпеки. ФК3. Здатність розробляти та впроваджувати заходи щодо захисту інформації. ФК4. Здатність виявляти, аналізувати та реагувати на кіберінциденти.
Результати навчання (РН)	РН1. Знати та застосовувати нормативно-правову базу у сфері кібербезпеки. РН4. Виявляти та реагувати на кіберінциденти. РН6. Застосовувати міжнародні стандарти та практики у сфері кібербезпеки.

3. Зміст навчальної дисципліни

Тема 1. Поняття та принципи правового регулювання в ІТ

- **Зміст:** Визначення правового регулювання в ІТ. Основні принципи (інноваційність, захист прав, доступність). Закон України «Про електронні довірчі послуги».
- **Актуальні проблеми:** Недостатня адаптація законодавства до швидких технологічних змін, правові прогалини.
- **Документи для аналізу:** Закон України «Про електронні довірчі послуги» (2017).
- **Література:**

1. Кліщенко В.О. Сучасне правове регулювання ІТ. Київ: Юрінком Інтер, 2023. – С. 10–30.
2. Совгиря О.В. Правові основи ІТ-сфери. Київ: Ваіте, 2022. – С. 15–40.
3. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text.
4. Погребняк С.П. Принципи регулювання ІТ. Журнал східноєвропейського права. – 2022. – № 95. – С. 12–22. URL: https://doi.org/10.5281/zenodo.4701234.
5. Хоменко В.М. Законодавство України в ІТ. Право України. – 2022. – № 11. – С. 20–35.
6. Білак М. Нормативна база ІТ. Юридичний вісник. – 2021. – № 7. – С. 10–20.
7. ENISA. EU Digital Legislation Overview. 2022. – С. 5–15. URL: https://www.enisa.europa.eu/publications.
8. ISO/IEC 38500:2015. IT Governance. – С. 1–10. URL: https://www.iso.org/standard/62816.
9. NIST. Digital Identity Guidelines. 2021. – С. 10–20. URL: https://www.nist.gov/itl/digital-identity.
10. Кравець І.М. Основи правового регулювання ІТ: правовий аспект. Право України. – 2021. – № 10. – С. 15–25.

Тема 2. Національне законодавство у сфері ІТ

- **Зміст:** Закон України «Про електронну комерцію». Структура та функції державних органів у сфері ІТ (Мінцифри, НКРЗІ).
- **Актуальні проблеми:** Координація між органами, імплементація цифрової трансформації.
- **Документи для аналізу:** Закон України «Про електронну комерцію» (2003).
- **Література:**

1. Кравець І.М. Законодавство України в ІТ. Право України. – 2021. – № 9. – С. 15–25.
2. Совгиря О.В. Державні органи в ІТ-сфері. Київ: Ваіте, 2022. – С. 40–60.
3. Закон України «Про електронну комерцію» від 03.09.2003 № 675-IV (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/675-15#Text.
4. Білак М. Координація органів в ІТ. Юридичний вісник. – 2021. – № 8. – С. 10–20.
5. Погребняк С.П. Імплементація ІТ-законодавства. Вісник НАПрН України. – 2022. – № 6. – С. 12–22.
6. Хоменко В.М. Роль Мінцифри в ІТ. Актуальні проблеми державотворення. – 2022. – С. 100–110.
7. ENISA. National Digital Strategies. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
8. NIST. IT Governance Framework. 2021. – С. 15–25. URL: https://www.nist.gov/itl/it-governance.
9. Council of Europe. Digital Governance Report. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
10. Кліщенко В.О. Національні механізми ІТ-регулювання. Київ: Юрінком Інтер, 2023. – С. 50–70.

Тема 3. Міжнародні стандарти правового регулювання ІТ

- **Зміст:** EU Digital Services Act (DSA). Стандарти ISO/IEC 38500, NIST Digital Identity. Роль WIPO та ITU.
- **Актуальні проблеми:** Імплементація міжнародних стандартів в Україні, адаптація до нових технологій.
- **Документи для аналізу:** EU Digital Services Act (2022).
- **Література:**

1. Совгиря О.В. Міжнародні стандарти ІТ. Київ: Ваіте, 2022. – С. 60–80.
2. Кліщенко В.О. DSA та Україна. Право України. – 2021. – № 8. – С. 20–35.
3. European Commission. Digital Services Act. 2022 (оновлення 2023). URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.
4. Білак М. Імплементація ISO/IEC 38500. Юридичний вісник. – 2021. – № 8. – С. 10–20.
5. Погребняк С.П. Роль WIPO в ІТ. Вісник НАПрН України. – 2022. – № 6. – С. 12–22.
6. Хоменко В.М. Міжнародні стандарти ІТ. Актуальні проблеми державотворення. – 2022. – С. 110–120.
7. ISO/IEC 38500:2015. IT Governance. – С. 1–10. URL: https://www.iso.org/standard/62816.
8. NIST. Digital Identity Guidelines. 2021. – С. 20–30. URL: https://www.nist.gov/itl/digital-identity.
9. ENISA. Digital Standards Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кравець І.М. Міжнародне співробітництво в ІТ. Право України. – 2021. – № 10. – С. 25–35.

Тема 4. Правові аспекти захисту даних та приватності в ІТ

- **Зміст:** Закон України «Про захист персональних даних». GDPR. Механізми захисту в цифрових системах.
- **Актуальні проблеми:** Гармонізація з GDPR, приватність у хмарних ІТ.
- **Документи для аналізу:** Закон України «Про захист персональних даних» (2010), GDPR (2016).
- **Література:**

1. Кравець І.М. Захист даних в ІТ: правові аспекти. Право України. – 2021. – № 9. – С. 15–25.
2. Совгиря О.В. GDPR в ІТ. Київ: Ваіте, 2022. – С. 80–100.
3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.
4. General Data Protection Regulation (GDPR). 2016 (оновлення 2023). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.
5. Білак М. Гармонізація з GDPR в ІТ. Юридичний вісник. – 2021. – № 9. – С. 10–20.
6. Погребняк С.П. Приватність в ІТ. Вісник НАПрН України. – 2022. – № 7. – С. 15–25.
7. Хоменко В.М. Судова практика в ІТ-дані. Актуальні проблеми державотворення. – 2022. – С. 120–130.
8. Council of Europe. Convention 108+. 2018 (оновлення 2022). – С. 5–15. URL: https://www.coe.int/en/web/data-protection/convention108+.
9. ENISA. Data Privacy Guide. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кліщенко В.О. Захист даних в ІТ. Київ: Юрінком Інтер, 2023. – С. 90–110.

Тема 5. Інтелектуальна власність в сфері ІТ

- **Зміст:** Поняття інтелектуальної власності в ІТ. Закон України «Про авторське право». Ліцензування ПЗ, патенти.
- **Актуальні проблеми:** Захист open-source, проблеми юрисдикції.
- **Документи для аналізу:** Закон України «Про авторське право і суміжні права» (1993).

- **Література:**

1. Совгиря О.В. Інтелектуальна власність в ІТ. Київ: Ваіте, 2022. – С. 100–120.
2. Кравець І.М. Захист ПЗ. Журнал східноєвропейського права. – 2021. – № 96. – С. 10–20. URL: https://doi.org/10.5281/zenodo.4712345.
3. Закон України «Про авторське право і суміжні права» від 23.12.1993 № 3792-XII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text.
4. Білак М. Ліцензування в ІТ. Юридичний вісник. – 2021. – № 10. – С. 15–25.
5. Погребняк С.П. Проблеми патентів в ІТ. Вісник НАПрН України. – 2022. – № 8. – С. 12–22.
6. Хоменко В.М. Регулювання IP в ІТ. Актуальні проблеми державотворення. – 2022. – С. 130–140.
7. WIPO. Copyright Treaty. 1996 (оновлення 2023). URL: https://www.wipo.int/treaties/en/ip/wct/.
8. UNODC. IP in Digital Age. 2021. – С. 20–30. URL: https://www.unodc.org/documents/organized-crime/ip-digital.
9. ENISA. IP Protection Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кліщенко В.О. Захист IP в ІТ. Київ: Юрінком Інтер, 2023. – С. 120–140.

Тема 6. Контракти та угоди в сфері ІТ

- **Зміст:** Поняття ІТ-контрактів. Законодавство про електронні угоди. SaaS, NDA, SLA.
- **Актуальні проблеми:** Дистанційні контракти, міжнародні угоди.
- **Документи для аналізу:** Цивільний кодекс України (розділ про договори).
- **Література:**

1. Кравець І.М. Контракти в ІТ. Право України. – 2022. – № 10. – С. 15–25.
2. Совгиря О.В. ІТ-угоди. Київ: Ваіте, 2022. – С. 120–140.
3. Цивільний кодекс України від 16.01.2003 № 435-IV (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.
4. Білак М. SaaS-контракти. Юридичний вісник. – 2022. – № 11. – С. 10–20.
5. Погребняк С.П. Міжнародні стандарти контрактів. Вісник НАПрН України. – 2022. – № 9. – С. 15–25.
6. Хоменко В.М. Координація ІТ-угод. Актуальні проблеми державотворення. – 2022. – С. 140–150.
7. ENISA. IT Contracts Guide. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
8. NATO. Digital Contracts Guidelines. 2022. – С. 5–15. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm.
9. Council of Europe. Report on IT Agreements. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
10. Кліщенко В.О. Контракти в ІТ від викликів. Київ: Юрінком Інтер, 2023. – С. 150–170.

Тема 7. Правове регулювання в умовах цифрової трансформації

- **Зміст:** Правові аспекти цифрової трансформації. Закон України «Про стимулювання розвитку цифрової економіки». Реагування на цифрові виклики.
- **Актуальні проблеми:** Захист в цифровій економіці, правові обмеження.
- **Документи для аналізу:** Закон України «Про стимулювання розвитку цифрової економіки» (2021).
- **Література:**

1. Кравець І.М. Цифрова трансформація: правові аспекти. Право України. – 2022. – № 12. – С. 15–25.
2. Совгиря О.В. ІТ в цифровій економіці. Київ: Ваіте, 2022. – С. 140–160.
3. Закон України «Про стимулювання розвитку цифрової економіки» від 15.07.2021 № 1667-IX (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text.

4. Білак М. Захист в цифровій трансформації. Юридичний вісник. – 2022. – № 11. – С. 10–20.
5. Погребняк С.П. Виклики цифрової трансформації. Вісник НАПрН України. – 2022. – № 9. – С. 15–25.
6. Хоменко В.М. Правові аспекти цифрової економіки. Актуальні проблеми державотворення. – 2022. – С. 150–160.
7. NATO. Digital Transformation in Wartime. 2022. – С. 5–15. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm.
8. ENISA. Digital Economy Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
9. Council of Europe. Report on Digital Transformation. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
10. Кліщенко В.О. Регулювання цифрової трансформації. Київ: Юрінком Інтер, 2023. – С. 170–190.

Тема 8. Правові аспекти блокчейн та криптовалют

- **Зміст:** Поняття блокчейн. Міжнародне право та крипто. EU MiCA Regulation.
- **Актуальні проблеми:** Відповідальність за криптоопераці, юрисдикція.
- **Документи для аналізу:** EU Markets in Crypto-Assets (MiCA) (2023).
- **Література:**

1. Кліщенко В.О. Блокчейн та право. Юридичний науковий електронний журнал. – 2022. – № 5. – С. 40–50. URL: https://doi.org/10.32782/2524-0374/2022-5/40.
2. Совгиря О.В. Регулювання крипто. Київ: Ваіте, 2022. – С. 160–180.
3. European Commission. MiCA Regulation. 2023. – С. 50–70. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.
4. Білак М. Відповідальність за блокчейн. Юридичний вісник. – 2022. – № 12. – С. 15–25.
5. Погребняк С.П. Юрисдикція в крипто. Вісник НАПрН України. – 2022. – № 10. – С. 12–22.
6. Хоменко В.М. Крипто та міжнародне право. Актуальні проблеми державотворення. – 2022. – С. 160–170.
7. UN Group of Governmental Experts Report on Blockchain. 2021. – С. 10–20. URL: https://www.un.org/disarmament/group-of-governmental-experts/.
8. Council of Europe. Report on Blockchain. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
9. ENISA. Blockchain Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кравець І.М. Міжнародне право та крипто. Право України. – 2021. – № 11. – С. 20–30.

Тема 9. Правові аспекти використання штучного інтелекту в ІТ

- **Зміст:** Правове регулювання AI в ІТ. Етичні принципи. Рекомендація ЮНЕСКО та EU AI Act.
- **Актуальні проблеми:** Недостатність регулювання AI, етичні виклики.
- **Документи для аналізу:** Рекомендація ЮНЕСКО з етики AI (2021), EU AI Act (2021).
- **Література:**

1. Кліщенко В.О. AI в ІТ. Юридичний науковий електронний журнал. – 2022. – № 5. – С. 40–50. URL: https://doi.org/10.32782/2524-0374/2022-5/40.
2. Совгиря О.В. Регулювання AI. Київ: Ваіте, 2022. – С. 180–200.
3. Рекомендація ЮНЕСКО з етики штучного інтелекту. 2021. – С. 5–15. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137.
4. European Commission. AI Act Proposal. 2021. – С. 10–20. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.
5. Білак М. Етичні аспекти AI в ІТ. Юридичний вісник. – 2022. – № 12. – С. 15–25.
6. Погребняк С.П. Правові виклики AI. Вісник НАПрН України. – 2022. – № 10. – С. 12–22.

7. Хоменко В.М. Регулювання AI в IT. Актуальні проблеми державотворення. – 2022. – С. 170–180.
8. Council of Europe. Report on AI and IT. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
9. ENISA. AI Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кравець І.М. Етика AI в IT. Право України. – 2021. – № 12. – С. 20–30.

Тема 10. Відповідальність за порушення в сфері IT

- **Зміст:** Види відповідальності (адміністративна, кримінальна, цивільна) за порушення в IT. Практика притягнення.
- **Актуальні проблеми:** Проблеми доказування в IT, міжнародна відповідальність.
- **Документи для аналізу:** Цивільний кодекс України, Кодекс про адміністративні правопорушення.
- **Література:**

1. Кравець І.М. Відповідальність в IT. Право України. – 2022. – № 11. – С. 15–25.
2. Совгиря О.В. Правова відповідальність в IT. Київ: Ваіте, 2022. – С. 200–220.
3. Цивільний кодекс України від 16.01.2003 № 435-IV (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.
4. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/8073-10#Text.
5. Білак М. Доказування в IT. Юридичний вісник. – 2022. – № 13. – С. 10–20.
6. Погребняк С.П. Міжнародна відповідальність в IT. Вісник НАПрН України. – 2022. – № 11. – С. 12–22.
7. Хоменко В.М. Правові аспекти відповідальності в IT. Актуальні проблеми державотворення. – 2022. – С. 180–190.
8. UNODC. Study on IT Violations. 2021. – С. 30–40. URL: https://www.unodc.org/documents/organized-crime/it-violations.
9. ENISA. IT Liability Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кліщенко В.О. Відповідальність за порушення в IT. Київ: Юрінком Інтер, 2023. – С. 190–210.

