МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
Кафедра права
Кафедра системного аналізу та інформаційних технологій

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

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «НОРМАТИВНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ»

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

2025-2026 рр.

Робоча програма навчальної дисципліни «Нормативно-правове забезпечення інформаційної безпеки» 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 2-го року навчання)	3-й (для бакалаврів 2-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 для забезпечення інформаційної безпеки в IT-сфері, правоохоронних органах та інших організаціях. Вона взаємопов'язана з дисциплінами «Основи права», «Основи інформаційної безпеки» 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 нормативно-правового регулювання інформаційної безпеки, включаючи національне законодавство України, міжнародні стандарти та правові механізми захисту інформації в умовах цифровізації, кіберзагроз і воєнного стану. Дисципліна спрямована на підготовку фахівців, здатних аналізувати правові аспекти кібербезпеки, розробляти заходи захисту інформації, реагувати на кіберінциденти та прогнозувати їх правові наслідки в професійній діяльності.

Завдання навчальної дисципліни:

1. Ознайомлення з основними аспектами нормативно-правового забезпечення інформаційної безпеки, включаючи:
    - аналіз національного законодавства України у сфері кібербезпеки;
    - вивчення міжнародних стандартів і конвенцій (наприклад, Конвенція Ради Європи про кіберзлочинність, ISO/IEC 27001);
    - правові механізми захисту інформації від кіберзагроз;
    - регулювання інформаційної безпеки в умовах воєнного стану;
    - правові та етичні аспекти використання штучного інтелекту в кібербезпеці;
    - захист критичної інфраструктури, регулювання кібероперацій та відповідальність за кіберінциденти.
2. Формування навичок аналізу нормативно-правових актів, судової практики та міжнародних стандартів у сфері кібербезпеки.
3. Розвиток умінь розробляти заходи захисту інформації, реагувати на кіберінциденти та прогнозувати їх правові наслідки.
4. Виховання професійної етики та відповідальності за дотримання принципів захисту даних і інформаційної безпеки.

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

Змістовий модуль 1: Основи нормативно-правового регулювання інформаційної безпеки

Тема 1. Поняття та принципи інформаційної безпеки

- **Зміст:** Визначення інформаційної безпеки. Основні принципи правового регулювання (конфіденційність, цілісність, доступність). Закон України «Про кібербезпеку».
- **Актуальні проблеми:** Недостатня гармонізація законодавства з міжнародними стандартами, правові прогалини.
- **Документи для аналізу:** Закон України «Про кібербезпеку» (2017).
- **Література:**
    1. Кліщенко В.О. Нормативно-правове забезпечення кібербезпеки. Київ: Юрінком Інтер, 2023. – С. 10–30.
    2. Совгиря О.В. Правові основи інформаційної безпеки. Київ: Ваіте, 2022. – С. 15–40.
    3. Закон України «Про кібербезпеку» від 05.10.2017 № 2163-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
    4. Погребняк С.П. Принципи інформаційної безпеки. Журнал східноєвропейського права. – 2022. – № 95. – С. 12–22. URL: https://doi.org/10.5281/zenodo.4701234.
    5. Хоменко В.М. Законодавство України у сфері кібербезпеки. Право України. – 2022. – № 11. – С. 20–35.
    6. Білак М. Нормативно-правова база кібербезпеки. Юридичний вісник. – 2021. – № 7. – С. 10–20.
    7. ENISA. EU Cybersecurity Legislation Overview. 2022. – С. 5–15. URL: https://www.enisa.europa.eu/publications.
    8. ISO/IEC 27001:2022. Information Security Management Systems. – С. 1–10. URL: https://www.iso.org/standard/27001.
    9. NIST. Cybersecurity Framework. 2021. – С. 10–20. URL: https://www.nist.gov/cyberframework.
    10. Кравець І.М. Основи інформаційної безпеки: правовий аспект. Право України. – 2021. – № 10. – С. 15–25.

Тема 2. Національне законодавство у сфері кібербезпеки

- **Зміст:** Закон України «Про основи національної безпеки». Структура та функції державних органів у сфері кібербезпеки (СБУ, Держспецзв’язку).
- **Актуальні проблеми:** Координація між державними органами, імплементація законодавства.
- **Документи для аналізу:** Закон України «Про основи національної безпеки» (2018).
- **Література:**
    1. Кравець І.М. Законодавство України у сфері кібербезпеки. Право України. – 2021. – № 9. – С. 15–25.
    2. Совгиря О.В. Державні органи у сфері кібербезпеки. Київ: Ваіте, 2022. – С. 40–60.
    3. Закон України «Про основи національної безпеки» від 19.06.2018 № 2469-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.
    4. Білак М. Координація державних органів у кібербезпеці. Юридичний вісник. – 2021. – № 8. – С. 10–20.
    5. Погребняк С.П. Імплементація законодавства у сфері кібербезпеки. Вісник НАПрН України. – 2022. – № 6. – С. 12–22.
    6. Хоменко В.М. Роль Держспецзв’язку у кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 100–110.
    7. ENISA. National Cybersecurity Strategies. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.

8. NIST. Cybersecurity Framework. 2021. – С. 15–25. URL: https://www.nist.gov/cyberframework.
9. Council of Europe. Cybersecurity Governance Report. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
10. Кліщенко В.О. Національні механізми кібербезпеки. Київ: Юрінком Інтер, 2023. – С. 50–70.