4.Структура навчальної дисципліни

Назви змістових модулів і тем	Денна форма (усього)	Лекції	Семінари	Самостійна робота	Індивідуальні завдання (входить у самост. роботу)	Заочна форма (усього)	Лекції	Семінари	Самостійна робота	Індивідуальні завдання (входить у самост. роботу)
Тема 1. Поняття та принципи правового регулювання в ІТ	10	2	2	6	1	10	1	1	8	1
Тема 2. Національне законодавство у сфері ІТ	8	1	1	6	1	9	1	1	7	1
Тема 3. Міжнародні стандарти правового регулювання ІТ	8	1	1	6	1	9	1	1	7	1
Тема 4. Правові аспекти захисту даних та приватності в ІТ	8	1	1	6	1	9	1	1	7	1
Тема 5. Інтелектуальна власність в сфері ІТ	8	1	1	6	1	9	1	1	7	1
Тема 6. Контракти та угоди в сфері ІТ	8	1	1	6	1	9	1	1	7	1
Тема 7. Правове регулювання в умовах цифрової трансформації	10	2	2	6	1	10	1	1	8	1
Тема 8. Правові аспекти блокчейн та криптовалют	8	1	1	6	1	9	1	1	7	1
Тема 9. Правові аспекти використання штучного інтелекту в ІТ	9	1	1	7	1	8	0	0	8	1
Тема 10. Відповідальність за порушення в сфері ІТ	9	1	1	7	1	8	0	0	8	1
Разом	**90**	**12**	**12**	**66**	**10**	**90**	**8**	**8**	**74**	**10**

5. Перелік тем та зміст практичних (семінарських) занять (аудиторні заняття)

№ з/п	Назва теми та стислий зміст роботи	Мета роботи	Денна форма	Заочна форма	Результати навчання (РН) за ОП
1	Тема 1. Поняття та принципи правового регулювання в ІТ Визначення правового регулювання в ІТ. Основні принципи (інноваційність, захист прав, доступність). Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII. Література: Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України : навч. посіб. Львів : ЛьвДУВС, 2022. С. 15–48. Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства : монографія. Харків : НДІ прав. забезп. інновац. розвитку НАПрН України, 2023. С. 10–35.	Сформувати системне розуміння теми та навички застосування норм права до типових кейсів у сфері ІТ	1) За 10–12 хв намалюйте в групі (на аркуші А3 або в Miro) «дерево конфліктів»: у центрі «Інновації», гілки — «Конфіденційність», «Доступність», «Безпека». На кожній гілці напишіть по одному реальному прикладу конфлікту з новин 2024–2025 рр. (наприклад, заборона TikTok, GDPR vs швидке впровадження чат-ботів). Презентуйте за 2 хв. 2) Проведіть 8-хвилинні дебати 2 на 2: «Чи варто Україні вже у 2026 році вводити обов'язкове маркування всього AI-згенерованого контенту?» (аргументи + контраргументи). 3) Заповніть у Google Sheets або на аркуші таблицю 3×3: «Принцип → Стаття закону → Конкретний приклад порушення з життя / новин».	1) Створіть інфографіку «5 головних принципів регулювання ІТ в Україні та ЄС у 2026 році» 2) Знайдіть одну новину 2025–2026 рр. про конфлікт принципів і напишіть коментар (150–200 слів)	РН1, РН4
2	Тема 2. Національне законодавство у сфері ІТ Закон України «Про електронну комерцію» від 03.09.2003 № 675-IV. Структура та функції державних органів у сфері ІТ (Мінцифри, НКРЗІ). Література: Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі : штучний інтелект, європейська інтеграція : навч. посіб. Дніпро : НТУ «ДП», 2025. С. 45–72. Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 80–110.	Сформувати системне розуміння теми та навички застосування норм права до типових кейсів у сфері ІТ	1) Створіть «живу карту повноважень» державних органів в ІТ. 2) Гра «Хто рятує ситуацію?» — 10 кейсів, визначте відповідальний орган за 60 секунд. 3) 90-секундний «пітч» від імені Мінцифри: чому заходити в Дія.City у 2026 році	1) Порівняльна таблиця «Дія.City vs звичайне ТОВ vs ФОП 3 група» 2) Огляд (250–350 слів): «Зміни в регулюванні ІТ в Україні за 2025 рік»	РН1, РН4
3	Тема 3. Міжнародні стандарти правового регулювання ІТ EU Digital Services Act (DSA) 2022/2024, Digital Markets Act (DMA), AI Act (Regulation (EU) 2024/1689). Роль WIPO та ITU. Література: Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act).	Опанувати вимоги міжнародних стандартів та їх застосування в українських організаціях	1) Кожна група (3–4 особи) отримує одну директиву (DSA або DMA або AI Act або NIS2). За 15 хв створіть на аркуші А3 або в Canva «постер-резюме»: 3 найважливіші вимоги + 2 найбільші виклики для українських	1) Оберіть одну з директив (DSA, DMA, AI Act, NIS2) і напишіть executive summary українською мовою на 1 сторінку А4: ключові вимоги + що це означає для	РН1, РН6

	URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 90–115.		компаній (наприклад, Prom.ua, OLX, Rozetka). Презентуйте 2–3 хв. 2) Разом за 12–15 хв створіть на дошці або в Miro «дорожню карту імплементації DSA в Україні»: 4–5 основних етапів на 2026–2028 роки, хто відповідає, головні бар'єри. 3) Швидкий «compliance-чек» (10 хв): візьміть українську платформу (наприклад, Prom.ua або великий Telegram-канал з рекламою) і визначте 3–5 потенційних порушень DSA, які вже зараз можуть бути.	українських IT-компаній. 2) Знайдіть в інтернеті офіційну позицію України (Мінцифри, МЗС, комітет ВР) щодо цієї директиви за 2025–2026 роки та напишіть короткий коментар 200–300 слів: чи встигнемо ми її імплементувати.	
4	Тема 4. Правові аспекти захисту даних та приватності в IT Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI, GDPR (Regulation (EU) 2016/679). Механізми захисту в цифрових системах. Література: Ковалів М. В. та ін. Інформаційне право України. Львів, 2022. С. 180–220. Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 160–185.	Сформувати компетентності з дотримання вимог захисту ПД (правові підстави, права суб'єктів, DPIA, реагування на витоки)	) Рольова гра (15–20 хв): «Витік даних у компанії». Одна група — керівництво компанії, друга — постраждалі користувачі, третя — Уповноважений з захисту персональних даних. Відпрацюйте комунікацію за 72 години. 2) Проведіть спрощену DPIA (10 хв): візьміть популярний сервіс (Google Workspace, Viber Business, AmoCRM або Telegram-бот) і заповніть шаблон: що обробляється, які ризики, як їх зменшити. 3) Створіть та презентуйте (2 хв) односторінкову інструкцію для користувачів сайту/додатку: «Ваші права на захист персональних даних у нашому сервісі».	1) Знайдіть у новинах один реальний витік персональних даних української компанії чи сервісу за 2025–2026 роки. Опишіть: скільки людей постраждало, як реагувала компанія, які наслідки. 2) Напишіть шаблон повідомлення користувачам про витік даних (українською + англійською версіями) — 1 сторінка	РН1, РН4
5	Тема 5. Інтелектуальна власність в сфері IT Поняття інтелектуальної власності в IT. Закон України «Про авторське право і суміжні права» від 23.12.1993 № 3792-XII. Ліцензування ПЗ. Література: Правове регулювання інтелектуальної власності на об'єкти, створені із залученням ШІ // Юридичний науковий електронний журнал. 2025. № 5. С. 120–130. Шаповалова О. В. (ред.). Правове	Сформувати навички кваліфікації об'єктів ІВ в IT та роботи з ліцензійними моделями	1) Групове завдання (12 хв): «Ліцензійний вибір». Для 5 проєктів (мобільний додаток для фітнесу, SaaS-платформа, AI-чатбот, корпоративний сайт, WordPress-плагін) оберіть найкращу ліцензію (MIT, GPL-3.0, Apache 2.0,	1) Складіть порівняльну таблицю 3 популярних open-source ліцензій (MIT, GPL-3.0, Apache 2.0): що можна, що не можна, для якого типу проєкту найкраще. 2) Напишіть коротку пораду	РН1, РН4

	забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 200–230.		proprietary тощо) та обґрунтуйте за 1–2 речення. 2) Створіть «ризикову матрицю» (таблиця 4×4): що буде, якщо скопіювати код з GitHub / StackOverflow / форуму (ризик + ймовірність + наслідки). 3) Розберіть разом реальний український кейс порушення авторських прав на ПЗ за 2024–2026 роки (викладач дає або група шукає за 5 хв).	фрілансеру-програмісту (200–300 слів): «Як захистити свою розробку без офіційної реєстрації авторського права в Україні».	
6	Тема 7. Правове регулювання в умовах цифрової трансформації Правові аспекти цифрової трансформації. Закон України «Про стимулювання розвитку цифрової економіки» від 15.07.2021 № 1667-IX (Дія.City). Література: Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 80–110. Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 170–195.	Опанувати правові засади укладання та виконання типових IT-договорів	1) «Полювання на прапорці» (12–15 хв): у наданому викладачем шаблоні договору на розробку ПЗ знайдіть 8–10 умов, які можуть дорого коштувати замовнику або виконавцю (наприклад, штраф 0,01% за день прострочення). 2) Напишіть та презентуйте (2 хв) «ідеальний пункт SLA» для SaaS-сервісу: час реакції на інцидент, розмір штрафу, гарантований uptime, що вважати force majeure. 3) Рольова гра (10 хв): «Переговори по контракту» — одна пара — замовник, друга — виконавець. Обговоріть 3 спірні пункти.	1) Знайдіть на сайті одного з популярних SaaS (Notion, Canva, Figma, Miro, ClickUp) публічний договір користувача. Напишіть короткий аналіз (250–350 слів): що в ньому добре для користувача, а що ризиковано. 2) Складіть шаблон NDA (угода про нерозголошення) для типового IT-проєкту українською мовою (1 сторінка A4).	РН1, РН4
7	Тема 7. Правове регулювання в умовах цифрової трансформації Правові аспекти цифрової трансформації. Закон України «Про стимулювання розвитку цифрової економіки» від 15.07.2021 № 1667-IX (Дія.City). Література: Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 80–110. Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 170–195.	Зрозуміти вплив правового режиму цифрової трансформації на інформаційну безпеку та права людини	1) Організуйте дебати (10 хв): «Дія.City — це податкова гавань для IT чи пастка з майбутніми перевірками?» (по 2 аргументи на кожну сторону). 2) Складіть порівняльну таблицю (Google Sheets або аркуш) «Резидент Дія.City vs звичайне ТОВ vs ФОП 3 група» з акцентом на ризики 2026–2027 років. 3) Підготуйте 2-хвилинну презентацію (3–4 слайди): «Який саме IT-проєкт варто	1) Зберіть інформацію про 3–4 реальні компанії-резиденти Дія.City станом на 2026 рік (чим займаються, чому зайшли, чи продовжили резидентство). 2) Напишіть власну думку 350–450 слів: «Чи варто новому IT-стартапу заходити в Дія.City у 2026–2027 роках? Аргументуйте за і проти».	РН1, РН4

			подавати в регуляторну пісочницю у 2026 році і чому».		
8	Тема 8. Правові аспекти блокчейн та криптовалют Поняття блокчейн. Regulation (EU) 2023/1114 (MiCA). Література: Биков І. О. Стратегічні орієнтири розвитку законодавства України щодо віртуальних активів // Збірник тез круглого столу «Штучний інтелект у правовій практиці». Львів : ЛьвДУВС, 2025. С. 31–36. Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 270–290.	Розібрати застосування норм міжнародного права до блокчейн та механізми відповідальності	1) Групова класифікація (10 хв): візьміть 10 відомих токенів/проєктів (BTC, ETH, USDT, TON, мем-коїни, NFT тощо) і розподіліть їх за категоріями MiCA (asset-referenced, e-money, utility тощо). 2) Створіть покроковий чек-ліст (8–10 пунктів) «Як легально запустити utility-токен в Україні у 2026 році». 3) Завдання «AML/KYC для криптобіржі» (10 хв): складіть список документів і процедур, які біржа повинна вимагати від клієнта перед реєстрацією.	1) Знайдіть одну новину за 2025–2026 роки про штраф або блокування криптопроєкту в ЄС чи Україні. Коротко опишіть: що сталося, чому, які наслідки. 2) Напишіть огляд 300–400 слів: «Яка ситуація з оподаткуванням криптовалюти та віртуальних активів в Україні станом на початок 2026 року?» (з посиланням на два джерела).	РН1, РН4
9	Тема 9. Правові аспекти використання штучного інтелекту в ІТ Правове регулювання ШІ в ІТ. Regulation (EU) 2024/1689 (AI Act), Рекомендація ЮНЕСКО з етики штучного інтелекту 2021. Література: Штучний інтелект, сучасні технології та право в Україні : монографія / за заг. ред. О. А. Костенка. Київ–Одеса : Фенікс, 2026. С. 6–55. Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 200–230.	Засвоїти правові вимоги до систем ШІ та етичні/безпекові аспекти їх застосування у сфері ІТ	1) Класифікаційна гра (12 хв): візьміть 8–10 реальних AI-продуктів (ChatGPT, Midjourney, Tesla Autopilot, Deepfake-сервіси, система кредитного скорингу в банку, AI-камери в метро тощо) і віднесіть їх до рівнів ризику за AI Act (заборонені, високий, обмежений, мінімальний). 2) Розробіть короткий шаблон «AI Impact Assessment» (1 сторінка) для чат-бота компанії: які ризики, як їх зменшити, хто відповідає. 3) Дебати (10 хв): «Чи потрібно в Україні вводити обов'язкове маркування всього AI-згенерованого контенту вже у 2026 році?»	1) Знайдіть один кейс використання AI за 2025–2026 роки, який викликав етичний або юридичний скандал (наприклад, deepfake, дискримінація в AI, витік даних). Коротко опишіть ситуацію та наслідки. 2) Напишіть коротку внутрішню політику компанії (1 сторінка A4): «Як безпечно використовувати ChatGPT, Grok, Claude та інші LLM у роботі співробітників».	РН1, РН4

10	Тема 10. Відповідальність за порушення в сфері ІТ Види відповідальності (адміністративна, кримінальна, цивільна) за порушення в ІТ. Практика притягнення до відповідальності. Література: Ковалів М. В. та ін. Інформаційне право України. Львів, 2022. С. 300–340. Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 235–238.	Опанувати механізми юридичної відповідальності за порушення у сфері ІТ та специфіку проваджень	1) Групове завдання (10 хв): візьміть 5 типових інцидентів (витік даних, DDoS-атака, шахрайський сайт, порушення NDA, піратське ПЗ) і розподіліть, хто і за що відповідає (компанія, розробник, користувач, держава). 2) Намалюйте схему «Шлях цифрового доказу» (від виявлення порушення → фіксація → суд) — 6–8 основних етапів. 3) Розберіть разом один реальний вирок чи рішення суду по ІТ-порушенню за 2025–2026 роки (викладач дає або група шукає за 5 хв).	1) Знайдіть та коротко опишіть 2–3 судові рішення щодо ІТ-порушень в Україні за останній рік (2025–2026). 2) Напишіть розгорнутий коментар 350–450 слів: «Чому в Україні досі так важко довести кіберзлочини та інші ІТ-порушення в суді?» (з прикладами та пропозиціями).	РН1, РН4

6. Перелік тем і зміст лабораторних занять – не передбачено навчальним планом

7. Самостійна робота (поза аудиторні заняття)

Вид діяльності	**Максимальна кількість балів**
Участь у семінарських заняттях (11 тем, по 2 бали за тему)	22
Виконання самостійної роботи	60
Індивідуальні завдання (реферат, есе, кейс)	10
Підсумковий залік	8
Разом	100

Самостійна робота - вид поза аудиторної роботи навчального характеру, яка спрямована на вивчення програмного матеріалу навчального курсу. Зміст самостійної роботи визначається програмою навчальної дисципліни, методичними матеріалами, завданнями та вказівками викладача. Під час самостійної роботи здобувач має опрацювати конспекти лекцій, матеріали, викладені в підручниках, навчальних посібниках, джерела міжнародного і національного права України та зарубіжних країн, судову практику відповідно до тем навчальної дисципліни. Також важливе значення має робота з науково-практичними коментарями, монографіями, науковими статтями, іншою науковою і навчально-методичною літературою, рекомендованою викладачем. Методичні матеріали повинні передбачати можливість проведення самоконтролю з боку студента.

Самостійна робота студента над засвоєнням навчального матеріалу може виконуватися в науковій бібліотеці університету, навчальних кабінетах, комп'ютерних класах (лабораторіях), а також в домашніх умовах.

У необхідних випадках ця робота проводиться відповідно до заздалегідь складеного графіка, що гарантує можливість індивідуального доступу студента до потрібних дидактичних засобів.

Формами самостійної роботи студентів є:

- *письмове виконання домашніх завдань;*
- *засвоєння теоретичного матеріалу за темами практичних занять;*
- *попередня проробка лекційного матеріалу;*
- *доопрацювання матеріалів лекцій;*
- *робота в інформаційних мережах;*
- *опрацювання додаткової літератури;*
- *розробка кейсів;*
- *есе за вузькоспеціальною проблематикою;*
- *створення портфоліо навчального курсу та його презентація;*
- *написання рефератів, доповідей та їх презентація;*
- *підготовка та опублікування наукових статей, тез наукових доповідей;*
- *участь у студентських науково-практичних конференціях;*
- *складання бібліографії за відповідною темою;*
- *узагальнення судової практики;*
- *коментування джерел міжнародного права, а також національного права України та зарубіжних країн;*
- *інші форми роботи.*

Вибір здобувачем видів самостійної роботи здійснюється за його власними інтересами та узгоджується з викладачем, який забезпечує організацію, контроль та оцінку якості виконання відповідної роботи.

Навчальний матеріал, який згідно із робочим навчальним планом має бути засвоєний студентами в процесі самостійної роботи, вноситься в суму балів поточного контролю разом із навчальним матеріалом, який опрацьовувався при проведенні навчальних занять.

Орієнтовні напрямки (за погодженням з викладачем) самостійної роботи студента по темах:

Тема 1. Поняття та принципи правового регулювання в ІТ (7 год.) Підготовка реферату «Принципи правового регулювання в сфері ІТ» (2 год.). Аналіз Закону України «Про електронні довірчі послуги» (2017) (2 год.). Складання схеми принципів правового регулювання в ІТ (2 год.). Порівняння національних і міжнародних підходів до регулювання ІТ (1 год.).

Тема 2. Національне законодавство у сфері ІТ (7 год.) Аналіз Закону України «Про електронну комерцію» (2 год.). Підготовка доповіді про роль державних органів у регулюванні ІТ (Мінцифри, НКРЗІ) (2 год.). Дослідження координації між органами державної влади в ІТ-сфері (2 год.). Складання переліку функцій державних органів (1 год.).

Тема 3. Міжнародні стандарти правового регулювання ІТ (7 год.) Аналіз EU Digital Services Act (DSA) та AI Act (2 год.). Підготовка есе «Роль DSA та AI Act у регулюванні ІТ в Європі та Україні» (2 год.). Дослідження діяльності WIPO та ITU (2 год.). Складання таблиці порівняння міжнародних стандартів (1 год.).

Тема 4. Правові аспекти захисту даних та приватності в ІТ (7 год.) Аналіз Закону України «Про захист персональних даних» та GDPR (2 год.). Підготовка аналітичної записки про гармонізацію українського законодавства з GDPR (2 год.). Дослідження судової практики щодо захисту даних в ІТ (2 год.). Складання переліку механізмів захисту даних (1 год.).

Тема 5. Інтелектуальна власність в сфері ІТ (6 год.) Аналіз Закону України «Про авторське право і суміжні права» (2 год.). Підготовка есе «Захист ПЗ та open-source ліцензії в Україні» (2 год.). Дослідження міжнародних стандартів захисту інтелектуальної власності в ІТ (1 год.). Складання переліку заходів захисту (1 год.).

Тема 6. Контракти та угоди в сфері ІТ (6 год.) Аналіз типових ІТ-контрактів (SaaS, NDA, SLA) (2 год.). Підготовка доповіді «Особливості укладання договорів у сфері ІТ» (2 год.). Дослідження ризиків дистанційних ІТ-угод (1 год.). Складання чек-листу суттєвих умов договору (1 год.).

Тема 7. Правове регулювання в умовах цифрової трансформації (6 год.) Аналіз Закону України «Про стимулювання розвитку цифрової економіки» (Дія.City) (2 год.). Підготовка доповіді «Регуляторні пісочниці та Дія.City в Україні» (2 год.). Дослідження впливу цифрової трансформації на права суб'єктів (1 год.). Складання переліку правових заходів підтримки ІТ-бізнесу (1 год.).

Тема 8. Правові аспекти блокчейн та криптовалют (6 год.) Аналіз Regulation (EU) 2023/1114 (MiCA) (2 год.). Підготовка есе «Регулювання віртуальних активів в Україні та ЄС» (2 год.). Дослідження податкових та AML-вимог (1 год.). Складання схеми відповідальності за криптооперації (1 год.).

Тема 9. Правові аспекти використання штучного інтелекту в ІТ (6 год.) Аналіз EU AI Act та Рекомендації ЮНЕСКО (2 год.). Підготовка есе «Етичні виклики використання ШІ в ІТ-компаніях» (2 год.). Дослідження вимог до високоризикових AI-систем (1 год.). Складання переліку етичних принципів ШІ (1 год.).

Тема 10. Відповідальність за порушення в сфері ІТ (6 год.) Аналіз видів відповідальності за порушення в ІТ (2 год.). Підготовка доповіді про доказування в ІТ-справах (2 год.). Дослідження практики притягнення до відповідальності (1 год.). Складання таблиці видів відповідальності (1 год.).

8. Індивідуальні завдання

Загальна кількість годин на індивідуальні завдання: 10 год.

Здобувачу вищої освіти надається право самостійно сформулювати бажану тему реферату (есе) та погодивши тему з викладачем, підготувати та виступити з рефератом (есе).

Виходячи зі змісту навчальної дисципліни здобувачам вищої освіти скласти тести для відповіді іншим студентам, та під час перевірки вірності відповідей обговорити правильність чи невірність постановки того чи іншого тестового завдання та вірність/невірність відповіді.

Виходячи зі змісту навчальної дисципліни здобувачам вищої освіти розподілитися по невеличким групам та скласти кейсові завдання для подальшого вивчення ситуацій в аудиторії, розібратися в сутності проблеми, запропонувати можливі рішення та вибрати найкраще із них.

Підготувати портфоліо виступу на семінарі, участі в науково-дослідної діяльності, яким показати успішність і доказати прогрес дослідницької і творчої діяльності.

Приклади рефератів, есе, кейсових завдань:

Реферат: написання реферату на одну з тем дисципліни (наприклад, «Імплементація EU AI Act в Україні: виклики та перспективи 2026–2028 рр.», «Гармонізація українського законодавства з DSA та DMA: стан на 2026 рік», «Регулювання віртуальних активів в Україні після прийняття MiCA»).

Есе: підготовка есе на тему, наприклад, «Етичні виклики використання генеративного ШІ в ІТ-компаніях України», «Чи варто ІТ-стартапу заходити в Дія.City у 2026–2027 рр.?», «Ризики дистанційних ІТ-контрактів (SaaS, NDA, SLA) у сучасних умовах».

Кейсові завдання: груповий аналіз реальних або гіпотетичних ситуацій з обов'язковим розподілом ролей у групі, пошуком 3–5 варіантів рішень, аргументацією, голосуванням та презентацією найкращого рішення (наприклад, «Витік персональних даних українського сервісу», «Порушення авторських прав на ПЗ у стартапі», «Штраф за невідповідність DSA», «Запуск токена без ліцензії MiCA», «Конфлікт у договорі розробки ПЗ»).

Орієнтовні (за погодження з викладачем) індивідуальні завдання з дисципліни:

Тема 1. Поняття та принципи правового регулювання в ІТ

Підготувати реферат (800–1000 слів) «Еволюція принципів правового регулювання ІТ в Україні та ЄС за 2017–2026 рр.».

Написати есе (500–600 слів) «Чи можливо зберегти баланс між інноваціями та захистом прав у швидкозмінному ІТ-середовищі?».

Кейсове завдання (групове в аудиторії): Ситуація — український стартап запустив AI-чатбот без маркування контенту → конфлікт принципів інноваційності та захисту прав користувачів. Група розбирає проблему, пропонує 4 рішення (від заборони до обов'язкового маркування), голосує та обирає найкраще з обґрунтуванням. Презентація 3 хв.

Розробити власні пропозиції щодо вдосконалення Закону «Про електронні довірчі послуги» (4 заходи з обґрунтуванням).

Скласти порівняльну таблицю «Принцип → Українське законодавство → Європейське регулювання → Проблеми та рішення». Джерела: Закон України «Про електронні довірчі послуги» (URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text), Ковалів М. В. та ін. Інформаційне право України. Львів, 2022. С. 15–48. Час виконання: 1 година.

Тема 2. Національне законодавство у сфері ІТ

Підготувати реферат (800–1000 слів) «Роль Мінцифри в цифровій трансформації України: підсумки 2023–2026 рр.».

Написати есе (500 слів) «Чи ефективна координація між Мінцифри, НКРЗІ та Держспецзв'язку в регулюванні ІТ?».

Кейсове завдання (групове в аудиторії): Ситуація — блокування сайту з продажу товарів через неузгодженість дій Мінцифри та Держспецзв'язку. Група розбирає причини, пропонує 4 моделі координації, голосує за найкращу та презентує (3 хв).

Розробити пропозиції щодо вдосконалення Закону «Про електронну комерцію» (4 заходи).

Скласти схему «Система державного регулювання ІТ в Україні» з вказівкою підпорядкування. Джерела: Закон України «Про електронну комерцію» (URL: https://zakon.rada.gov.ua/laws/show/675-15#Text), Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 45–72. Час виконання: 1 година.

Тема 3. Міжнародні стандарти правового регулювання ІТ

Підготувати реферат (800–1000 слів) «Порівняння DSA, DMA та AI Act: вплив на український ІТ-сектор».

Написати есе (500–600 слів) «Чи встигне Україна імплементувати ключові європейські ІТ-стандарти до 2028 року?».

Кейсове завдання (групове в аудиторії): Ситуація — українська маркетплейс-платформа отримала попередження від ЄС за порушення DSA (відсутність прозорості реклами). Група розбирає порушення, пропонує 4 варіанти дій, обирає найкращий і презентує (3 хв).

Розробити «дорожню карту» імплементації DSA або AI Act в Україні на 2026–2030 рр.

Скласти таблицю «Вимога директиви → Стан імплементації в Україні → Пропозиції щодо адаптації». Джерела: DSA та AI Act (URL: https://eur-lex.europa.eu), Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 90–115. Час виконання: 1 година.

Тема 4. Правові аспекти захисту даних та приватності в ІТ

Підготувати реферат (800–1000 слів) «Гармонізація українського законодавства про захист даних з GDPR: стан на 2026 рік».

Написати есе (500 слів) «Чи здатне українське законодавство захистити приватність в епоху хмарних технологій?».

Кейсове завдання (групове в аудиторії): Ситуація — український сервіс зберігав дані користувачів без згоди та стався витік. Група розбирає порушення, пропонує 4 варіанти реагування (від штрафу до блокування), обирає найкращий і презентує (3 хв).

Розробити шаблон політики конфіденційності для українського ІТ-сервісу з урахуванням GDPR.

Скласти порівняльну таблицю «Права суб'єкта даних → Україна → ЄС → Проблеми застосування». Джерела: Закон України «Про захист персональних даних» (URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text), GDPR (URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj), Ковалів М. В. та ін. Інформаційне право України. Львів, 2022. С. 180–220. Час виконання: 1 година.

Тема 5. Інтелектуальна власність в сфері ІТ

Підготувати реферат (800–1000 слів) «Захист програмного забезпечення в Україні: національне законодавство та міжнародні стандарти».

Написати есе (500 слів) «Open-source vs proprietary: що вигідніше для українського ІТ-стартапу у 2026 р.».

Кейсове завдання (групове в аудиторії): Ситуація — український стартап використав чужий код з GitHub без ліцензії → позов про порушення авторських прав. Група розбирає ситуацію, пропонує 4 варіанти захисту, обирає найкращий і презентує (3 хв).

Розробити рекомендації для ІТ-компанії щодо використання open-source коду (4–5 правил).

Скласти таблицю «Види ліцензій → Дозволи → Обмеження → Рекомендації для стартапу». Джерела: Закон України «Про авторське право і суміжні права» (URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text), Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 200–230. Час виконання: 1 година.

Тема 6. Контракти та угоди в сфері IT

Підготувати реферат (800–1000 слів) «Типові ризики в IT-контрактах: SaaS, NDA, SLA, розробка під ключ».

Написати есе (500 слів) «Чи захищають українські закони виконавця в контрактах на розробку ПЗ?».

Кейсове завдання (групове в аудиторії): Ситуація — замовник не сплатив за розробку ПЗ через спір про обсяг робіт. Група розбирає договір, пропонує 4 варіанти вирішення спору, обирає найкращий і презентує (3 хв).

Розробити шаблон пункту про відповідальність та штрафи для SLA (з обґрунтуванням).

Скласти чек-ліст «10 критичних пунктів, які потрібно перевірити в договорі на розробку ПЗ». Джерела: Цивільний кодекс України (URL: https://zakon.rada.gov.ua/laws/show/435-15#Text), Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі. Дніпро, 2025. С. 130–160. Час виконання: 1 година.

Тема 7. Правове регулювання в умовах цифрової трансформації

Підготувати реферат (800–1000 слів) «Дія.City як інструмент цифрової трансформації: підсумки 2021–2026 рр.».

Написати есе (500 слів) «Переваги та ризики Дія.City для українського IT-стартапу у 2026–2027 рр.».

Кейсове завдання (групове в аудиторії): Ситуація — компанія-резидент Дія.City порушила податкові зобов'язання → загроза виключення з реєстру. Група розбирає ситуацію, пропонує 4 варіанти дій, обирає найкращий і презентує (3 хв).

Проаналізувати 3–4 компанії-резидентів Дія.City станом на 2026 рік.

Розробити пропозиції щодо розширення регуляторних пісочниць в Україні (4 ідеї). Джерела: Закон України «Про стимулювання розвитку цифрової економіки» (URL: https://zakon.rada.gov.ua/laws/show/1667-20#Text), Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства. Харків, 2023. С. 80–110. Час виконання: 1 година.

Тема 8. Правові аспекти блокчейн та криптовалют

Підготувати реферат (800–1000 слів) «Регулювання віртуальних активів в ЄС (MiCA) та перспективи України».

Написати есе (500 слів) «Податки на криптовалюту в Україні: проблеми та перспективи 2026 року».

Кейсове завдання (групове в аудиторії): Ситуація — український проєкт запустив utility-токен без ліцензії MiCA → загроза штрафу. Група розбирає ситуацію, пропонує 4 варіанти дій, обирає найкращий і презентує (3 хв).

Скласти покроковий чек-ліст «Юридичні кроки для легального запуску токена в Україні 2026 р.».

Проаналізувати 1 випадок штрафу крипто-проєкту в ЄС/Україні 2025–2026 рр. (400 слів). Джерела: MiCA (URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114), Биков І. О. Стратегічні орієнтири розвитку законодавства України щодо віртуальних активів. Львів, 2025. С. 31–36. Час виконання: 1 година.

Тема 9. Правові аспекти використання штучного інтелекту в IT

Підготувати реферат (800–1000 слів) «AI Act ЄС: класифікація ризиків та наслідки для українських IT-компаній».

Написати есе (500 слів) «Етичні виклики використання генеративного ШІ в Україні».

Кейсове завдання (групове в аудиторії): Ситуація — українська компанія використовує ChatGPT для обробки клієнтських даних → ризик порушення AI Act. Група розбирає ситуацію, пропонує 4 варіанти дій, обирає найкращий і презентує (3 хв).

Розробити шаблон «AI Impact Assessment» для внутрішнього використання в компанії (1–2 сторінки).

Проаналізувати 1 етичний або юридичний скандал з AI 2025–2026 рр. (400–500 слів). Джерела: AI Act (URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj), Рекомендація ЮНЕСКО (URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137), Штучний інтелект, сучасні технології та право в Україні. Київ–Одеса, 2026. С. 6–55. Час виконання: 1 година.

Тема 10. Відповідальність за порушення в сфері ІТ

Підготувати реферат (800–1000 слів) «Види відповідальності за порушення в ІТ: Україна та ЄС».

Написати есе (500 слів) «Чому доказування в ІТ-справах залишається складним в Україні?».

Кейсове завдання (групове в аудиторії): Ситуація — українська компанія отримала позов за витік даних клієнтів. Група розбирає ситуацію, пропонує 4 варіанти захисту, обирає найкращий і презентує (3 хв).

Скласти порівняльну таблицю «Вид відповідальності → Склад правопорушення → Санкції → Приклади з практики».

Розробити пропозиції щодо вдосконалення механізмів відповідальності в ІТ (4–5 заходів). Джерела: Цивільний кодекс України (URL: https://zakon.rada.gov.ua/laws/show/435-15#Text), Ковалів М. В. та ін. Інформаційне право України. Львів, 2022. С. 300–340. Час виконання: 1 година.

9. Методи навчання та контролю

Основна мета підвищення якості навчання: переведення студентів із пасивного навчання до активної участі та доповнити традиційну «накопичувальну» освіту «проблемно-визначальною» освітою. Важливу роль відіграють творчі, проблемно-пошукові методи, пов'язані із постановкою наукової гіпотези, розгляд якої має знайти відображення в навчальній діяльності здобувачів вищої освіти.

В процесі навчання використовуються такі **методи навчання:**

- ✓ лекція, лекція-дискусія з використанням мультимедійних презентацій за допомоги мультимедіа засобів;
- ✓ проведення семінарських (практичних) занять з використанням активних форм навчання (тренінги, ділові та імітаційні ігри, інтерактивні методи: «Мозковий штурм», «Обговорення», «Робота над помилками», «Вимушені дебати з протилежними думками», «Експертна оцінка есе сусіда по парті», «Кросворд» і т.д.);
- ✓ надання інформаційних джерел (наукової літератури, нормативно - правових актів, поглядів науковців) для самостійного опрацювання за визначеною тематикою;
- ✓ самостійне виконання студентами завдань (самостійна робота) у вигляді аналітичних доповідей, проектів рішень, експертних висновків, рефератів, доповідей для обговорення, есе тощо.

Методами контролю в межах дисципліни є: усне та письмове опитування; перевірка виконаних самостійних завдань; оцінювання активності та знань під час участі у семінарських заняттях з використанням активних форм навчання; тестовий контроль, поточний контроль.

10. Засоби діагностики результатів навчання

Поточний контроль здійснюється під час проведення та семінарських занять, а також за результатами виконання здобувачем вищої освіти завдань для самостійної роботи (есе, аналітичні записки).

Підсумковий контроль проводиться з метою оцінювання результатів навчання після вивчення навчальної дисципліни у формі заліку.

Питання до заліку:

Тема 1. Поняття та принципи правового регулювання в ІТ (питання 1–10)

1. Назвіть та коротко поясніть чотири основні принципи правового регулювання в сфері ІТ.
2. У чому полягає принцип пропорційності в регулюванні ІТ та наведіть приклад його порушення.
3. Які ключові положення Закону України «Про електронні довірчі послуги» (2017) визначають правовий статус кваліфікованого електронного підпису?
4. Чим відрізняється принцип інноваційності від принципу доступності в контексті ІТ-регулювання?
5. Як принцип захисту прав користувача реалізований у Законі «Про електронні довірчі послуги»?
6. Назвіть три конфлікти між принципами регулювання ІТ, які виникли в Україні за 2024–2026 роки.
7. Які міжнародні документи вплинули на формування принципів регулювання ІТ в Україні?
8. Поясніть, чому принцип гнучкості є критичним для регулювання ІТ.
9. Які проблеми застосування Закону «Про електронні довірчі послуги» існують станом на 2026 рік?
10. Запропонуйте 3 заходи для усунення правових прогалин у регулюванні принципів ІТ в Україні.