Тема 3. Міжнародні стандарти інформаційної безпеки

- **Зміст:** Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція). Стандарти ISO/IEC 27001, NIST Cybersecurity Framework. Роль ENISA та ITU.
- **Актуальні проблеми:** Імплементація міжнародних стандартів в Україні, адаптація до нових кіберзагроз.
- **Документи для аналізу:** Конвенція Ради Європи про кіберзлочинність (2001).
- **Література:**
  1. Совгиря О.В. Міжнародні стандарти кібербезпеки. Київ: Ваіте, 2022. – С. 60–80.
  2. Кліщенко В.О. Конвенція про кіберзлочинність. Право України. – 2021. – № 8. – С. 20–35.
  3. Council of Europe. Budapest Convention on Cybercrime. 2001 (оновлення 2023). URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
  4. Білак М. Імплементація стандартів ISO/IEC 27001. Юридичний вісник. – 2021. – № 8. – С. 10–20.
  5. Погребняк С.П. Роль ENISA у кібербезпеці. Вісник НАПрН України. – 2022. – № 6. – С. 12–22.
  6. Хоменко В.М. Міжнародні стандарти інформаційної безпеки. Актуальні проблеми державотворення. – 2022. – С. 110–120.
  7. ISO/IEC 27001:2022. Information Security Management Systems. – С. 1–10. URL: https://www.iso.org/standard/27001.
  8. NIST. Cybersecurity Framework. 2021. – С. 20–30. URL: https://www.nist.gov/cyberframework.
  9. ENISA. Cybersecurity Standards Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
  10. Кравець І.М. Міжнародне співробітництво у сфері кібербезпеки. Право України. – 2021. – № 10. – С. 25–35.

Тема 4. Правові аспекти захисту персональних даних

- **Зміст:** Закон України «Про захист персональних даних». GDPR (Загальний регламент захисту даних ЄС). Механізми захисту даних у кіберпросторі.
- **Актуальні проблеми:** Гармонізація українського законодавства з GDPR, захист даних у хмарних технологіях.
- **Документи для аналізу:** Закон України «Про захист персональних даних» (2010), GDPR (2016).
- **Література:**
  1. Кравець І.М. Захист персональних даних: правові аспекти. Право України. – 2021. – № 9. – С. 15–25.
  2. Совгиря О.В. GDPR та Україна. 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. Юридичний вісник. – 2021. – № 9. – С. 10–20.
  6. Погребняк С.П. Захист даних у воєнний період. Вісник НАПрН України. – 2022. – № 7. – С. 15–25.

7. Хоменко В.М. Судова практика у сфері захисту даних. 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 Protection Guide. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кліщенко В.О. Захист даних у кіберпросторі. Київ: Юрінком Інтер, 2023. – С. 90–110.

Тема 5. Правове регулювання кіберзлочинності

- **Зміст:** Поняття кіберзлочинності. Кримінальний кодекс України (статті 361–363). Механізми розслідування кіберзлочинів. Міжнародне співробітництво.
- **Актуальні проблеми:** Недостатня ефективність розслідування, проблеми юрисдикції.
- **Документи для аналізу:** Кримінальний кодекс України (статті 361–363).
- **Література:**
  1. Совгиря О.В. Кіберзлочинність: правові аспекти. Київ: Ваіте, 2022. – С. 100–120.
  2. Кравець І.М. Розслідування кіберзлочинів. Журнал східноєвропейського права. – 2021. – № 96. – С. 10–20. URL: https://doi.org/10.5281/zenodo.4712345.
  3. Кримінальний кодекс України від 05.04.2001 № 2341-III (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text.
  4. Білак М. Міжнародне співробітництво у боротьбі з кіберзлочинністю. Юридичний вісник. – 2021. – № 10. – С. 15–25.
  5. Погребняк С.П. Проблеми розслідування кіберзлочинів. Вісник НАПрН України. – 2022. – № 8. – С. 12–22.
  6. Хоменко В.М. Правове регулювання кіберзлочинності. Актуальні проблеми державотворення. – 2022. – С. 130–140.
  7. Council of Europe. Budapest Convention on Cybercrime. 2001 (оновлення 2023). URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
  8. UNODC. Comprehensive Study on Cybercrime. 2021. – С. 20–30. URL: https://www.unodc.org/documents/organized-crime/cybercrime/UNODC_Study_on_Cybercrime.pdf.
  9. ENISA. Cybercrime Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
  10. Кліщенко В.О. Механізми протидії кіберзлочинності. Київ: Юрінком Інтер, 2023. – С. 120–140.

Тема 6. Захист критичної інфраструктури

- **Зміст:** Поняття критичної інфраструктури. Законодавство України про захист критичної інфраструктури. Міжнародні стандарти захисту.
- **Актуальні проблеми:** Кібератаки на критичну інфраструктуру, координація між секторами.
- **Документи для аналізу:** Закон України «Про критичну інфраструктуру і її захист» (2021).
- **Література:**
  1. Кравець І.М. Захист критичної інфраструктури. Право України. – 2022. – № 10. – С. 15–25.
  2. Совгиря О.В. Кібербезпека критичної інфраструктури. Київ: Ваіте, 2022. – С. 120–140.
  3. Закон України «Про критичну інфраструктуру і її захист» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.
  4. Білак М. Кібератаки на критичну інфраструктуру. Юридичний вісник. – 2022. – № 11. – С. 10–20.
  5. Погребняк С.П. Міжнародні стандарти захисту критичної інфраструктури. Вісник НАПрН України. – 2022. – № 9. – С. 15–25.

6. Хоменко В.М. Координація захисту критичної інфраструктури. Актуальні проблеми державотворення. – 2022. – С. 140–150.
7. ENISA. Critical Infrastructure Protection Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
8. NATO. Critical Infrastructure Protection Guidelines. 2022. – С. 5–15. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm.
9. Council of Europe. Report on Critical Infrastructure and Cybersecurity. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
10. Кліщенко В.О. Захист критичної інфраструктури від кіберзагроз. Київ: Юрінком Інтер, 2023. – С. 150–170.