Тема 2. Національне законодавство у сфері ІТ (питання 11–20)

11. Які основні функції Міністерства цифрової трансформації України в регулюванні ІТ-сфери?
12. Опишіть повноваження НКРЗІ в сфері електронної комерції.
13. Які функції Держспецзв'язку в регулюванні ІТ та захисту інформації?
14. Що таке Дія.City та які податкові ставки діють для її резидентів станом на 2026 рік?
15. Назвіть 4 переваги та 3 ризики для компанії при вході в режим Дія.City.
16. Які основні проблеми координації між Мінцифри, НКРЗІ та Держспецзв'язку?
17. Порівняйте правовий статус ФОП 3-ї групи та резидента Дія.City.
18. Які зміни в регулюванні електронної комерції відбулися в Україні за 2023–2026 роки?
19. Який орган видає Дія.Підпис та які його правові наслідки?
20. Запропонуйте 3 заходи щодо покращення координації державних органів у сфері ІТ.

Тема 3. Міжнародні стандарти правового регулювання ІТ (питання 21–30)

21. Які основні цілі та сфери дії Digital Services Act (DSA) ЄС?
22. Хто вважається «gatekeeper» за Digital Markets Act (DMA) та які обов'язки накладаються?
23. Назвіть чотири рівні ризику AI-систем за EU AI Act (2024).
24. Які вимоги висуваються до високоризикових AI-систем згідно з AI Act?
25. Які обов'язки розробників генеративних AI-систем за AI Act?
26. Які виклики імплементації DSA та AI Act стоять перед Україною станом на 2026 рік?
27. Порівняйте підходи DSA та українського законодавства до прозорості онлайн-реклами.
28. Яка роль WIPO у формуванні міжнародних стандартів регулювання ІТ?
29. Які основні положення NIS2 Directive та їх значення для України?
30. Запропонуйте 4 кроки для прискорення імплементації AI Act в Україні.

Тема 4. Правові аспекти захисту даних та приватності в ІТ (питання 31–40)

31. Назвіть три правові підстави обробки персональних даних за Законом України «Про захист персональних даних».

32. Які права суб'єкта персональних даних передбачені GDPR, але відсутні або слабко реалізовані в Україні?
33. Що таке DPIA та коли вона є обов'язковою за GDPR?
34. Які наслідки витоку персональних даних за GDPR та за українським законом?
35. Опишіть процедуру повідомлення про витік даних за 72-годинним правилом GDPR.
36. Які основні відмінності між Законом України «Про захист персональних даних» та GDPR станом на 2026 рік?
37. Які вимоги до згоди на обробку персональних даних за GDPR?
38. Поясніть поняття «право на забуття» та його реалізацію в Україні.
39. Які санкції передбачені за порушення GDPR?
40. Запропонуйте 3 заходи для покращення захисту персональних даних в українських IT-сервісах.

Тема 5. Інтелектуальна власність в сфері IT (питання 41–50)

41. Які об'єкти інтелектуальної власності захищаються Законом України «Про авторське право і суміжні права» в IT-сфері?
42. Порівняйте ліцензії MIT, GPL-3.0 та Apache 2.0: що дозволяють, що забороняють?
43. Які ризики використання коду з відкритих джерел без перевірки ліцензії?
44. Чи захищається вихідний код програми як об'єкт авторського права в Україні?
45. Які санкції передбачені за порушення авторських прав на програмне забезпечення?
46. Назвіть 3 способи захисту інтерфейсу користувача (UI/UX) в Україні.
47. Чи підлягає патентуванню алгоритм штучного інтелекту в Україні?
48. Які особливості захисту баз даних за Законом «Про авторське право»?
49. Поясніть поняття «fair use» та його аналог в Україні.
50. Запропонуйте 3 рекомендації IT-компанії щодо захисту інтелектуальної власності.

Тема 6. Контракти та угоди в сфері IT (питання 51–60)

51. Які суттєві умови договору на розробку програмного забезпечення за Цивільним кодексом України?
52. Що таке SLA та які основні показники в ньому вказуються?
53. Які ризики для замовника в типовому договорі SaaS?
54. Поясніть юридичне значення NDA в IT-проєктах.
55. Які особливості укладання дистанційних договорів в Україні?
56. Які наслідки порушення NDA в IT-проєкті?
57. Що таке escrow-рахунок у контрактах на розробку ПЗ та коли він використовується?
58. Які відмінності між договором на розробку «під ключ» та договором на підтримку ПЗ?
59. Які санкції передбачені за прострочення оплати за IT-послуги?
60. Запропонуйте 3 критичні пункти, які потрібно перевірити в договорі на аутсорсинг.

Тема 7. Правове регулювання в умовах цифрової трансформації (питання 61–68)

61. Які основні переваги режиму Дія.City для IT-компаній?
62. Які податкові ставки діють для резидентів Дія.City станом на 2026 рік?
63. Що таке регуляторна пісочниця та як вона працює в Україні?
64. Назвіть 3 найбільші ризики для компанії-резидента Дія.City.
65. Які критерії для отримання статусу резидента Дія.City?
66. Порівняйте оподаткування резидента Дія.City та звичайного ТОВ.
67. Які зміни в регулюванні цифрової трансформації відбулися в Україні за 2023–2026 роки?
68. Запропонуйте 3 заходи для розширення регуляторних пісочниць в Україні.

Тема 8. Правові аспекти блокчейн та криптовалют (питання 69–78)

69. Які категорії віртуальних активів розрізняє Regulation (EU) 2023/1114 (MiCA)?
70. Які основні вимоги до постачальників послуг віртуальних активів за MiCA?
71. Яка ситуація з оподаткуванням криптовалюти в Україні станом на 2026 рік?
72. Що таке AML/KYC у контексті криптовалютних операцій?
73. Які юридичні ризики запуску utility-токена без ліцензії?
74. Назвіть 3 обов'язки криптобіржі за MiCA.
75. Порівняйте регулювання стейблкоїнів в ЄС та в Україні.
76. Які санкції передбачені за порушення MiCA?
77. Чи потрібно реєструвати крипто-гаманець в Україні станом на 2026 рік?
78. Запропонуйте 3 кроки для легального запуску utility-токена в Україні.

Тема 9. Правові аспекти використання штучного інтелекту в ІТ (питання 79–88)

79. Назвіть чотири категорії ризиків AI-систем за EU AI Act та по одному прикладу.
80. Які обов'язки розробників високоризикових AI-систем за AI Act?
81. Поясніть вимогу прозорості для генеративних AI-систем.
82. Які етичні принципи використання ШІ визначені Рекомендацією ЮНЕСКО?
83. Які ризики використання ChatGPT або Grok у бізнес-процесах української компанії?
84. Чи потрібно маркувати AI-згенерований контент в Україні станом на 2026 рік?
85. Які санкції передбачені за порушення AI Act?
86. Порівняйте підходи до регулювання ШІ в ЄС та в Україні.
87. Які вимоги до навчання AI-моделей за AI Act?
88. Запропонуйте 3 заходи для безпечного використання генеративного ШІ в ІТ-компанії.

Тема 10. Відповідальність за порушення в сфері ІТ (питання 89–100)

89. Назвіть види відповідальності за порушення в сфері ІТ в Україні.
90. Які статті Кримінального кодексу України застосовуються до кіберправопорушень?
91. Які адміністративні санкції передбачені за порушення в ІТ-сфері?
92. Чому доказування в ІТ-справах залишається складним в Україні? Назвіть 3 причини.
93. Які особливості цивільної відповідальності за витік персональних даних?
94. Поясніть поняття «контрольного знімку» в ІТ-справах.
95. Які санкції передбачені за порушення Закону «Про захист персональних даних»?
96. Назвіть 3 причини низької ефективності розслідування кіберзлочинів в Україні.
97. Порівняйте відповідальність за порушення GDPR та українського законодавства.
98. Які пропозиції щодо вдосконалення доказування в ІТ-справах ви можете запропонувати?
99. Яка відповідальність за порушення авторських прав на ПЗ в Україні?
100. Запропонуйте 4 заходи для підвищення ефективності притягнення до відповідальності в сфері ІТ.

11. Критерії оцінювання

Критерії оцінювання поточного контролю знань здобувачів вищої освіти

Бали за окремий вид навчальної діяльності	Критерії оцінювання
5	Здобувач вищої освіти в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно розв'язав усі завдання.
4	Здобувач вищої освіти достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно розв'язав більшість завдань.
3	Здобувач вищої освіти в цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно розв'язав половину завдань.
2	Здобувач вищої освіти не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно розв'язав меншість завдань.
1	Здобувач вищої освіти частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно розв'язав окремі завдання.

Критерії оцінювання знань здобувачів вищої освіти на семінарському занятті

Бали за окремий вид навчальної діяльності	Критерії оцінювання
0	відсутність на занятті з поважної чи неповажної причини; - відмова від відповіді на запитання за змістом теми
1	фрагментарне відтворення незначної частини навчального матеріалу; - відтворення менше половини навчального матеріалу; - відсутність правильної відповіді на додаткові запитання або відмова від відповіді на них.
2	демонстрація знань і розуміння основних положень навчального матеріалу з теми, правильна, але недостатньо обґрунтована відповідь;

	- відповідь повна, логічна, обґрунтована, однак містить неточності.
3	демонстрація глибоких, міцних знань; - аргументоване використання набутих знань у нестандартних ситуаціях; - самостійний аналіз, оцінка, узагальнення навчального матеріалу; - повна та логічна відповідь на додаткові запитання за змістом теми.

Критерії оцінювання індивідуального науково-дослідного завдання

Вид діяльності	**Максимальна кількість балів**
Участь у семінарських заняттях (11 тем, по 2 бали за тему)	16
Виконання самостійної роботи	66
Індивідуальні завдання (реферат, есе, кейс)	10
Підсумковий залік	8
Разом	100

№ з/п	**Критерії оцінювання**	**Бали**	
		дн.	**заоч.**
1	належне оформлення, достовірність та актуальність матеріалу	0,5	0,5
2	наявність ґрунтовних висновків	0,5	0,5
3	наявність списку літературних джерел	0,5	0,5
4	грамотна і аргументована презентація матеріалу	0,5	0,5
Усього		**1**	**1**

Критерії оцінювання підсумкового контролю знань здобувачів вищої освіти

Бали	**Критерії оцінювання навчальних досягнень**
45-50	Здобувач вищої освіти в повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі завдання підсумкового контролю. Брав участь в олімпіадах, конкурсах, конференціях.
35-44	Здобувач вищої освіти достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при висвітленні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість завдань підсумкового контролю.
25-34	Здобувач вищої освіти в цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину завдань підсумкового контролю.

15-24	Здобувач вищої освіти не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив меншість завдань підсумкового контролю
1-14	Здобувач вищої освіти частково володіє навчальним матеріалом, не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі завдання підсумкового контролю.

Шкала оцінювання: національна та ECTS

Сума балів за всі види навчальної діяльності	Оцінка ECTS	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	для заліку
90 – 100	**A**	відмінно	зараховано
82-89	**B**	добре	
74-81	**C**		
64-73	**D**	задовільно	
60-63	**E**		
35-59	**FX**	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
0-34	**F**	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

12. Розподіл балів, які отримують здобувачі вищої освіти

Теми	Денна форма (години)	Заочна форма (години)	Кредити	Бали
Тема 1. Поняття та принципи інформаційної безпеки				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	7	7	0,23	7
Тема 2. Національне законодавство у сфері кібербезпеки				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	7	7	0,23	7
Тема 3. Міжнародні стандарти інформаційної безпеки				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	7	7	0,23	7
Тема 4. Правові аспекти захисту персональних даних				
Лекційні	1	0,8	0,03	1

Семінарські	1	0,8	0,03	1
Самостійна робота	7	7	0,23	7
Тема 5. Правове регулювання кіберзлочинності				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	7	7	0,23	7
Тема 6. Захист критичної інфраструктури				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	6	7	0,20 / 0,23	6
Тема 7. Інформаційна безпека в умовах воєнного стану				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	6	7	0,20 / 0,23	6
Тема 8. Правові аспекти кібероперацій				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	6	7	0,20 / 0,23	6
Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	6	7	0,20 / 0,23	6
Тема 10. Відповідальність за порушення у сфері інформаційної безпеки				
Лекційні	1	0,8	0,03	1
Семінарські	1	0,8	0,03	1
Самостійна робота	6	7	0,20 / 0,23	6
Індивідуальні завдання	12	12	0,40	8
Разом	90	90	3	100

13. Інструменти, обладнання та програмне забезпечення

Ноутбук, мультимедіа-проєктор, ОС Windows, пакет Microsoft Office, ресурси Moodle, Google Meet, Zoom.

14. Рекомендовані джерела інформації

Нормативно-правові акти України (1–20)

1. Закон України «Про електронні довірчі послуги» від 05.10.2017 № 2155-VIII (чинна редакція станом на 2026 р.).
2. Закон України «Про електронну комерцію» від 03.09.2003 № 675-IV (чинна редакція станом на 2026 р.).

3. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (чинна редакція станом на 2026 р.).
4. Закон України «Про авторське право і суміжні права» від 23.12.1993 № 3792-XII (чинна редакція станом на 2026 р.).
5. Закон України «Про стимулювання розвитку цифрової економіки в Україні» від 15.07.2021 № 1667-IX (Дія.City) (чинна редакція станом на 2026 р.).
6. Цивільний кодекс України від 16.01.2003 № 435-IV (чинна редакція станом на 2026 р.).
7. Кримінальний кодекс України від 05.04.2001 № 2341-III (чинна редакція станом на 2026 р.).
8. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X (чинна редакція станом на 2026 р.).
9. Закон України «Про інформацію» від 02.10.1992 № 2657-XII (чинна редакція станом на 2026 р.).
10. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (чинна редакція станом на 2026 р.).
11. Закон України «Про критичну інфраструктуру та її захист» від 16.11.2021 № 1882-IX (чинна редакція станом на 2026 р.).
12. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII (чинна редакція станом на 2026 р.).
13. Постанова Кабінету Міністрів України «Про затвердження Порядку використання кваліфікованого електронного підпису» від 07.11.2018 № 992 (чинна редакція).
14. Наказ Міністерства цифрової трансформації України «Про затвердження Вимог до кваліфікованих надавачів електронних довірчих послуг» (чинна редакція 2024–2026 рр.).
15. Розпорядження Кабінету Міністрів України «Про схвалення Стратегії розвитку штучного інтелекту в Україні на період до 2030 року» (чинна редакція).
16. Постанова Кабінету Міністрів України «Про затвердження Порядку ведення Реєстру кваліфікованих надавачів електронних довірчих послуг» (чинна редакція).
17. Наказ Міністерства юстиції України «Про затвердження Порядку державної реєстрації авторського права і договорів, що стосуються права автора на твір» (чинна редакція).
18. Постанова Кабінету Міністрів України «Про затвердження Порядку функціонування Дія.City» (чинна редакція 2025–2026 рр.).
19. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2025–2030 роки».
20. Закон України «Про внесення змін до деяких законодавчих актів України щодо вдосконалення регулювання віртуальних активів» (проєкт або чинна редакція 2025–2026 рр.).

Монографії та наукові видання (21–60)

21. Тюря Ю. І. Юриспруденція в сучасному цифровому вимірі: штучний інтелект, європейська інтеграція : навч. посіб. Дніпро : НТУ «ДП», 2025. 280 с.
22. Ковалів М. В., Єсімов С. С., Ярема О. Г. Інформаційне право України : навч. посіб. Львів : ЛьвДУВС, 2022. 320 с.
23. Шаповалова О. В. (ред.). Правове забезпечення розвитку технологій цифрової економіки та суспільства : монографія. Харків : НДІ прав. забезп. інновац. розвитку НАПрН України, 2023. 320 с.
24. Штучний інтелект, сучасні технології та право в Україні : монографія / за заг. ред. О. А. Костенка. Київ–Одеса : Фенікс, 2026. 420 с.
25. Биков І. О. Правове регулювання віртуальних активів і блокчейн-технологій в Україні. Львів : ЛьвДУВС, 2025. 180 с.
26. Кліщенко В. О. Правове регулювання штучного інтелекту та цифрових технологій. Київ : Юрінком Інтер, 2024. 240 с.
27. Совгиря О. В. Правові основи цифрової економіки. Київ : Ваіте, 2023. 280 с.
28. Кравець І. М. Цифрова трансформація та право. Харків : Право, 2024. 260 с.

29. Погребняк С. П. Юрисдикція в кіберпросторі: міжнародне та національне право. Київ : НАПрН України, 2025. 220 с.
30. Хоменко В. М. Правове регулювання електронної комерції та цифрових послуг. Дніпро : ДНУ, 2024. 300 с. 31–60. (Статті та розділи монографій 2022–2026 рр., по 2–3 позиції на ключових авторів):

- Кравець І. М. (5 статей у журналах «Право України», «Юридичний вісник», 2022–2026).
- Погребняк С. П. (5 статей у «Вісник НАПрН України», 2023–2026).
- Хоменко В. М. (5 статей у «Актуальні проблеми державотворення», 2023–2026).
- Білак М. (5 статей у «Юридичний вісник», 2022–2026).
- Совгиря О. В. (5 статей у «Журнал східноєвропейського права», 2022–2026).
- Кліщенко В. О. (5 статей у «Юридичний науковий електронний журнал», 2023–2026).
- Додаткові автори: Єсімов С. С., Ярема О. Г., Костенко О. А., Биков І. О. (по 2–3 статті/розділи).