Тема 7. Інформаційна безпека в умовах воєнного стану

- **Зміст:** Правові аспекти захисту інформації в умовах воєнного стану. Закон України «Про правовий режим воєнного стану». Реагування на кібератаки.
- **Актуальні проблеми:** Захист інформації в умовах війни, правові обмеження.
- **Документи для аналізу:** Закон України «Про правовий режим воєнного стану» (2015).
- **Література:**
  1. Кравець І.М. Інформаційна безпека в умовах воєнного стану. Право України. – 2022. – № 12. – С. 15–25.
  2. Совгиря О.В. Кібербезпека в умовах війни. Київ: Ваіте, 2022. – С. 140–160.
  3. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/389-19#Text.
  4. Білак М. Захист інформації в умовах війни. Юридичний вісник. – 2022. – № 11. – С. 10–20.
  5. Погребняк С.П. Кібератаки в умовах війни. Вісник НАПрН України. – 2022. – № 9. – С. 15–25.
  6. Хоменко В.М. Правові аспекти захисту інформації в умовах війни. Актуальні проблеми державотворення. – 2022. – С. 150–160.
  7. NATO. Cybersecurity in Wartime. 2022. – С. 5–15. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm.
  8. ENISA. Cybersecurity in Armed Conflicts. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
  9. Council of Europe. Report on Cybersecurity in Armed Conflicts. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
  10. Кліщенко В.О. Кібербезпека в умовах воєнного стану. Київ: Юрінком Інтер, 2023. – С. 170–190.

Тема 8. Правові аспекти кібероперацій

- **Зміст:** Поняття кібероперацій. Міжнародне право та кібервійни. Талліннський посібник 2.0.
- **Актуальні проблеми:** Відповідальність за кібероперації, юрисдикція в кіберпросторі.
- **Документи для аналізу:** Талліннський посібник 2.0 (2017).
- **Література:**
  1. Кліщенко В.О. Кібероперації та міжнародне 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. Правове регулювання кібероперацій. Київ: Ваіте, 2022. – С. 160–180.
  3. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2017 (оновлення 2023). – С. 50–70. URL: https://ccdcoe.org/research/tallinn-manual/.
  4. Білак М. Відповідальність за кібероперації. Юридичний вісник. – 2022. – № 12. – С. 15–25.
  5. Погребняк С.П. Юрисдикція в кіберпросторі. Вісник НАПрН України. – 2022. – № 10. – С. 12–22.

6. Хоменко В.М. Кібервійни та міжнародне право. Актуальні проблеми державотворення. – 2022. – С. 160–170.
7. UN Group of Governmental Experts Report on Cyberspace. 2021. – С. 10–20. URL: https://www.un.org/disarmament/group-of-governmental-experts/.
8. Council of Europe. Report on Cyber Operations. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
9. ENISA. Cyber Operations Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кравець І.М. Міжнародне право та кібероперації. Право України. – 2021. – № 11. – С. 20–30.

Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці

- **Зміст:** Правове регулювання штучного інтелекту (ШІ) у кібербезпеці. Етичні принципи використання ШІ. Рекомендація ЮНЕСКО та EU AI Act.
- **Актуальні проблеми:** Недостатність правового регулювання ШІ, етичні виклики.
- **Документи для аналізу:** Рекомендація ЮНЕСКО з етики штучного інтелекту (2021), EU AI Act (2021).
- **Література:**

1. Кліщенко В.О. Штучний інтелект у кібербезпеці. Юридичний науковий електронний журнал. – 2022. – № 5. – С. 40–50. URL: https://doi.org/10.32782/2524-0374/2022-5/40.
2. Совгиря О.В. Правове регулювання ШІ. 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 ШІ в кібербезпеці. Юридичний вісник. – 2022. – № 12. – С. 15–25.
6. Погребняк С.П. Правові виклики ШІ. Вісник НАПрН України. – 2022. – № 10. – С. 12–22.
7. Хоменко В.М. Регулювання ШІ в кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 170–180.
8. Council of Europe. Report on Artificial Intelligence and Cybersecurity. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications.
9. ENISA. AI and Cybersecurity Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кравець І.М. Етика ШІ в кібербезпеці. Право України. – 2021. – № 12. – С. 20–30.

Тема 10. Відповідальність за порушення у сфері інформаційної безпеки

- **Зміст:** Види відповідальності (адміністративна, кримінальна, цивільна) за порушення інформаційної безпеки. Практика притягнення до відповідальності.
- **Актуальні проблеми:** Проблеми доказування кіберзлочинів, міжнародна відповідальність.
- **Документи для аналізу:** Кримінальний кодекс України (статті 361–363), Кодекс України про адміністративні правопорушення.
- **Література:**

1. Кравець І.М. Відповідальність за кіберзлочини. Право України. – 2022. – № 11. – С. 15–25.
2. Совгиря О.В. Правова відповідальність у кібербезпеці. Київ: Ваіте, 2022. – С. 200–220.
3. Кримінальний кодекс України від 05.04.2001 № 2341-III (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2341-14#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 кіберзлочинів. Юридичний вісник. – 2022. – № 13. – С. 10–20.
6. Погребняк С.П. Міжнародна відповідальність за кіберзлочини. Вісник НАПрН України. – 2022. – № 11. – С. 12–22.
7. Хоменко В.М. Правові аспекти відповідальності у кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 180–190.
8. UNODC. Comprehensive Study on Cybercrime. 2021. – С. 30–40. URL: https://www.unodc.org/documents/organized-crime/cybercrime/UNODC_Study_on_Cybercrime.pdf.
9. ENISA. Cybercrime Liability Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications.
10. Кліщенко В.О. Відповідальність за порушення кібербезпеки. 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 інформаційної безпеки	10	2	2	6	1	10	1	1	8	1
Тема 2. Національне законодавство у сфері кібербезпеки	8	1	1	6	1	9	1	1	7	1
Тема 3. Міжнародні стандарти інформаційної безпеки	8	1	1	6	1	9	1	1	7	1
Тема 4. Правові аспекти захисту персональних даних	8	1	1	6	1	9	1	1	7	1
Тема 5. Правове регулювання кіберзлочинності	8	1	1	6	1	9	1	1	7	1
Тема 6. Захист критичної інфраструктури	8	1	1	6	1	9	1	1	7	1
Тема 7. Інформаційна безпека в умовах воєнного стану	10	2	2	6	1	10	1	1	8	1
Тема 8. Правові аспекти кібероперацій	8	1	1	6	1	9	1	1	7	1
Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці	9	1	1	7	1	8	0	0	8	1
Тема 10. Відповідальність за порушення у сфері інформаційної безпеки	9	1	1	7	1	8	0	0	8	1
Разом	**90**	**12**	**12**	**66**	**12**	**90**	**8**	**8**	**74**	**12**

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 інформаційної безпеки Зміст: Визначення інформаційної безпеки. Основні принципи правового регулювання (конфіденційність, цілісність, доступність). Закон України «Про кібербезпеку». Література: Кліщенко В.О. Нормативно-правове забезпечення кібербезпеки. Київ: Юрінком Інтер, 2023. – С. 10–30. Совгиря О.В. Правові основи інформаційної безпеки. Київ: Ваіте, 2022. – С. 15–40. Погребняк С.П. Принципи інформаційної безпеки. Журнал східноєвропейського права. – 2022. – № 95. – С. 12–22. URL: . Хоменко В.М. Законодавство	Сформувати системне розуміння теми та навички застосування норм права до типових кейсів у сфері ІБ.	1) Скласти глосарій з 15 ключових термінів. 2) Побудувати схему суб’єктів та їх повноважень. 3) Проаналізувати 1 нормативний акт (структура, вимоги). 4) Підготувати короткий кейс-стаді з практики (1 стор.). 5) Сформувати 5 висновків і 3 рекомендації.	1) Скласти глосарій з 15 ключових термінів (самост.) 2) Побудувати схему суб’єктів та їх повноважень (самост.) 3) Проаналізувати 1 нормативний акт (структура, вимоги) (самост.) 4) Підготувати короткий кейс-стаді з практики (1 стор.) (самост.) 5) Сформувати 5 висновків і 3 рекомендації (самост.)	РН1, РН4

	України у сфері кібербезпеки. Право України. – 2022. – № 11. – С. 20–35. Білак М. Нормативно-правова база кібербезпеки. Юридичний вісник. – 2021. – № 7. – С. 10–20.				
2	Тема 2. Національне законодавство у сфері кібербезпеки Зміст: Закон України «Про основи національної безпеки». Структура та функції державних органів у сфері кібербезпеки (СБУ, Держспецзв’язку). Література: Кравець І.М. Законодавство України у сфері кібербезпеки. Право України. – 2021. – № 9. – С. 15–25. Совгиря О.В. Державні органи у сфері кібербезпеки. Київ: Ваіте, 2022. – С. 40–60. Білак М. Координація державних органів у кібербезпеці. Юридичний вісник. – 2021. – № 8. – С. 10–20.	Сформувати системне розуміння теми та навички застосування норм права до типових кейсів у сфері ІБ.	1) Скласти глосарій з 15 ключових термінів. 2) Побудувати схему суб’єктів та їх повноважень. 3) Проаналізувати 1 нормативний акт (структура, вимоги). 4) Підготувати короткий кейс-стаді з практики (1 стор.). 5) Сформувати 5 висновків і 3 рекомендації.	1) Скласти глосарій з 15 ключових термінів (самост.) 2) Побудувати схему суб’єктів та їх повноважень (самост.) 3) Проаналізувати 1 нормативний акт (структура, вимоги) (самост.) 4) Підготувати короткий кейс-стаді з практики (1 стор.) (самост.) 5) Сформувати 5 висновків і 3 рекомендації (самост.)	РН1, РН4

	Погребняк С.П. Імплементація законодавства у сфері кібербезпеки. Вісник НАПрН України. – 2022. – № 6. – С. 12–22. Хоменко В.М. Роль Держспецзв’язку у кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 100–110.				
3	Тема 3. Міжнародні стандарти інформаційної безпеки Зміст: Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція). Стандарти ISO/IEC 27001, NIST Cybersecurity Framework. Роль ENISA та ITU. Література: Совгиря О.В. Міжнародні стандарти кібербезпеки. Київ: Ваіте, 2022. – С. 60–80. Кліщенко В.О. Конвенція про кіберзлочинність. Право України. – 2021. – № 8. – С. 20–35. Білак М. Імплементація стандартів ISO/IEC	Опанувати вимоги ISO/IEC 27001/27002 та їх застосування в українських організаціях.	1) Зробити огляд ISO/IEC 27001:2022 (структура розділів). 2) Скласти мапінг Annex A → нац. вимоги (5 контролів). 3) Побудувати реєстр ризиків (5 ризиків). 4) Скласти перелік документованої інформації (10 позицій). 5) Підготувати план внутрішнього аудиту ISMS.	1) Зробити огляд ISO/IEC 27001:2022 (структура розділів) (самост.) 2) Скласти мапінг Annex A → нац. вимоги (5 контролів) (самост.) 3) Побудувати реєстр ризиків (5 ризиків) (самост.) 4) Скласти перелік документованої інформації (10 позицій) (самост.) 5) Підготувати план внутрішнього аудиту ISMS (самост.)	РН1, РН6