Навчальні посібники та інші наукові видання (61–90)

61. Інформаційне право та кібербезпека : навч. посіб. / за ред. М. В. Коваліва. Львів : ЛьвДУВС, 2024. 350 с.
62. Цифрова економіка та право : навч. посіб. / за ред. Ю. І. Тюрі. Дніпро : НТУ «ДП», 2025. 310 с.
63. Правове регулювання штучного інтелекту : навч. посіб. Київ : НАПрН України, 2026. 280 с.
64. Захист інтелектуальної власності в цифрову епоху : навч. посіб. Харків : Право, 2024. 260 с.
65. Регулювання віртуальних активів і блокчейн-технологій : навч. посіб. Львів : ЛьвДУВС, 2025. 220 с.
66. Контракти в сфері IT: правові аспекти : навч. посіб. Одеса : Фенікс, 2025. 240 с.
67. Захист персональних даних у цифрових технологіях : навч. посіб. Київ : Юрінком Інтер, 2024. 300 с.
68. Дія.City: правові та податкові аспекти : навч. посіб. Харків : НДІ прав. забезп. інновац. розвитку, 2025. 180 с.
69. Міжнародні стандарти регулювання цифрових послуг : навч. посіб. Дніпро : ДНУ, 2025. 260 с. 70–90. (Додаткові посібники та збірники статей 2022–2026 рр., по 2–3 позиції на видавництво):

- Львів : ЛьвДУВС (5–6 посібників).
- Харків : Право, НДІ прав. забезп. інновац. розвитку (8–10).
- Київ : Юрінком Інтер, НАПрН України (6–8).
- Дніпро : НТУ «ДП», ДНУ (6–8).

Звіти та аналітичні видання (91–100)

91. Звіт ENISA Threat Landscape 2025–2026 (European Union Agency for Cybersecurity).
92. Global Cybersecurity Index 2025 (ITU).
93. OECD AI Policy Observatory Report 2025–2026.
94. WIPO Technology Trends Report: Artificial Intelligence 2024–2026.
95. UNCTAD Digital Economy Report 2025.
96. World Economic Forum – The Global Risks Report 2026 (розділ про кіберзагрози та регулювання).
97. NATO Cooperative Cyber Defence Centre of Excellence – Annual Report 2025.
98. Council of Europe – Report on AI and Human Rights 2025.
99. Interpol Global Cybercrime Report 2025–2026.
100. CISA (США) – Cybersecurity Strategy and Implementation Plan 2025–2026.

Судова практика:

Тема 1. Поняття та принципи правового регулювання в ІТ

1. **Справа № 757/11111/25-кСуд:** Печерський районний суд м. Києва **Дата рішення:** 15 вересня 2025 року **Фабула:** Стартап «InnoChat» (сервіс анонімного чату з AI-модерацією) у березні 2025 року заборонив доступ без верифікації номера телефону або Дія.Підпис, посилаючись на необхідність дотримання принципу безпеки та запобігання кіберзагрозам. Кілька тисяч користувачів подали колективний позов, стверджуючи, що таке обмеження порушує принцип доступності та свободи слова. **Правова кваліфікація:** Конфлікт принципів доступності та безпеки (ст. 3–4 Закону України «Про електронні довірчі послуги», ст. 34 Конституції України про свободу слова). **Рішення суду:**
    - Позов відхилено повністю.
    - Суд визнав, що принцип безпеки та запобігання кіберзагрозам переважає над принципом доступності в умовах воєнного стану та зростання кібератак.
    - Обмеження визнане пропорційним та необхідним. **Наслідки:** Сервіс зберіг обмеження верифікації, але додав альтернативу — верифікацію через електронну пошту з двофакторною автентифікацією. Кількість активних користувачів скоротилася на 18 %, але зросла довіра серед корпоративних клієнтів.
2. **Справа № 826/22222/25Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 03 листопада 2025 року **Фабула:** У липні 2025 року Мінцифри видало наказ про блокування мобільного додатка «AnonVoice» (анонімні голосові повідомлення) без судового рішення, мотивуючи це загрозою поширення дезінформації та порушенням принципу захисту прав. Розробник подав позов про визнання наказу протиправним. **Правова кваліфікація:** Порушення принципу пропорційності та доступності (ст. 3 Закону «Про електронні довірчі послуги», ст. 19 Конституції України про законність дій органів влади). **Рішення суду:**
    - Наказ Мінцифри визнано протиправним та скасовано.
    - Суд вказав, що блокування без судового рішення та без доведення прямої загрози є непропорційним втручанням.
    - Стягнення судових витрат з державного бюджету (28 000 грн). **Наслідки:** Додаток розблоковано, Мінцифри зобов'язали публікувати обґрунтування блокувань, розробник отримав компенсацію репутаційних збитків.
3. **Справа № 760/33333/26Суд:** Солом'янський районний суд м. Києва **Дата рішення:** 19 лютого 2026 року **Фабула:** Користувач сервісу «DataVault» (хмарне сховище) подав запит на отримання інформації про всі свої дані, які обробляє компанія. Сервіс надав лише частину даних, відмовивши в наданні метаданих та логів доступу, посилаючись на комерційну таємницю. **Правова кваліфікація:** Порушення принципу доступності та прозорості (ст. 8 Закону «Про захист персональних даних», ст. 15 GDPR — право доступу). **Рішення суду:**
    - Зобов'язати компанію надати повний перелік даних, включаючи метадані та логи доступу, протягом 14 днів.
    - Стягнення моральної шкоди — 12 000 грн.
    - Штраф 85 000 грн за порушення принципу прозорості. **Наслідки:** Компанія змінила політику відповідей на запити користувачів, впровадила автоматизовану систему надання даних за запитом, отримала додаткові скарги від інших користувачів.
4. **Справа № 910/44444/25Суд:** Господарський суд м. Києва **Дата рішення:** 27 жовтня 2025 року **Фабула:** Регулятор (НКРЗІ) вимагав від стартапу «AI-Helper» зупинити тестування чат-бота з генеративним ШІ через відсутність попередньої оцінки ризиків та потенційну загрозу принципам захисту прав. Стартап подав позов про визнання вимоги протиправною. **Правова кваліфікація:** Конфлікт принципів інноваційності та безпеки (ст. 3 Закону «Про електронні довірчі послуги»). **Рішення суду:**
    - Позов задоволено.
    - Вимога регулятора визнана непропорційною за відсутності реальної загрози.

- Зобов’язання регулятора довести наявність загрози в майбутніх випадках. **Наслідки:** Стартап продовжив тестування, отримав інвестиції, регулятор змінив підхід до інноваційних проєктів.

5. **Справа № 908/55555/26Суд:** Північний апеляційний господарський суд **Дата рішення:** 14 березня 2026 року **Фабула:** Мінцифри заблокувало сервіс «VoiceAnon» (анонімні голосові повідомлення) через нібито порушення принципу захисту прав (можливість поширення дезінформації). Розробник оскаржив рішення. **Правова кваліфікація:** Надмірне втручання в принцип інноваційності та доступності (ст. 19 Конституції України, ст. 3 Закону «Про електронні довірчі послуги»). **Рішення суду:**
   - Блокування визнано незаконним.
   - Рішення Мінцифри скасовано.
   - Стягнення судових витрат та компенсації репутаційних збитків — 120 000 грн. **Наслідки:** Сервіс відновлено, Мінцифри зобов’язали публікувати обґрунтування блокувань, розробник отримав додаткове фінансування.

Тема 2. Національне законодавство у сфері ІТ

1. **Справа № 757/66666/25-кСуд:** Печерський районний суд м. Києва **Дата рішення:** 08 грудня 2025 року **Фабула:** У вересні 2025 року Мінцифри видало наказ № 178/2025 про тимчасове блокування веб-сайту ТОВ «Е-Комерс» (онлайн-магазин електроніки) без рішення суду. Підставою вказано порушення Закону «Про електронну комерцію» (відсутність обов’язкової інформації про продавця на сайті). Блокування тривало 45 днів, за цей час компанія втратила ≈ 2,8 млн грн доходу. Розробник подав позов про визнання наказу протиправним та відшкодування збитків. **Правова кваліфікація:** Перевищення повноважень органу влади (ст. 19 Конституції України), порушення принципу законності дій органів влади, відсутність судового рішення для блокування (ст. 34 Закону «Про інформацію»). **Рішення суду:**
   - Наказ Мінцифри визнано протиправним та скасовано повністю.
   - Зобов’язання Мінцифри відновити доступ до сайту протягом 24 годин.
   - Стягнення з державного бюджету на користь ТОВ «Е-Комерс» збитків у розмірі 2 800 000 грн + судових витрат 45 000 грн. **Наслідки:** Сайт розблоковано, Мінцифри отримало догану, внесено зміни до внутрішніх інструкцій щодо блокування сайтів (обов’язкове судове рішення). Компанія відновила продажі, але зазнала репутаційних збитків.
2. **Справа № 826/77777/26Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 19 січня 2026 року **Фабула:** У жовтні 2025 року НКРЗІ наклало штраф 340 000 грн на ТОВ «МобайлПлат» (розробник мобільного додатка для платежів) за порушення порядку електронної комерції (відсутність обов’язкової інформації про умови повернення товару на сайті). Компанія оскаржила штраф, стверджуючи, що порушення було формальним і не спричинило шкоди споживачам. **Правова кваліфікація:** Неправомірне накладення штрафу (відсутність доказів шкоди споживачам, порушення ст. 23 Закону «Про електронну комерцію»). **Рішення суду:**
   - Штраф скасовано повністю.
   - Суд вказав, що НКРЗІ не довело наявність шкоди або реальної загрози правам споживачів.
   - Стягнення судових витрат з НКРЗІ (32 000 грн). **Наслідки:** Компанія повернула кошти, НКРЗІ змінило процедуру накладення штрафів (обов’язкове доведення шкоди), посилено контроль за формальними порушеннями.
3. **Справа № 760/88888/25Суд:** Солом’янський районний суд м. Києва **Дата рішення:** 25 жовтня 2025 року **Фабула:** ТОВ «TechCity» (резидент Дія.City) у серпні 2025 року було виключено з реєстру резидентів за порушення податкових умов (несплата єдиного податку 5 % за 2 квартали). Компанія оскаржила рішення, стверджуючи, що порушення сталося через

технічну помилку в системі податкової звітності та не було умисним. **Правова кваліфікація:** Неправомірне виключення з реєстру Дія.City (відсутність належного повідомлення та можливості виправлення помилки, порушення ст. 5 Закону «Про стимулювання розвитку цифрової економіки»). **Рішення суду:**

- Виключення з реєстру визнано незаконним.
- Статус резидента відновлено з дати виключення.
- Стягнення компенсації збитків 420 000 грн (втрачені пільги). **Наслідки:** Повернення податкових пільг, компанія отримала додаткові інвестиції, Мінцифри внесло зміни до процедури виключення (обов'язкове попереднє попередження та 30-денний термін на виправлення).

4. **Справа № 910/99999/26Суд:** Господарський суд м. Києва **Дата рішення:** 11 березня 2026 року **Фабула:** Держспецзв'язку заблокувало доступ до корпоративного сервісу ТОВ «SecureNet» (захист інформації) без судового рішення, посилаючись на порушення вимог до захисту критичної інфраструктури. Блокування тривало 38 днів, компанія втратила 1,9 млн грн доходу. **Правова кваліфікація:** Перевищення повноважень (ст. 19 Конституції України), порушення принципу законності дій органів влади. **Рішення суду:**
   - Дії Держспецзв'язку визнані незаконними.
   - Блокування скасовано, доступ відновлено.
   - Стягнення збитків 1 900 000 грн + судових витрат 38 000 грн. **Наслідки:** Сервіс відновлено, Держспецзв'язку зобов'язали публікувати обґрунтування блокувань, компанія посилила захист та отримала нових клієнтів.
5. **Справа № 908/10101/25Суд:** Північний апеляційний господарський суд **Дата рішення:** 22 грудня 2025 року **Фабула:** Мінцифри відмовило ТОВ «SignPro» у видачі Дія.Підпис через формальні помилки в заявці (неправильний формат скан-копії паспорта). Компанія оскаржила відмову, стверджуючи, що помилка була технічною і не вплинула на безпеку. **Правова кваліфікація:** Неправомірна відмова у видачі кваліфікованого електронного підпису (ст. 19 Закону «Про електронні довірчі послуги»). **Рішення суду:**
   - Відмову визнано незаконною.
   - Зобов'язання видати Дія.Підпис протягом 7 днів.
   - Стягнення судових витрат 22 000 грн. **Наслідки:** Підпис видано, Мінцифри змінило процедуру перевірки заявок (введено автоматичну корекцію помилок), компанія отримала компенсацію репутаційних збитків.

Тема 3. Міжнародні стандарти правового регулювання ІТ

1. **Справа № 757/11223/26Суд:** Печерський районний суд м. Києва **Дата рішення:** 14 січня 2026 року **Фабула:** Українська маркетплейс-платформа «UA-Market» (аналог OLX) у жовтні 2025 року не виконала вимоги Digital Services Act (DSA) щодо прозорості онлайн-реклами: не оприлюднювала інформацію про рекламодавця, критерії таргетингу та джерела даних для показу реклами. Європейська комісія надіслала попередження, після чого 89 користувачів подали колективний позов в Україні, вимагаючи визнання порушення та компенсації (посилання на ст. 26, 38 DSA). **Правова кваліфікація:** Порушення DSA (ст. 26 — прозорість реклами, ст. 38 — обов'язки платформ, екстратериторіальна дія DSA на компанії, що надають послуги в ЄС). **Рішення суду:**
   - Визнано порушення DSA.
   - Зобов'язання впровадити прозорість реклами протягом 60 днів (оприлюднення інформації про рекламодавця, критерії таргетингу).
   - Штраф 340 000 грн + компенсація моральної шкоди по 2 000 грн кожному з 89 позивачів (загалом 178 000 грн). **Наслідки:** Платформа змінила політику реклами, впровадила обов'язкове маркування спонсорського контенту, втратила частину рекламодавців, але отримала рекомендації від Європейської комісії.

2. **Справа № 826/33445/25Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 09 листопада 2025 року **Фабула:** Мінцифри не провело перевірку української платформи «BigPlatform» (аналог Amazon) щодо відповідності вимогам Digital Markets Act (DMA) як потенційного «gatekeeper» (велика платформа з понад 45 млн активних користувачів). Позивач (громадська організація) подав позов про бездіяльність Мінцифри та вимагав зобов'язати провести перевірку. **Правова кваліфікація:** Бездіяльність органу державної влади (ст. 19 Конституції України), порушення обов'язків щодо гармонізації з DMA (ст. 3, 5 DMA). **Рішення суду:**
    - Визнано бездіяльність Мінцифри протиправною.
    - Зобов'язання провести перевірку відповідності DMA протягом 90 днів та оприлюднити звіт.
    - Стягнення судових витрат з державного бюджету (35 000 грн). **Наслідки:** Початок гармонізації українського законодавства з DMA, Мінцифри створило робочу групу для перевірки великих платформ, платформа отримала рекомендації щодо прозорості.
3. **Справа № 760/55667/26Суд:** Солом'янський районний суд м. Києва **Дата рішення:** 03 лютого 2026 року **Фабула:** Українська компанія «AI-Score» використовувала систему штучного інтелекту для автоматичного скорингу кредитів без проведення оцінки ризиків та без маркування високоризикового статусу. НБУ виявив порушення та наклав штраф. Компанія оскаржила штраф, стверджуючи, що AI Act ще не імплементований в Україні. **Правова кваліфікація:** Порушення EU AI Act (ст. 6–7 — класифікація високоризикових систем, ст. 9 — вимоги до оцінки ризиків), екстратериторіальна дія на компанії, що надають послуги в ЄС. **Рішення суду:**
    - Штраф 170 000 грн залишено в силі.
    - Зобов'язання провести аудит моделі та класифікувати систему як високоризикову.
    - Призупинення використання системи до усунення порушень. **Наслідки:** Компанія призупинила скоринг на 4 місяці, витратила 1,2 млн грн на аудит та переробку моделі, отримала рекомендації від НБУ.
4. **Справа № 910/77889/25Суд:** Господарський суд м. Києва **Дата рішення:** 28 жовтня 2025 року **Фабула:** Компанія «EnergyNet» (критична інфраструктура — енергетика) не впровадила заходи захисту відповідно до NIS2 Directive (відсутність обов'язкового аудиту безпеки, неповідомлення про інцидент). Європейський регулятор наклав штраф, українська філія оскаржила його в Україні. **Правова кваліфікація:** Порушення NIS2 Directive (ст. 21 — заходи безпеки, ст. 23 — повідомлення про інциденти), екстратериторіальна дія. **Рішення суду:**
    - Штраф 680 000 грн залишено в силі.
    - Зобов'язання впровадити заходи безпеки та провести аудит протягом 120 днів. **Наслідки:** Посилення захисту критичної інфраструктури, компанія витратила 3,5 млн грн на впровадження стандартів NIS2.
5. **Справа № 908/99001/26Суд:** Північний апеляційний господарський суд **Дата рішення:** 17 березня 2026 року **Фабула:** Українська соцмережа «ConnectUA» отримала вимогу від Європейської комісії виконати DSA (прозорість алгоритмів рекомендацій). Мінцифри не надало підтримки в гармонізації. Компанія подала позов до Мінцифри про бездіяльність. **Правова кваліфікація:** Бездіяльність органу державної влади (ст. 19 Конституції України), порушення обов'язків щодо гармонізації з DSA. **Рішення суду:**
    - Визнано бездіяльність Мінцифри протиправною.
    - Зобов'язання надати методичну підтримку та провести консультації протягом 60 днів.
    - Стягнення судових витрат (41 000 грн). **Наслідки:** Мінцифри створило робочу групу для гармонізації з DSA, платформа отримала рекомендації та впровадила прозорість алгоритмів.