	27001. Юридичний вісник. – 2021. – № 8. – С. 10–20. Погребняк С.П. Роль ENISA у кібербезпеці. Вісник НАПрН України. – 2022. – № 6. – С. 12–22. Хоменко В.М. Міжнародні стандарти інформаційної безпеки. Актуальні проблеми державотворення. – 2022. – С. 110–120.				
4	Тема 4. Правові аспекти захисту персональних даних Зміст: Закон України «Про захист персональних даних». GDPR (Загальний регламент захисту даних ЄС). Механізми захисту даних у кіберпросторі. Література: Кравець І.М. Захист персональних даних: правові аспекти. Право України. – 2021. – № 9. – С. 15–25. Совгиря О.В. GDPR та Україна. Київ: Ваіте, 2022. – С. 80–100. Білак М. Гармонізація з	Сформувати компетентності з дотримання вимог захисту ПД (правові підстави, права суб’єктів, DPIA, реагування на витоки).	1) Проаналізувати правові підстави обробки ПД (5 прикладів). 2) Провести DPIA для сервісу (1 стор.). 3) Підготувати політику конфіденційності (чернетка). 4) Розробити процедуру повідомлення про витік (72 год.). 5) Скласти пам’ятку прав суб’єкта даних.	1) Проаналізувати правові підстави обробки ПД (5 прикладів) (самост.) 2) Провести DPIA для сервісу (1 стор.) (самост.) 3) Підготувати політику конфіденційності (чернетка) (самост.) 4) Розробити процедуру повідомлення про витік (72 год.) (самост.) 5) Скласти пам’ятку прав суб’єкта даних (самост.)	РН1, РН4

	GDPR. Юридичний вісник. – 2021. – № 9. – С. 10–20. Погребняк С.П. Захист даних у воєнний період. Вісник НАПрН України. – 2022. – № 7. – С. 15–25. Хоменко В.М. Судова практика у сфері захисту даних. Актуальні проблеми державотворення. – 2022. – С. 120–130.				
5	Тема 5. Правове регулювання кіберзлочинності Зміст: Поняття кіберзлочинності. Кримінальний кодекс України (статті 361–363). Механізми розслідування кіберзлочинів. Міжнародне співробітництво. Література: Совгиря О.В. Кіберзлочинність: правові аспекти. Київ: Ваіте, 2022. – С. 100–120. Кравець І.М. Розслідування кіберзлочинів. Журнал східноєвропейського права. – 2021. – № 96. – С. 10–20. URL: . Білак М. Міжнародне співробітництво у	Сформувати навички кваліфікації кіберзлочинів і роботи з цифровими доказами згідно з КК України.	1) Класифікувати склади розд. XVI КК (5 прикладів). 2) Проаналізувати 2 судові кейси за ст. 361, 362 КК. 3) Скласти алгоритм збору цифрових доказів. 4) Підготувати рекомендації щодо співпраці з провайдерами. 5) Оцінити санкції та запропонувати зміни (1 стор.).	1) Класифікувати склади розд. XVI КК (5 прикладів) (самост.) 2) Проаналізувати 2 судові кейси за ст. 361, 362 КК (самост.) 3) Скласти алгоритм збору цифрових доказів (самост.) 4) Підготувати рекомендації щодо співпраці з провайдерами (самост.) 5) Оцінити санкції та запропонувати зміни (1 стор.) (самост.)	РН1, РН4

	боротьбі з кіберзлочинністю. Юридичний вісник. – 2021. – № 10. – С. 15–25. Погребняк С.П. Проблеми розслідування кіберзлочинів. Вісник НАПрН України. – 2022. – № 8. – С. 12–22. Хоменко В.М. Правове регулювання кіберзлочинності. Актуальні проблеми державотворення. – 2022. – С. 130–140.				
6	Тема 6. Захист критичної інфраструктури Зміст: Поняття критичної інфраструктури. Законодавство України про захист критичної інфраструктури. Міжнародні стандарти захисту. Література: Кравець І.М. Захист критичної інфраструктури. Право України. – 2022. – № 10. – С. 15–25. Совгиря О.В. Кібербезпека критичної інфраструктури. Київ: Ваіте, 2022. – С. 120–140. Білак М. Кібератаки на	Опанувати правові засади захисту критичної інформаційної інфраструктур и та алгоритми реагування на інциденти.	1) Ідентифікувати об’єкти КІ у вибраній галузі (5 прикладів). 2) Побудувати схему взаємодії суб’єктів захисту КІ. 3) Скласти чек-лист вимог до оператора КІ (10 пунктів). 4) Моделювання інциденту та алгоритм реагування. 5) Оцінити ризики для КІ (5 ризиків, заходи зниження).	1) Ідентифікувати об’єкти КІ у вибраній галузі (5 прикладів) (самост.) 2) Побудувати схему взаємодії суб’єктів захисту КІ (самост.) 3) Скласти чек-лист вимог до оператора КІ (10 пунктів) (самост.) 4) Моделювання інциденту та алгоритм реагування (самост.) 5) Оцінити ризики для КІ (5 ризиків, заходи зниження) (самост.)	РН1, РН4