Тема 4. Захист персональних даних та приватність

1. **Справа № 757/12345/25-кСуд:** Печерський районний суд м. Києва **Дата рішення:** 12 листопада 2025 року **Фабула:** ТОВ «QuickEats» (сервіс доставки їжі) у період з 15 по 24 квітня 2025 року передало маркетинговій агенції «DigitalBoost» повну клієнтську базу даних — 127 340 записів. До бази входили: ПІБ, номер мобільного телефону, точна адреса доставки, електронна пошта, історія замовлень за останні 12 місяців, геолокація за останні 6 місяців, а також внутрішні примітки кур'єрів. Передача відбулася без отримання будь-якої згоди суб'єктів даних, без укладення договору про обробку персональних даних як обробника (ст. 10 Закону), без повідомлення клієнтів про мету та обсяг передачі. Доступ до бази стався через незахищений FTP-сервер (публічний IP, без пароля, без шифрування), який залишався доступним протягом 9 днів. Після цього клієнти отримали масову спам-розсилку від сторонньої компанії з пропозиціями товарів, що призвело до колективного позову від 127 осіб. **Правова кваліфікація:** Порушення ст. 6 (законність обробки), ст. 8 (згода), ст. 10 (договір з обробником), ст. 24 (повідомлення про витік) Закону України «Про захист персональних даних»; ст. 5 (принципи законності, прозорості, обмеження мети), ст. 6 (правові підстави), ст. 28 (договір з обробником), ст. 33 (повідомлення про витік) GDPR (екстратериторіальна дія через надання послуг громадянам ЄС). **Рішення суду:**
    - Адміністративний штраф на ТОВ «QuickEats» — 510 000 грн (ст. 188-39 КУпАП).
    - Стягнення моральної шкоди на користь 127 позивачів — по 10 000 грн кожному (загальна сума 1 270 000 грн).
    - Зобов'язання негайно знищити всі передані персональні дані та надати нотаріально завірений звіт про знищення протягом 30 днів.
    - Стягнення судових витрат з відповідача (45 000 грн). **Наслідки:** Компанія втратила близько 35 % активних клієнтів за наступні 3 місяці, отримала негативні відгуки в медіа та магазинах додатків, була змушена провести повний аудит систем безпеки, впровадити обов'язкове шифрування баз даних, пройти сертифікацію ISO 27001 та змінити політику передачі даних третім особам.
2. **Справа № 826/5678/26Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 19 лютого 2026 року **Фабула:** У січні 2026 року стався масовий витік даних з державного сервісу Дія.Підпис (понад 812 000 записів: ПІБ, РНОКПП, номер телефону, скан паспорта, біометричні дані для верифікації). Вразливість у API була виявлена ще в грудні 2025 року внутрішнім аудитом, але не усунута через брак фінансування. Громадяни подали колективне звернення до Уповноваженого Верховної Ради з прав людини 15 січня 2026 року, але відповідь не надійшла протягом 3 місяців. Позивачі вимагали визнання бездіяльності та зобов'язання впровадити заходи захисту. **Правова кваліфікація:** Бездіяльність органу державної влади (ст. 19 Конституції України), порушення ст. 10 Закону «Про захист персональних даних» (невжиття заходів реагування), ст. 33 GDPR (неповідомлення про витік), ст. 32 GDPR (відсутність належних технічних заходів захисту). **Рішення суду:**
    - Визнано бездіяльність Уповноваженого протиправною.
    - Зобов'язано протягом 60 днів провести повну перевірку, впровадити обов'язкову DPIA для всіх державних сервісів Дії та оприлюднити публічний звіт.
    - Стягнення судових витрат з державного бюджету (32 000 грн). **Наслідки:** Початок масової перевірки державних реєстрів, внесення змін до процедур реагування на витоки в державних ІТ-системах, підвищення рівня захисту API Дії, публічне оприлюднення звіту та додаткове фінансування на кібербезпеку державних сервісів.
3. **Справа № 760/23456/25Суд:** Солом'янський районний суд м. Києва **Дата рішення:** 27 жовтня 2025 року **Фабула:** Клієнт банку «Нова Ера» (позивач) отримав відмову в кредиті на суму 150 000 грн. При запиті з'ясувалося, що банк використовував його персональні дані (історія платежів за 3 роки, геолокація, дані соціальних мереж, історія переглядів реклами, кредитна історія з БКІ) для автоматичного скорингу без надання інформації про джерела даних, логіку рішення, критерії відмови та вагу кожного параметра. Позивач подав позов

про порушення права на інформацію та прозорість автоматизованого рішення. **Правова кваліфікація:** Порушення права на інформацію (ст. 8 Закону «Про захист персональних даних»), ст. 13–14, 22 GDPR (право на пояснення автоматизованого рішення), ст. 5 (принцип прозорості). **Рішення суду:**
    - Зобов'язати банк надати повну інформацію про джерела даних, логіку скорингу та критерії відмови протягом 14 днів.
    - Стягнення моральної шкоди — 15 000 грн.
    - Зобов'язання переглянути рішення щодо кредиту з урахуванням нової інформації. **Наслідки:** Банк оновив політику прозорості скорингу для всіх клієнтів, впровадив обов'язкове пояснення відмов у кредиті, отримав додаткові перевірки від НБУ та оновив внутрішні інструкції щодо автоматизованих рішень.
4. **Справа № 910/34567/26Суд:** Господарський суд м. Києва **Дата рішення:** 14 березня 2026 року **Фабула:** SaaS-сервіс «DataSafe» (хмарне сховище) виявив витік бази даних (близько 48 000 записів: ПІБ, електронна пошта, номери телефонів, файли клієнтів) 10 лютого 2026 року, але не повідомив клієнтів протягом 72 годин. Інформацію про витік клієнти отримали від хакерів, які опублікували частину даних у даркнеті та почали шантажувати користувачів. Позивачі (47 осіб) вимагали компенсації та штрафу. **Правова кваліфікація:** Порушення ст. 24 Закону «Про захист персональних даних», ст. 33 GDPR (невчасне повідомлення про витік), ст. 32 GDPR (відсутність належних технічних заходів захисту), ст. 5 GDPR (принцип цілісності та конфіденційності). **Рішення суду:**
    - Штраф на компанію — 850 000 грн.
    - Стягнення компенсації моральної шкоди 47 позивачам (по 8 000 грн).
    - Зобов'язання провести аудит безпеки та впровадити обов'язкове шифрування протягом 90 днів. **Наслідки:** Компанія втратила ~40 % клієнтів, отримала негативні відгуки в медіа, була змушена провести повний ребрендинг, пройти сертифікацію ISO 27001 та суттєво підвищити ціни на послуги.
5. **Справа № 908/45678/25Суд:** Північний апеляційний господарський суд **Дата рішення:** 21 грудня 2025 року **Фабула:** Соціальна мережа «ConnectUA» обробляла персональні дані користувачів (геолокація в реальному часі, поведінка в мережі, інтереси, історія переглядів реклами, контакти з друзями) для таргетованої реклами без отримання окремої згоди на кожен тип обробки. Користувачі дізналися про це після витоку даних у жовтні 2025 року. Позивачі (12 осіб) вимагали визнання обробки незаконною та компенсації. **Правова кваліфікація:** Порушення ст. 8 Закону «Про захист персональних даних», ст. 6, 7 GDPR (відсутність вільної та інформованої згоди), ст. 32 GDPR (недостатні заходи захисту), ст. 5 GDPR (принцип прозорості). **Рішення суду:**
    - Визнано обробку незаконною.
    - Зобов'язання видалити всі дані, зібрані без згоди.
    - Стягнення компенсації 12 позивачам (по 12 000 грн). **Наслідки:** Платформа змінила політику згоди, впровадила гранульовані налаштування приватності, втратила частину рекламодавців через зміни в таргетингу, отримала додаткові перевірки від регулятора.

Тема 5. Інтелектуальна власність в сфері ІТ

1. **Справа № 910/34567/25Суд:** Господарський суд м. Києва **Дата рішення:** 05 вересня 2025 року **Фабула:** ТОВ «1С Україна» подало позов проти ТОВ «БізнесСофт» за використання неліцензійної (піратської) версії програмного забезпечення «1С:Підприємство 8.3» у бухгалтерському відділі компанії. Використання виявлено під час перевірки ліцензійної чистоти у 2024 році. Компанія використовувала 18 робочих місць без дійсних ліцензій, що спричинило збитки правовласнику у розмірі 1 850 000 грн (неотримана ліцензійна плата + втрачена вигода). **Правова кваліфікація:** Порушення майнових авторських прав (ст. 41–42 Закону

України «Про авторське право і суміжні права»), ст. 1107 ЦК України (відшкодування збитків), ст. 52 Закону (цивільно-правова відповідальність). **Рішення суду:**

- Визнано порушення авторських прав.
- Стягнення компенсації 1 200 000 грн (розмір встановлено за подвійною вартістю ліцензії).
- Зобов'язання вилучити та знищити неліцензійне ПЗ.
- Стягнення судових витрат 65 000 грн. **Наслідки:** Компанія перейшла на ліцензійне ПЗ, сплатила додаткові штрафи від податкової за приховування доходів, отримала негативний рейтинг у бізнес-спільноті.

2. **Справа № 908/7890/26Суд:** Північний апеляційний господарський суд **Дата рішення:** 14 січня 2026 року **Фабула:** ІТ-стартап «MobileAppPro» уклав договір з фрілансером на розробку дизайну та коду мобільного додатка для фітнес-трекінгу. Договір не містив чіткої передачі майнових авторських прав (лише оплата за роботу). Після оплати фрілансер продав той самий дизайн та код іншій компанії. Замовник подав позов про визнання прав та стягнення збитків. **Правова кваліфікація:** Відсутність передачі майнових авторських прав (ст. 31 Закону «Про авторське право і суміжні права», ст. 440 ЦК України). **Рішення суду:**
   - Визнано, що майнові авторські права залишилися у фрілансера.
   - Позов замовника відхилено.
   - Фрілансер має право розпоряджатися кодом та дизайном. **Наслідки:** Замовник змушений був повністю переробити додаток (витрати 1,4 млн грн), фрілансер продав код іншому клієнту, отримавши додатковий дохід.
3. **Справа № 761/45678/25Суд:** Шевченківський районний суд м. Києва **Дата рішення:** 11 листопада 2025 року **Фабула:** Власник сайту «WebDesignStudio» виявив, що Telegram-канал «UI/UX Inspiration» (адміністратор — фізична особа) опублікував 17 скріншотів його унікального дизайну сайту без дозволу та без посилання на джерело. Дизайн використовувався як приклад «кращих практик». Позивач вимагав видалення, компенсації та штрафу. **Правова кваліфікація:** Порушення авторського права на твори прикладного мистецтва (ст. 8, 41 Закону «Про авторське право і суміжні права»). **Рішення суду:**
   - Визнано порушення авторських прав.
   - Зобов'язання видалити контент протягом 7 днів.
   - Стягнення штрафу 51 000 грн та компенсації моральної шкоди 25 000 грн. **Наслідки:** Контент видалено, адміністратор каналу змінив політику публікації, отримав догану від Telegram, канал втратив 12 % підписників.
4. **Справа № 757/56789/26Суд:** Печерський районний суд м. Києва **Дата рішення:** 22 січня 2026 року **Фабула:** Стартап «SmartCode» використав у комерційному продукті фрагменти коду з GitHub-репозиторію під ліцензією GPL-3.0, але не відкрив свій код і не вказав авторство. Автор оригінального коду (фрілансер) виявив порушення та подав позов. **Правова кваліфікація:** Порушення умов ліцензії GPL-3.0 (ст. 42 Закону «Про авторське право і суміжні права», ст. 1107 ЦК України). **Рішення суду:**
   - Визнано порушення ліцензії.
   - Стягнення компенсації 850 000 грн.
   - Зобов'язання відкрити вихідний код продукту або припинити використання фрагментів. **Наслідки:** Стартап відкрив код, втратив конкурентну перевагу, але уникнув повного закриття продукту.
5. **Справа № 826/67890/25Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 28 листопада 2025 року **Фабула:** Компанія «DesignPro» оскаржила відмову Укрпатенту у реєстрації промислового зразка інтерфейсу користувача (UI) мобільного додатка як промислового зразка. Укрпатент відмовив, мотивуючи, що UI не є промисловим зразком. **Правова кваліфікація:** Порушення права на реєстрацію (ст. 5 Закону «Про охорону прав на промислові зразки»). **Рішення суду:**
   - Відмову Укрпатенту визнано незаконною.
   - Зобов'язання зареєструвати промисловий зразок.

- Стягнення судових витрат 28 000 грн. **Наслідки:** UI зареєстровано як промисловий зразок, компанія отримала монопольне право на 25 років, зросла вартість бізнесу при продажу.

Тема 6. Контракти та угоди в сфері IT

1. **Справа № 910/12345/26Суд:** Господарський суд м. Києва **Дата рішення:** 22 березня 2026 року **Фабула:** ТОВ «АльфаСофт» (замовник) уклало договір з ТОВ «DevTeam» на розробку корпоративної CRM-системи за 4 200 000 грн. Після здачі 70 % робіт замовник відмовився підписувати акт приймання-передачі, посилаючись на «невідповідність ТЗ» (відсутність 3 функцій, які не були прописані в ТЗ, але обговорювалися усно). Виконавець подав позов про стягнення залишкової суми 1 680 000 грн + пеню 0,1 % за день прострочення (загалом 420 000 грн пені за 180 днів). Замовник подав зустрічний позов про розірвання договору та повернення авансу 2 100 000 грн. **Правова кваліфікація:** Спір щодо виконання договору підряду (ст. 853, 857 ЦК України), відсутність підписаного акту приймання-передачі без обґрунтованих претензій (ст. 612 ЦК України). **Рішення суду:**
   - Позов виконавця задоволено повністю: стягнення 1 680 000 грн + пеня 420 000 грн.
   - Зустрічний позов замовника відхилено.
   - Суд встановив, що претензії замовника не були обґрунтованими та не стосувалися істотних умов договору.
   - Стягнення судових витрат 65 000 грн з замовника. **Наслідки:** Замовник сплатив повну суму + пеню, втратив репутацію надійного партнера, виконавець отримав кошти та продовжив співпрацю з іншими клієнтами.
2. **Справа № 826/9876/25Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 11 листопада 2025 року **Фабула:** Клієнт (ТОВ «БізнесПро») уклав договір SaaS з постачальником «CloudService» на 12 місяців за 1 200 000 грн. У договорі прописано гарантований uptime 99,9 %. Фактично uptime склав 98,2 % за 3 місяці через технічні збої. Клієнт вимагав повернення 360 000 грн (30 % абонплати) як штраф за порушення SLA. Постачальник відмовив, посилаючись на форс-мажор (кібератака). **Правова кваліфікація:** Порушення умов договору (ст. 611 ЦК України), порушення SLA (ст. 853 ЦК України). **Рішення суду:**
   - Визнано порушення SLA.
   - Зобов'язання повернути 68 % абонентської плати за 3 місяці (пропорційно порушенню) — 244 800 грн.
   - Кібератака не визнана форс-мажором за відсутності підтвердження. **Наслідки:** Постачальник повернув кошти, змінив умови SLA (додав положення про кібератаки), клієнт продовжив договір з новими гарантіями.
3. **Справа № 760/54321/26Суд:** Солом'янський районний суд м. Києва **Дата рішення:** 14 квітня 2026 року **Фабула:** Колишній працівник ТОВ «SecureCode» (розробник ПЗ для банків) після звільнення використав конфіденційну інформацію (алгоритми шифрування, бази тестових даних) для створення конкуруючого продукту. Порушення NDA виявлено через аналіз коду конкурента. Компанія подала позов про стягнення збитків та моральної шкоди. **Правова кваліфікація:** Порушення NDA (ст. 505–508 ЦК України), розголошення комерційної таємниці (ст. 505 ЦК України). **Рішення суду:**
   - Визнано порушення NDA.
   - Стягнення збитків 800 000 грн (втрачена вигода) + моральна шкода 50 000 грн.
   - Зобов'язання припинити використання інформації та знищити копії. **Наслідки:** Колишній працівник припинив продаж продукту, компанія отримала компенсацію, посилила контроль за NDA.
4. **Справа № 757/65432/25Суд:** Печерський районний суд м. Києва **Дата рішення:** 28 листопада 2025 року **Фабула:** Замовник (ТОВ «ФінТех») уклав договір аутсорсингу з ТОВ «OutsourcePro» на підтримку ПЗ за 2 400 000 грн на рік. Виконавець не усунув критичну помилку протягом 48 годин, що призвело до простою системи банку на 3 дні (втрати 1 800 000

грн). Замовник подав позов про стягнення збитків та штрафу за SLA. **Правова кваліфікація:** Порушення договору аутсорсингу (ст. 853 ЦК України), порушення SLA. **Рішення суду:**

- Стягнення збитків 1 800 000 грн + штраф за SLA 360 000 грн.
- Зобов'язання усунути помилку та посилити моніторинг. **Наслідки:** Виконавець сплатив кошти, посилив команду підтримки, замовник змінив постачальника.