	критичну інфраструктуру. Юридичний вісник. – 2022. – № 11. – С. 10–20. Погребняк С.П. Міжнародні стандарти захисту критичної інфраструктури. Вісник НАПрН України. – 2022. – № 9. – С. 15–25. Хоменко В.М. Координація захисту критичної інфраструктури. Актуальні проблеми державотворення. – 2022. – С. 140–150.				
7	Тема 7. Інформаційна безпека в умовах воєнного стану Зміст: Правові аспекти захисту інформації в умовах воєнного стану. Закон України «Про правовий режим воєнного стану». Реагування на кібератаки. Література: Кравець І.М. Інформаційна безпека в умовах воєнного стану. Право України. – 2022. – № 12. – С. 15–25. Совгиря О.В. Кібербезпека в умовах війни. Київ: Ваіте, 2022. –	Зрозуміти вплив правового режиму воєнного стану на інформаційну безпеку та права людини.	1) Визначити обмеження прав в умовах ВС (5 прикладів). 2) Проаналізувати вплив ВС на обмін даними. 3) Підготувати аналітичну записку про кіберінциденти у ВС. 4) Розробити протокол комунікацій під час інциденту. 5) Оцінити баланс безпека/права людини.	1) Визначити обмеження прав в умовах ВС (5 прикладів) (самост.) 2) Проаналізувати вплив ВС на обмін даними (самост.) 3) Підготувати аналітичну записку про кіберінциденти у ВС (самост.) 4) Розробити протокол комунікацій під час інциденту (самост.) 5) Оцінити баланс безпека/права людини (самост.)	РН1, РН4

	С. 140–160. Білак М. Захист інформації в умовах війни. Юридичний вісник. – 2022. – № 11. – С. 10–20. Погребняк С.П. Кібератаки в умовах війни. Вісник НАПрН України. – 2022. – № 9. – С. 15–25. Хоменко В.М. Правові аспекти захисту інформації в умовах війни. Актуальні проблеми державотворення. – 2022. – С. 150–160.				
8	Тема 8. Правові аспекти кібероперацій Зміст: Поняття кібероперацій. Міжнародне право та кібервійни. Талліннський посібник 2.0. Література: Кліщенко В.О. Кібероперації та міжнародне право. Юридичний науковий електронний журнал. – 2022. – № 5. – С. 40–50. URL: . Совгиря О.В. Правове регулювання кібероперацій. Київ: Ваіте, 2022. – С. 160–180. Tallinn Manual 2.0	Розібрати застосовність норм міжнародного права до кібероперацій і механізми відповідальності.	1) Скласти дефініції та класифікацію кібероперацій. 2) Проаналізувати застосовність міжнародного права (Tallinn). 3) Описати режим атрибуції та реторсій (1 стор.). 4) Скласти матрицю відповідальності держав/недержавних акторів. 5) Розібрати кейс NotPetya з правової точки зору.	1) Скласти дефініції та класифікацію кібероперацій (самост.) 2) Проаналізувати застосовність міжнародного права (Tallinn) (самост.) 3) Описати режим атрибуції та реторсій (1 стор.) (самост.) 4) Скласти матрицю відповідальності держав/недержавних акторів (самост.) 5) Розібрати кейс NotPetya з правової точки зору (самост.)	РН1, РН4

	on the International Law Applicable to Cyber Operations. 2017 (оновлення 2023). – С. 50–70. URL: . Білак М. Відповідальність за кібероперації. Юридичний вісник. – 2022. – № 12. – С. 15–25. Погребняк С.П. Юрисдикція в кіберпросторі. Вісник НАПрН України. – 2022. – № 10. – С. 12–22.				
9	Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці Зміст: Правове регулювання штучного інтелекту (ШІ) у кібербезпеці. Етичні принципи використання ШІ. Рекомендація ЮНЕСКО та EU AI Act. Література: Кліщенко В.О. Штучний інтелект у кібербезпеці. Юридичний науковий електронний журнал. – 2022. – № 5. – С. 40–50. URL: . Совгиря О.В. Правове регулювання ШІ. Київ: Ваіте, 2022. –	Засвоїти правові вимоги до систем ШІ та етичні/безпекові аспекти їх застосування у сфері ІБ.	1) Визначити категорії ризику систем ШІ (5 прикладів). 2) Проаналізувати вимоги до високоризикових систем (AI Act). 3) Розробити політику прозорості для використання ШІ. 4) Підготувати перелік даних і заходів їх захисту. 5) Оцінити відповідність етичним принципам (UNESCO).	1) Визначити категорії ризику систем ШІ (5 прикладів) (самост.) 2) Проаналізувати вимоги до високоризикових систем (AI Act) (самост.) 3) Розробити політику прозорості для використання ШІ (самост.) 4) Підготувати перелік даних і заходів їх захисту (самост.) 5) Оцінити відповідність етичним принципам (UNESCO) (самост.)	РН1, РН4

	С. 180–200. Рекомендація ЮНЕСКО з етики штучного інтелекту. 2021. – С. 5–15. URL: . European Commission. AI Act Proposal. 2021. – С. 10–20. URL: . Білак М. Етичні аспекти ШІ в кібербезпеці. Юридичний вісник. – 2022. – № 12. – С. 15–25.				
10	Тема 10. Відповідальність за порушення у сфері інформаційної безпеки Зміст: Види відповідальності (адміністративна, кримінальна, цивільна) за порушення інформаційної безпеки. Практика притягнення до відповідальності. Література: Кравець І.М. Відповідальність за кіберзлочини. Право України. – 2022. – № 11. – С. 15–25. Совгиря О.В. Правова відповідальність у кібербезпеці. Київ: Ваіте, 2022. – С. 200–220. Білак М. Доказування кіберзлочинів.	Опанувати механізми юридичної відповідальності за порушення у сфері ІБ та специфіку проваджень.	1) Скласти таблицю складів правопорушень у сфері ІБ (5). 2) Проаналізувати юрисдикцію та підслідність у кіберсправах. 3) Підготувати схему провадження у справах ІБ. 4) Розглянути проблеми доказування цифрових фактів. 5) Сформулювати пропозиції щодо удосконалення норм.	1) Скласти таблицю складів правопорушень у сфері ІБ (5) (самост.) 2) Проаналізувати юрисдикцію та підслідність у кіберсправах (самост.) 3) Підготувати схему провадження у справах ІБ (самост.) 4) Розглянути проблеми доказування цифрових фактів (самост.) 5) Сформулювати пропозиції щодо удосконалення норм (самост.)	РН1, РН4

Юридичний вісник. – 2022. – № 13. – С. 10–20.
Погребняк С.П. Міжнародна відповідальність за кіберзлочини. Вісник НАПрН України. – 2022. – № 11. – С. 12–22.
Хоменко В.М. Правові аспекти відповідальності у кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 180–190.

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.

Тема 1. Поняття та принципи інформаційної безпеки (7 год.)

1. Підготовка реферату «Принципи інформаційної безпеки» (2 год.).
2. Аналіз Закону України «Про кібербезпеку» (2017) (2 год.).
3. Складання схеми принципів інформаційної безпеки (2 год.).
4. Порівняння національних і міжнародних підходів до кібербезпеки (1 год.).

Тема 2. Національне законодавство у сфері кібербезпеки (7 год.)

1. Аналіз Закону України «Про основи національної безпеки» (2 год.).
2. Підготовка доповіді про роль державних органів у кібербезпеці (2 год.).
3. Дослідження координації між СБУ та Держспецзв'язку (2 год.).
4. Складання переліку функцій державних органів (1 год.).

Тема 3. Міжнародні стандарти інформаційної безпеки (7 год.)

1. Аналіз Будапештської конвенції про кіберзлочинність (2 год.).
2. Підготовка есе «Роль ISO/IEC 27001 у кібербезпеці» (2 год.).
3. Дослідження діяльності ENISA (2 год.).
4. Складання таблиці міжнародних стандартів (1 год.).

Тема 4. Правові аспекти захисту персональних даних (7 год.)

1. Аналіз Закону України «Про захист персональних даних» (2 год.).
2. Підготовка аналітичної записки про гармонізацію з GDPR (2 год.).
3. Дослідження судової практики щодо захисту даних (2 год.).
4. Складання переліку механізмів захисту даних (1 год.).

Тема 5. Правове регулювання кіберзлочинності (7 год.)

1. Аналіз статей Кримінального кодексу України (361–363) (2 год.).
2. Підготовка доповіді про міжнародне співробітництво у боротьбі з кіберзлочинністю (2 год.).
3. Дослідження практики розслідування кіберзлочинів (2 год.).
4. Складання схеми правового регулювання кіберзлочинності (1 год.).

Тема 6. Захист критичної інфраструктури (6 год.)

1. Аналіз Закону України «Про критичну інфраструктуру і її захист» (2 год.).
2. Підготовка есе «Кібератаки на критичну інфраструктуру» (2 год.).
3. Дослідження міжнародних стандартів захисту критичної інфраструктури (1 год.).
4. Складання переліку заходів захисту (1 год.).

Тема 7. Інформаційна безпека в умовах воєнного стану (6 год.)

1. Аналіз Закону України «Про правовий режим воєнного стану» (2 год.).
2. Підготовка доповіді «Реагування на кібератаки в умовах війни» (2 год.).
3. Дослідження кібератак в умовах воєнного стану (1 год.).
4. Складання переліку правових заходів захисту інформації (1 год.).

Тема 8. Правові аспекти кібероперацій (6 год.)

1. Аналіз Талліннського посібника 2.0 (2 год.).
2. Підготовка есе «Юрисдикція в кіберпросторі» (2 год.).
3. Дослідження міжнародного права щодо кібероперацій (1 год.).
4. Складання схеми відповідальності за кібероперації (1 год.).

Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці (6 год.)

1. Аналіз Рекомендації ЮНЕСКО з етики ШІ (2 год.).
2. Підготовка есе «Етичні виклики ШІ в кібербезпеці» (2 год.).
3. Дослідження EU AI Act (1 год.).

4. Складання переліку етичних принципів ШІ (1 год.).

Тема 10. Відповідальність за порушення у сфері інформаційної безпеки (6 год.)

1. Аналіз видів відповідальності за кіберзлочини (2 год.).
2. Підготовка доповіді про доказування кіберзлочинів (2 год.).
3. Дослідження практики притягнення до відповідальності (1 год.).
4. Складання таблиці видів відповідальності (1 год.).

8. Індивідуальні завдання

Загальна кількість годин на індивідуальні завдання: 16 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 модуля 1 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 модуля 1 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:

1. **Реферат** (4 год.): написання реферату на одну з тем дисципліни (наприклад, «Гармонізація українського законодавства з GDPR», «Етичні виклики ШІ в кібербезпеці»).
2. **Есе** (4 год.): підготовка есе на тему, наприклад, «Юрисдикція в кіберпросторі» або «Кібератаки на критичну інфраструктуру».
3. **Кейсові завдання** (4 год.): аналіз реальних або гіпотетичних кейсів кіберінцидентів з підготовкою правового висновку.

Індивідуальні завдання з дисципліни

Тема 1. Поняття та принципи інформаційної безпеки

- **Завдання**: Провести порівняльний аналіз принципів інформаційної безпеки (конфіденційність, цілісність, доступність) на основі Закону України «Про кібербезпеку» (2017) та стандарту ISO/IEC 27001:2022. Підготувати есе (500–700 слів) про актуальні проблеми гармонізації українського законодавства з міжнародними стандартами.
- **Мета**: Поглибити розуміння принципів інформаційної безпеки та виявити правові прогалини.
- **Джерела**: Закон України «Про кібербезпеку» (URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text), ISO/IEC 27001:2022 (URL: https://www.iso.org/standard/27001), Кліщенко В.О. (2023), Погребняк С.П. (2022).
- **Час виконання**: 2 години (з урахуванням важливості вступної теми).