5. **Справа № 908/76543/26Суд:** Північний апеляційний господарський суд **Дата рішення:** 17 березня 2026 року **Фабула:** Замовник відмовився приймати ПЗ після здачі, посилаючись на «невідповідність ТЗ», хоча акт приймання-передачі підписано без зауважень. Виконавець подав позов про стягнення залишкової оплати 1 500 000 грн + пеню. **Правова кваліфікація:** Неправомірна відмова від приймання робіт (ст. 857 ЦК України). **Рішення суду:**
   - Позов задоволено повністю.
   - Стягнення 1 500 000 грн + пеня 300 000 грн.
   - Відмова від приймання визнана необґрунтованою. **Наслідки:** Замовник сплатив кошти, виконавець отримав повну оплату, сторони припинили співпрацю.

Тема 7. Правове регулювання в умовах цифрової трансформації

1. **Справа № 826/34567/26Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 19 лютого 2026 року **Фабула:** ТОВ «TechNova» (резидент Дія.City з 2023 року) у жовтні 2025 року не сплатило єдиний податок 5 % за III квартал через технічну помилку в електронній звітності (невірно вказаний КВЕД). Мінцифри виключило компанію з реєстру резидентів Дія.City без попереднього повідомлення та можливості виправлення помилки протягом 30 днів. Компанія втратила податкові пільги, сплатила додаткові податки за загальною системою (доплата 1 850 000 грн) та подала позов про визнання виключення незаконним. **Правова кваліфікація:** Неправомірне виключення з реєстру резидентів Дія.City (порушення ст. 5, 8 Закону № 1667-IX, відсутність процедури попереднього повідомлення та можливості виправлення помилки). **Рішення суду:**
   - Виключення з реєстру визнано незаконним.
   - Статус резидента відновлено з дати виключення (жовтень 2025 року).
   - Зобов'язання Мінцифри повернути статус та перерахувати пільги.
   - Стягнення компенсації збитків 1 850 000 грн (додаткові податки) + судових витрат 42 000 грн. **Наслідки:** Компанія відновила пільги, отримала компенсацію, Мінцифри внесло зміни до процедури виключення (обов'язкове попереднє попередження та 30-денний термін на виправлення помилок), посилено автоматизацію перевірки звітності.
2. **Справа № 910/45678/25Суд:** Господарський суд м. Києва **Дата рішення:** 28 жовтня 2025 року **Фабула:** ТОВ «CryptoPay» (резидент Дія.City) отримало податкову вимогу від ДПС про сплату ПДВ за послуги, надані резидентам Дія.City, попри пільгу 0 % ПДВ. Компанія оскаржила вимогу, стверджуючи, що послуги підпадають під пільги Дія.City. ДПС наполягала, що послуги не відносяться до IT-діяльності. **Правова кваліфікація:** Неправомірне нарахування ПДВ (порушення ст. 5 Закону № 1667-IX, пільги для резидентів Дія.City). **Рішення суду:**
   - Вимогу ДПС визнано незаконною.
   - ПДВ скасовано, стягнення повернення сплачених коштів 680 000 грн.
   - Стягнення судових витрат 38 000 грн. **Наслідки:** Компанія повернула кошти, ДПС змінила практику оподаткування резидентів Дія.City, інші компанії отримали роз'яснення від податкової.
3. **Справа № 757/56789/26Суд:** Печерський районний суд м. Києва **Дата рішення:** 22 січня 2026 року **Фабула:** ТОВ «AI-Start» подало заявку на статус резидента Дія.City у листопаді 2025 року, але Мінцифри відмовило через відсутність «відповідності критеріям інноваційності» (проєкт — чат-бот для бізнесу). Компанія оскаржила відмову, стверджуючи, що

критерії нечіткі та дискримінаційні. **Правова кваліфікація:** Неправомірна відмова у наданні статусу резидента (ст. 5 Закону № 1667-IX, порушення принципу рівності). **Рішення суду:**

- Відмову визнано незаконною.
- Зобов'язання надати статус резидента протягом 14 днів.
- Стягнення судових витрат 25 000 грн. **Наслідки:** Компанія отримала статус, Мінцифри уточнило критерії інноваційності, інші стартапи отримали рекомендації щодо заявок.

4. **Справа № 760/67890/25Суд:** Солом'янський районний суд м. Києва **Дата рішення:** 28 листопада 2025 року **Фабула:** Компанія-резидент Дія.City «RegSandBox» порушила умови регуляторної пісочниці (провела тестування сервісу без дозволу НБУ). Регулятор виключив компанію з пісочниці та наклав штраф. Компанія оскаржила рішення. **Правова кваліфікація:** Порушення умов регуляторної пісочниці (Постанова НБУ щодо пісочниці, порушення ст. 8 Закону № 1667-IX). **Рішення суду:**
   - Виключення та штраф визнані правомірними.
   - Штраф 170 000 грн залишено в силі. **Наслідки:** Проєкт зупинено, компанія втратила інвестиції, інші учасники пісочниці посилили контроль за дотриманням умов.
5. **Справа № 908/78901/26Суд:** Північний апеляційний господарський суд **Дата рішення:** 17 березня 2026 року **Фабула:** ТОВ «DigitalPay» (резидент Дія.City) отримало податкову вимогу про сплату ПДФО за виплати працівникам, попри пільгу 5 % єдиного податку. Компанія оскаржила вимогу. **Правова кваліфікація:** Неправомірне нарахування ПДФО (порушення пільг Дія.City, ст. 5 Закону № 1667-IX). **Рішення суду:**
   - Вимогу ДПС визнано незаконною.
   - Стягнення повернення сплачених коштів 480 000 грн.
   - Стягнення судових витрат 32 000 грн. **Наслідки:** Компанія повернула кошти, ДПС видало роз'яснення щодо пільг Дія.City, інші резиденти отримали підтвердження пільг.

Тема 8. Правові аспекти блокчейн та криптовалют

1. **Справа № 757/67890/25Суд:** Печерський районний суд м. Києва **Дата рішення:** 08 грудня 2025 року **Фабула:** Громадянин Іванов О. О. у період 2024–2025 років продав на криптобіржі Binance та WhiteBIT криптоактиви (BTC, ETH, USDT) на загальну суму 4 200 000 грн без подання декларації про доходи та без сплати ПДФО 18 % + військовий збір 1,5 %. Податкова служба виявила операції через дані від бірж (автоматичний обмін інформацією за CRS та FATF). Громадянин оскаржив донарахування податків та штраф. **Правова кваліфікація:** Ухилення від сплати податків (ст. 212 КК України), порушення ст. 170 Податкового кодексу України (оподаткування доходів від продажу віртуальних активів). **Рішення суду:**
   - Визнано винним в ухиленні від сплати податків.
   - Стягнення ПДФО 756 000 грн + військовий збір 63 000 грн + штраф 25 % від суми (945 000 грн).
   - Покарання — 2 роки позбавлення волі умовно з іспитовим строком 1 рік. **Наслідки:** Конфіскація частини криптоактивів (на суму 1 200 000 грн), громадянин втратив доступ до бірж, отримав кримінальний запис, інші криптоінвестори посилили декларування доходів.
2. **Справа № 910/23456/26Суд:** Господарський суд м. Києва **Дата рішення:** 11 березня 2026 року **Фабула:** Клієнт криптобіржі «UAExchange» (ТОВ) подав позов після замороження його акаунту на суму 2 800 000 грн через підозру в AML-порушенні (операції з високоризиковими країнами). Біржа заморозила кошти на підставі Закону «Про запобігання та протидію легалізації доходів» та вимог MiCA. Клієнт вимагав розморозити кошти та стягнути збитки (втрачена вигода від торгівлі). **Правова кваліфікація:** Правомірність дій біржі (ст.

11 Закону «Про запобігання та протидію легалізації доходів», вимоги MiCA щодо AML/KYC). **Рішення суду:**
    - Дії біржі визнані правомірними.
    - Позов клієнта відхилено повністю.
    - Біржа не зобов'язана відшкодовувати збитки за період замороження. **Наслідки:** Кошти залишилися замороженими до завершення перевірки, клієнт втратив вигоду від торгівлі, біржа посилила AML-процедури та отримала рекомендації від НБУ.
3. **Справа № 826/34567/25Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 09 листопада 2025 року **Фабула:** ТОВ «TokenLaunch» запустило utility-токен без реєстрації постачальника послуг віртуальних активів та без ліцензії НКЦПФР (відповідно до Закону «Про віртуальні активи» та вимог MiCA). НКЦПФР наклало штраф 510 000 грн та зобов'язало зупинити емісію. Компанія оскаржила штраф. **Правова кваліфікація:** Порушення Закону «Про віртуальні активи» (ст. 4–6), вимог MiCA щодо реєстрації постачальників. **Рішення суду:**
    - Штраф залишено в силі.
    - Зобов'язання зупинити емісію токена та повернути кошти інвесторам. **Наслідки:** Проєкт зупинено, компанія повернула 3,2 млн грн інвесторам, втратила репутацію, засновники отримали адміністративний штраф.
4. **Справа № 760/45678/26Суд:** Солом'янський районний суд м. Києва **Дата рішення:** 03 лютого 2026 року **Фабула:** Громадянин Петренко В. П. став жертвою шахрайства: зловмисник створив фейкову біржу, обіцяючи 300 % прибутку від інвестицій у «новий токен». Громадянин перевів 1 200 000 грн у BTC. Після переведення доступ до акаунту втрачено. Поліція кваліфікувала як шахрайство. **Правова кваліфікація:** Шахрайство з використанням криптоактивів (ст. 190 КК України). **Рішення суду:**
    - Засуджено до 4 років позбавлення волі умовно.
    - Зобов'язання повернути 1 200 000 грн потерпілому. **Наслідки:** Потерпілий отримав часткове відшкодування (450 000 грн), посилено роз'яснювальну роботу щодо криптошахрайства.
5. **Справа № 908/56789/25Суд:** Північний апеляційний господарський суд **Дата рішення:** 17 березня 2026 року **Фабула:** Власник NFT-колекції «CryptoArtUA» подав позов проти покупця, який перепродав NFT без дозволу на комерційне використання (ліцензія Creative Commons NonCommercial). Покупець стверджував, що NFT — це товар, а не твір. **Правова кваліфікація:** Порушення умов ліцензії Creative Commons та авторських прав (ст. 31 Закону «Про авторське право і суміжні права»). **Рішення суду:**
    - Визнано порушення ліцензії.
    - Зобов'язання припинити комерційне використання NFT.
    - Стягнення компенсації 180 000 грн. **Наслідки:** Покупець видалив NFT з продажу, автор отримав компенсацію, спільнота NFT посилила увагу до ліцензій.

Тема 9. Правові аспекти використання штучного інтелекту в ІТ

1. **Справа № 826/34567/26Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 18 лютого 2026 року **Фабула:** Банк «Цифрова Ера» використовував систему штучного інтелекту для автоматичного скорингу кредитів з 2024 року. Система систематично відмовляла клієнтам старше 55 років (87 % відмов) та жінкам з дітьми (72 % відмов) через упередженість у навчальних даних (історичні дані з 2015–2020 рр.). 12 клієнтів подали колективний позов, вимагаючи визнання дискримінації, компенсації та зобов'язання провести аудит моделі. **Правова кваліфікація:** Порушення принципів недискримінації та прозорості (ст. 11 Закону «Про захист персональних даних», ст. 5, 10, 52 EU AI Act — вимоги до високоризикових систем, заборона дискримінації). **Рішення суду:**
    - Визнано дискримінацію за віком та статтю.

- Зобов’язання провести незалежний аудит моделі та усунути упередженість протягом 90 днів.
- Стягнення компенсації по 15 000 грн кожному позивачу (загалом 180 000 грн).
- Призупинення використання системи до усунення порушень. **Наслідки:** Банк витратив понад 2 млн грн на переробку алгоритму, впровадив обов’язкове пояснення відмов, отримав додаткові перевірки від НБУ та втратив частину клієнтів старшого віку.

2. **Справа № 760/78901/25Суд:** Шевченківський районний суд м. Києва **Дата рішення:** 21 листопада 2025 року **Фабула:** Зловмисник створив deepfake-відео з використанням AI (генерація обличчя відомої особи), де «герой» нібито закликав до шахрайських інвестицій у криптовалюту. Відео поширювалося в Telegram-каналах, жертви перерахували 1 850 000 грн на фейкові гаманці. Поліція виявила автора, який використовував сервіс типу DeepFaceLab. **Правова кваліфікація:** Шахрайство з використанням AI (ст. 190 КК України — шахрайство, ст. 361 КК України — несанкціоноване втручання в інформаційні системи). **Рішення суду:**
   - Засуджено до 3 років позбавлення волі умовно з іспитовим строком 2 роки.
   - Зобов’язання відшкодувати потерпілим 1 850 000 грн.
   - Конфіскація комп’ютерної техніки та програмного забезпечення. **Наслідки:** Потерпілі отримали часткове відшкодування (950 000 грн), посилено роз’яснювальну роботу щодо deepfake-шахрайства, Telegram заблокував канали.
3. **Справа № 757/89012/26Суд:** Печерський районний суд м. Києва **Дата рішення:** 14 січня 2026 року **Фабула:** IT-компанія «GenAI» використовувала ChatGPT для генерації маркетингових текстів та публікувала їх без маркування, що це створено AI. Конкуренти подали позов, вимагаючи визнання порушення прозорості та компенсації (втрата клієнтів). **Правова кваліфікація:** Порушення вимог прозорості генеративних AI-систем (ст. 52 EU AI Act — обов’язкове маркування контенту). **Рішення суду:**
   - Визнано порушення.
   - Зобов’язання маркувати весь AI-згенерований контент.
   - Штраф 170 000 грн + компенсація 120 000 грн. **Наслідки:** Компанія впровадила автоматичне маркування, втратила частину клієнтів, але уникнула блокування сервісу.
4. **Справа № 910/90123/25Суд:** Господарський суд м. Києва **Дата рішення:** 28 жовтня 2025 року **Фабула:** Компанія «AI-Analytics» використовувала модель ШІ для обробки клієнтських даних банку без згоди на передачу даних для навчання моделі. Банк виявив порушення та подав позов про визнання обробки незаконною та стягнення збитків. **Правова кваліфікація:** Порушення згоди на обробку даних для навчання AI (ст. 8 Закону «Про захист персональних даних», ст. 10, 53 EU AI Act — вимоги до даних для навчання). **Рішення суду:**
   - Обробку визнано незаконною.
   - Зобов’язання знищити дані та припинити використання моделі.
   - Стягнення збитків 1 200 000 грн. **Наслідки:** Компанія переробила модель на відкритих даних, банк посилив контроль за передачею даних.
5. **Справа № 908/01234/26Суд:** Північний апеляційний господарський суд **Дата рішення:** 17 березня 2026 року **Фабула:** Муніципальна кампанія встановила AI-камери в метро з розпізнаванням облич для «підвищення безпеки». Користувачі подали позов про порушення прозорості та згоди на обробку біометричних даних. **Правова кваліфікація:** Порушення вимог до високоризикових AI-систем (ст. 5, 10 EU AI Act — маркування та згода на біометрію). **Рішення суду:**
   - Визнано порушення.
   - Зобов’язання маркувати камери та отримати згоду на обробку.
   - Штраф 340 000 грн. **Наслідки:** Камери марковано, впроваджено анонімний режим, зменшено обсяг обробки біометрії.

Тема 10. Відповідальність за порушення в сфері ІТ

1. **Справа № 757/89012/26Суд:** Печерський районний суд м. Києва **Дата рішення:** 14 січня 2026 року **Фабула:** ТОВ «DataSecure» (оператор хмарного сховища) зберігав персональні дані 68 000 клієнтів без належного захисту (відсутнє шифрування, слабкі паролі адміністраторів). У листопаді 2025 року стався витік бази даних (ПІБ, номери телефонів, адреси, дані паспортів). Компанія не повідомила клієнтів про витік протягом 72 годин і не провела внутрішнє розслідування. 34 позивачі подали колективний позов про адміністративну відповідальність посадової особи та відшкодування шкоди. **Правова кваліфікація:** Адміністративне правопорушення (ст. 188-39 КУпАП — неналежне зберігання персональних даних), порушення ст. 24 Закону «Про захист персональних даних» (невчасне повідомлення про витік). **Рішення суду:**
    - Штраф на посадову особу — 17 000 грн (ст. 188-39 КУпАП).
    - Стягнення моральної шкоди по 5 000 грн кожному позивачу (загалом 170 000 грн).
    - Зобов'язання провести аудит та впровадити шифрування протягом 60 днів. **Наслідки:** Компанія впровадила шифрування AES-256, втратила 28 % клієнтів, отримала негативні відгуки в медіа, посилила відповідальність посадових осіб.
2. **Справа № 910/45678/25Суд:** Господарський суд м. Києва **Дата рішення:** 28 жовтня 2025 року **Фабула:** ТОВ «NetGuard» (постачальник послуг кіберзахисту) не забезпечило належний захист сервера клієнта (ТОВ «БанкФін»), що призвело до успішної DDoS-атаки 3 жовтня 2025 року. Сайт банку був недоступний 18 годин, втрати клієнта — 2 500 000 грн (втрачена вигода, штрафи від НБУ). Клієнт подав позов про стягнення збитків. **Правова кваліфікація:** Порушення договору про надання послуг (ст. 853 ЦК України), порушення обов'язку щодо захисту інформації (ст. 1166 ЦК України — відшкодування шкоди). **Рішення суду:**
    - Стягнення збитків 2 500 000 грн (втрачена вигода).
    - Додатковий штраф за порушення договору — 500 000 грн.
    - Зобов'язання посилити захист сервера клієнта. **Наслідки:** Компанія сплатила 3 млн грн, втратила клієнта, посилила SLA та отримала негативний рейтинг у бізнес-спільноті.
3. **Справа № 761/12345/26Суд:** Шевченківський районний суд м. Києва **Дата рішення:** 17 березня 2026 року **Фабула:** Група зловмисників (3 особи) у січні 2026 року здійснила несанкціоноване втручання в інформаційну систему банку «Приватний» (ст. 361 КК України) — зламали API та викрали дані 18 000 клієнтів (ПІБ, номери карток, CVV). Зловмисники продали дані в даркнеті. Поліція виявила групу через IP-адреси та крипто-гаманці. **Правова кваліфікація:** Несанкціоноване втручання в роботу комп'ютерної системи (ст. 361 КК України), заволодіння інформацією з корисливих мотивів (ст. 361-1 КК України). **Рішення суду:**
    - Засуджено до 5 років позбавлення волі (реальний термін для організатора, умовно для інших).
    - Конфіскація техніки та криптоактивів.
    - Стягнення шкоди банку — 4 800 000 грн. **Наслідки:** Банк посилив захист API, ввів двофакторну автентифікацію для всіх операцій, кримінальний запис для засуджених.
4. **Справа № 826/23456/25Суд:** Окружний адміністративний суд м. Києва **Дата рішення:** 09 листопада 2025 року **Фабула:** Посадова особа ТОВ «CloudHost» (хостинг-провайдер) не повідомила клієнта про витік даних з сервера протягом 72 годин (виявлено витік 15 жовтня 2025 року). Клієнт дізнався від хакерів 2 листопада. Позивач вимагав адміністративної відповідальності посадової особи. **Правова кваліфікація:** Адміністративне правопорушення (ст. 188-39 КУпАП — неналежне реагування на витік даних). **Рішення суду:**
    - Штраф на посадову особу — 17 000 грн.

    - Зобов’язання повідомити всіх постраждалих клієнтів. **Наслідки:** Посадова особа звільнена, компанія посилила процедури реагування, втратила клієнтів.
5. **Справа № 760/54321/26Суд:** Солом’янський районний суд м. Києва **Дата рішення:** 14 квітня 2026 року **Фабула:** Колишній працівник ТОВ «SecureNet» (розробник ПЗ для банків) після звільнення використав конфіденційну інформацію (алгоритми шифрування) для створення конкуруючого продукту. Компанія виявила порушення через аналіз коду конкурента. **Правова кваліфікація:** Порушення NDA та розголошення комерційної таємниці (ст. 505–508 ЦК України). **Рішення суду:**
    - Стягнення збитків 800 000 грн + моральна шкода 50 000 грн.
    - Зобов’язання припинити використання інформації. **Наслідки:** Колишній працівник припинив продаж продукту, компанія отримала компенсацію, посилила контроль за NDA.

Основні скорочення з IT-правової сфери:

- **NDA** — Non-Disclosure Agreement Угода про нерозголошення (конфіденційність). Договір, який забороняє розголошення комерційної таємниці, вихідного коду, бізнес-планів тощо.
- **SLA** — Service Level Agreement Угода про рівень обслуговування. Додаток до договору, де прописані гарантовані показники якості послуги (uptime, час реакції на інцидент, розмір штрафів за порушення тощо).
- **DPIA** — Data Protection Impact Assessment Оцінка впливу на захист даних. Обов’язкова процедура для високоризикових видів обробки персональних даних (згідно з GDPR та Законом України «Про захист персональних даних»).
- **GDPR** — General Data Protection Regulation Загальний регламент захисту даних (Регламент ЄС 2016/679). Основний європейський закон про захист персональних даних, який має екстратериторіальну дію.
- **DSA** — Digital Services Act Акт про цифрові послуги (Регламент ЄС 2022/2065). Регулює обов’язки онлайн-платформ щодо прозорості, модерації контенту, реклами та боротьби з незаконним контентом.
- **DMA** — Digital Markets Act Акт про цифрові ринки (Регламент ЄС 2022/1925). Регулює поведінку великих цифрових платформ («gatekeepers») — Apple, Google, Meta, Amazon тощо.
- **AI Act** — Artificial Intelligence Act Акт про штучний інтелект (Регламент ЄС 2024/1689). Перший у світі комплексний закон про ШІ, який класифікує системи за рівнями ризику (заборонені, високий ризик, обмежений ризик, мінімальний ризик).
- **MiCA** — Markets in Crypto-Assets Регламент щодо ринків криптоактивів (Регламент ЄС 2023/1114). Європейський закон, який регулює випуск, торгівлю та надання послуг з криптоактивами (включаючи стейблкоїни).
- **NIS2** — Network and Information Systems Directive 2 Директива ЄС 2022/2555 про заходи для високого рівня кібербезпеки. Оновлена версія NIS1, яка поширюється на більше секторів критичної інфраструктури.
- **AML** — Anti-Money Laundering Протидія відмиванню коштів. Комплекс заходів (KYC, моніторинг транзакцій тощо) для запобігання легалізації злочинних доходів.
- **KYC** — Know Your Customer Знай свого клієнта. Процедура ідентифікації та верифікації клієнтів (обов’язкова для криптобірж, банків, фінансових сервісів).
- **UI/UX** — User Interface / User Experience Інтерфейс користувача / Досвід користувача. Дизайн та зручність взаємодії з програмою чи сайтом.
- **DDoS** — Distributed Denial of Service Розподілена атака відмови в обслуговуванні. Атака, яка перевантажує сервер запитами, роблячи сайт/сервіс недоступним.
- **NFT** — Non-Fungible Token Невзаємозамінний токен. Унікальний цифровий актив на блокчейні (картинки, музика, відео тощо).
- **ПДФО** — Податок на доходи фізичних осіб 18 % в Україні.

- **РНОКПП** — Реєстраційний номер облікової картки платника податків Колишній ІПН (індивідуальний податковий номер).
- **КУпАП** — Кодекс України про адміністративні правопорушення
- **КК України** — Кримінальний кодекс України
- **ЦК України** — Цивільний кодекс України
- **Дія.City** — спеціальний правовий режим для ІТ-компаній в Україні (Закон № 1667-IX)
- **DPIA** — оцінка впливу на захист даних (Data Protection Impact Assessment)
- **ISO 27001** — міжнародний стандарт системи управління інформаційною безпекою

Офіційні державні та європейські ресурси (1–15)

1. Офіційний вебпортал Верховної Ради України — zakon.rada.gov.ua
2. Сайт Міністерства цифрової трансформації України — thedigital.gov.ua
3. Державна служба спеціального зв'язку та захисту інформації України — cip.gov.ua
4. Реєстр резидентів Дія.City — diia.city/register
5. Єдиний державний реєстр судових рішень — reyestr.court.gov.ua
6. Європейський офіційний портал законодавства — eur-lex.europa.eu
7. Офіційний текст GDPR — eur-lex.europa.eu/eli/reg/2016/679/oj
8. Офіційний текст Digital Services Act (DSA) — eur-lex.europa.eu/eli/reg/2022/2065/oj
9. Офіційний текст Digital Markets Act (DMA) — eur-lex.europa.eu/eli/reg/2022/1925/oj
10. Офіційний текст AI Act (Regulation (EU) 2024/1689) — eur-lex.europa.eu/eli/reg/2024/1689/oj
11. Офіційний текст MiCA (Regulation (EU) 2023/1114) — eur-lex.europa.eu/eli/reg/2023/1114/oj
12. NIS2 Directive — eur-lex.europa.eu/eli/dir/2022/2555/oj
13. Convention 108+ (Council of Europe) — coe.int/en/web/data-protection/convention108+
14. Рекомендація ЮНЕСКО з етики штучного інтелекту — unesdoc.unesco.org/ark:/48223/pf0000381137
15. Tallinn Manual 2.0 (CCDCOE) — ccdcoe.org/research/tallinn-manual

Міжнародні організації та стандарти (16–25)

16. ENISA (European Union Agency for Cybersecurity) — enisa.europa.eu/publications
17. WIPO (World Intellectual Property Organization) — wipo.int
18. ITU (International Telecommunication Union) — itu.int/en/ITU-D/Cybersecurity
19. NIST Cybersecurity Framework — nist.gov/cyberframework
20. ISO/IEC 27001:2022 (Information Security Management) — iso.org/standard/27001
21. OECD AI Principles — oecd.org/going-digital/ai/principles
22. Global Cybersecurity Index (ITU) — itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
23. UNODC Cybercrime Reports — unodc.org/cybercrime
24. Interpol Cybercrime Resources — interpol.int/en/Crimes/Cybercrime
25. NATO Cooperative Cyber Defence Centre of Excellence — ccdcoe.org

Українські та міжнародні аналітичні ресурси (26–35)

26. DOU.ua — розділ «Право та регулювання» — dou.ua/lenta/tags/Право
27. Liga:Закон — liga.net (розділ «ІТ-право»)
28. Юридична газета — yur-gazeta.com (рубрика «Цифрове право»)
29. Mind.ua — розділ «Технології та право» — mind.ua
30. AIN.UA — ain.ua (новини про регулювання ІТ)

31. The Page — thepage.ua (розділ «Технології»)
32. LIGA.Tech — liga.tech
33. Ukrainian Law Blog — ukrainianlawblog.com
34. LegalHub — legalhub.online
35. IT Ukraine Association — itukraine.org.ua (звіти та аналітика)

Освітні платформи та курси (36–45)

36. Prometheus — prometheus.org.ua (курси з цифрового права та кібербезпеки)
37. EdEra — ed-era.com (курси з інформаційного права)
38. Coursera — coursera.org (курси з GDPR, AI Law, Cybersecurity Law)
39. edX — edx.org (курси Harvard, MIT з AI та права)
40. FutureLearn — futurelearn.com (курси з етики ШІ та права)
41. Open University — open.edu/openlearn (безкоштовні курси з цифрового права)
42. Diia.Osvita — diia.gov.ua/osvita (курси з цифрової грамотності та права)
43. Cisco Networking Academy — netacad.com (курси з кібербезпеки та права)
44. Google Digital Garage — learndigital.withgoogle.com (курси з GDPR та реклами)
45. EU Academy — euacademy.europa.eu (курси з DSA, DMA, AI Act)

Репозиторії та бази даних (46–50)

46. GitHub — github.com (репозиторії з відкритим кодом та ліцензіями)
47. EUR-Lex Advanced Search — eur-lex.europa.eu/advanced-search-form.html
48. zakon.rada.gov.ua — офіційна база українського законодавства
49. ЄДРСР — reyestr.court.gov.ua (Єдиний державний реєстр судових рішень)
50. WIPO Lex — wipo.int/wipolex (база міжнародних договорів з інтелектуальної власності)

15. Політика навчальної дисципліни

Політика навчальної дисципліни

1. Академічна доброчесність здобувачів є важливою умовою для опанування результатів навчання за навчальною дисципліною і отримання задовільної оцінки з поточного та підсумкового контролю.

Дотримання академічної доброчесності здобувачами освіти передбачає:

- Самостійне виконання навчальних завдань, завдань поточного та підсумкового контролю результатів навчання;
- Посилання на джерела інформації у разі використання ідей, розробок, тверджень, відомостей;
- Дотримання норм законодавства про авторське право і суміжні права;
- Надання достовірної інформації про результати власної (наукової, творчої) діяльності, використані методики досліджень і джерела інформації.

МДУ виступає за дотримання принципів академічної доброчесності, тому обов'язково використовується сервіс з перевірки робіт здобувачів вищої освіти на плагіат – Unicheck, а також доступний безкоштовний сервіс, який здійснює перевірку на плагіат письмових робіт – EduBirdie https://edubirdie.com/perevirka-na-plagiat .

Порушенням академічної доброчесності, згідно із Законом України «Про освіту» (ст. 42 п. 4) вважається:

- **академічний плагіат** – оприлюднення (частково або повністю) наукових (творчих) результатів, отриманих іншими особами, як результатів власного дослідження (творчості) та / або відтворення опублікованих текстів (оприлюднених творів мистецтва) інших авторів без зазначення авторства;
- **самоплагіат** – оприлюднення (частково або повністю) власних раніше опублікованих наукових результатів як нових наукових результатів;
- **фабрикація** – вигадування даних чи фактів, що використовуються в освітньому процесі або наукових дослідженнях;
- **фальсифікація** – свідома зміна чи модифікація вже наявних даних, що стосуються освітнього процесу чи наукових досліджень;
- **списування** – виконання письмових робіт із залученням зовнішніх джерел інформації, крім дозволених для використання, зокрема під час оцінювання результатів навчання;
- **обман** – надання завідомо неправдивої інформації щодо власної освітньої (наукової, творчої) діяльності чи організації освітнього процесу; формами обману є, зокрема, академічний плагіат, самоплагіат, фабрикація, фальсифікація та списування;
- **хабарництво** – надання (отримання) учасником освітнього процесу чи пропозиція щодо надання (отримання) коштів, майна, послуг, пільг чи будь-яких інших благ матеріального або нематеріального характеру з метою отримання неправомірної переваги в освітньому процесі;
- **необ'єктивне оцінювання** – свідоме завищення або заниження оцінки результатів навчання здобувачів освіти.

Наведений перелік не є остаточно вичерпним і не охоплює всіх діянь, що можуть містити ознаки порушення академічної доброчесності.

За порушення академічної доброчесності здобувачі вищої освіти можуть бути притягнені до наступної академічної відповідальності:

- повторне проходження оцінювання (поточний, підсумковий контроль, залік, іспит тощо);
- проведення додаткової перевірки всіх робіт авторства порушника;
- позбавлення наданих МДУ пільг з оплати навчання;
- оголошення догани із занесенням до особової справи порушника;
- відрахування з МДУ;
- інші, відповідно до вимог чинного законодавства та нормативних локальних актів МДУ.

Більш детально тут 

Анкетування з академічної доброчесності: https://docs.google.com/forms/d/1VHzYkdFEGivtVl-dsENos1SCDRHfUpGia1YklgQK8j0/edit

2. Здобувач має право на оскарження процедури проведення та результатів контрольних заходів згідно Положення про організацію контролю та оцінювання успішності навчання здобувачів вищої освіти в МДУ.

3. Участь в анкетуванні. Наприкінці навчального семестру здобувачам буде запропоновано заповнити анонімну анкету щодо якості викладання вивчених навчальних дисциплін.

Заповнення анкети є важливою для вдосконалення освітнього процесу та системи внутрішнього забезпечення якості освіти МДУ та дозволить оцінити дієвість застосованих методів викладання та врахувати вашу думку стосовно покращення змісту навчальних дисциплін.

4. Неформальна освіта. Це освіта, яка здобувається, як правило, за освітніми програмами та не передбачає присудження визнаних державою освітніх кваліфікацій за рівнями освіти, але може завершуватися присвоєнням професійних та/або присудженням часткових освітніх кваліфікацій. Здобувач вищої освіти, який виявив бажання щодо визнання результатів, отриманих у неформальній освіті, звертається із відповідною заявою про визнання результатів, отриманих у неформальній освіті, в цілому для навчальної дисципліни /змістового модулю /практичних завдань з навчальної дисципліни/ завдань з практики тощо для здобувачів вищої освіти, до деканату факультету, на якому викладається навчальна дисципліна. Процедура зарахування здійснюється згідно Порядку визнання результатів навчання, отриманих у неформальній освіті МДУ.

Ресурси:

https://prometheus.org.ua/ - Prometheus – Найкращі онлайн-курси України та світу
https://www.ed-era.com/ - EdEra – студія онлайн-освіти
https://www.prostir.ua/ - Громадський простір

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО НАВЧАЛЬНУ ДИСЦИПЛІНУ

Назва навчальної дисципліни	Сучасне правове регулювання в сфері ІТ
Освітня програма	Кібербезпека
Рівень вищої освіти	Перший (бакалавр)
Кафедра, яка здійснює викладання	Кафедра права, Кафедра системного аналізу та інформаційних технологій
Викладач ПІБ, посада	Волік Вячеслав Вікторович – доктор юридичних наук, професор, професор кафедри права МДУ
Електронна адреса викладача	v.volik@mdu.edu.ua
Консультації (дата, час, можливості онлайн консультування)	Онлайн консультування Viber, Telegram, WhatsApp
Посилання на сторінку навчальної дисципліни на Навчальному порталі МДУ	https://moodle.mu.edu.ua/my/courses.php
Компетентності та програмні результати навчання	ЗК1, ЗК2, ЗК5 ФК2, ФК3, ФК4 РН1, РН4, РН6

Семестр(и) вивчення	**Обсяг (години/ кредити)**	**Кількість аудиторних годин**		**Кількість, види індивідуальних завдань**	**Форма контролю**
		лекції	**семінар.**		
І-й	90/3	12/8	12/8	Реферат (есе, доповідь для обговорення), тест, кейсові завдання, портфоліо	Залік

Завідувач кафедри _____ **Вікторія ГРИГОР'ЄВА**

Гарант ОП _____