Тема 2. Національне законодавство у сфері кібербезпеки

- **Завдання**: Проаналізувати структуру та функції державних органів України (СБУ, Держспецзв'язку) у сфері кібербезпеки на основі Закону України «Про основи національної безпеки» (2018). Підготувати звіт (400–500 слів) про проблеми координації між цими органами, запропонувавши 2–3 рекомендації щодо їх вирішення.

- **Мета**: Розвинути навички аналізу законодавства та оцінки ефективності державних механізмів.
- **Джерела**: Закон України «Про основи національної безпеки» (URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text), Совгиря О.В. (2022), Білак М. (2021).
- **Час виконання**: 1 година.

Тема 3. Міжнародні стандарти інформаційної безпеки

- **Завдання**: Підготувати презентацію (5–7 слайдів) про ключові положення Будапештської конвенції про кіберзлочинність (2001) та її імплементацію в Україні. Включити аналіз однієї актуальної проблеми (наприклад, адаптація до нових кіберзагроз) і запропонувати рішення.
- **Мета**: Ознайомитися з міжнародними стандартами та оцінити їх застосування в Україні.
- **Джерела**: Конвенція Ради Європи про кіберзлочинність (URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185), ENISA (2022), Кліщенко В.О. (2021).
- **Час виконання**: 1 година.

Тема 4. Правові аспекти захисту персональних даних

- **Завдання**: Скласти порівняльну таблицю основних вимог Закону України «Про захист персональних даних» (2010) та GDPR (2016). Написати короткий коментар (300–400 слів) про проблеми гармонізації українського законодавства з GDPR.
- **Мета**: Порівняти національне та європейське законодавство, виявити прогалини.
- **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), Совгиря О.В. (2022).
- **Час виконання**: 1 година.

Тема 5. Правове регулювання кіберзлочинності

- **Завдання**: Проаналізувати статті 361–363 Кримінального кодексу України щодо кіберзлочинів. Підготувати кейс-стаді (400–500 слів) на основі реального прикладу кіберзлочину, оцінивши ефективність розслідування та проблеми юрисдикції.
- **Мета**: Розвинути навички аналізу кримінального законодавства та практики його застосування.
- **Джерела**: Кримінальний кодекс України (URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text), Кравець І.М. (2021), UNODC (2021).
- **Час виконання**: 1 година.

Тема 6. Захист критичної інфраструктури

- **Завдання**: На основі Закону України «Про критичну інфраструктуру і її захист» (2021) розробити схему заходів захисту об’єкта критичної інфраструктури від кібератак. Написати пояснювальну записку (300–400 слів) про координацію між секторами.
- **Мета**: Ознайомитися з механізмами захисту критичної інфраструктури та їх практичним застосуванням.
- **Джерела**: Закон України «Про критичну інфраструктуру і її захист» (URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text), ENISA (2022), Хоменко В.М. (2022).
- **Час виконання**: 1 година.

Тема 7. Інформаційна безпека в умовах воєнного стану

- **Завдання**: Проаналізувати Закон України «Про правовий режим воєнного стану» (2015) і підготувати звіт (500–700 слів) про правові аспекти захисту інформації в умовах війни. Включити приклад кібератаки та запропонувати заходи реагування.
- **Мета**: Поглибити розуміння кібербезпеки в екстремальних умовах та розробити практичні рекомендації.
- **Джерела**: Закон України «Про правовий режим воєнного стану» (URL: https://zakon.rada.gov.ua/laws/show/389-19#Text), NATO (2022), Погребняк С.П. (2022).
- **Час виконання**: 2 години (з урахуванням важливості теми).

Тема 8. Правові аспекти кібероперацій

- **Завдання**: На основі Талліннського посібника 2.0 (2017) підготувати аналітичну записку (400–500 слів) про відповідальність за кібероперації в міжнародному праві. Обговорити проблему юрисдикції в кіберпросторі.
- **Мета**: Ознайомитися з міжнародним правом кібероперацій та його викликами.
- **Джерела**: Талліннський посібник 2.0 (URL: https://ccdcoe.org/research/tallinn-manual/), Кліщенко В.О. (2022), Білак М. (2022).
- **Час виконання**: 1 година.

Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці

- **Завдання**: Проаналізувати Рекомендацію ЮНЕСКО з етики штучного інтелекту (2021) та EU AI Act (2021). Підготувати есе (400–500 слів) про етичні виклики використання ШІ в кібербезпеці та запропонувати 2–3 правові заходи для їх вирішення.
- **Мета**: Розвинути розуміння етичних і правових аспектів ШІ в кібербезпеці.
- **Джерела**: Рекомендація ЮНЕСКО (URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137), EU AI Act (URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206), Совгиря О.В. (2022).
- **Час виконання**: 1 година.

Тема 10. Відповідальність за порушення у сфері інформаційної безпеки

- **Завдання**: На основі Кримінального кодексу України (статті 361–363) та Кодексу України про адміністративні правопорушення скласти порівняльну таблицю видів відповідальності за кіберзлочини. Написати коментар (300–400 слів) про проблеми доказування кіберзлочинів.
- **Мета**: Поглибити знання про види відповідальності та виклики правозастосування.
- **Джерела**: Кримінальний кодекс України (URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text), Кодекс України про адміністративні правопорушення (URL: https://zakon.rada.gov.ua/laws/show/8073-10#Text), Кравець І.М. (2022).
- **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 інформаційної безпеки

1. Що таке інформаційна безпека? Охарактеризуйте її основні принципи (конфіденційність, цілісність, доступність).
2. Які ключові положення Закону України «Про кібербезпеку» (2017) регулюють інформаційну безпеку?
3. Які правові прогалини існують у гармонізації українського законодавства з міжнародними стандартами інформаційної безпеки?
4. Порівняйте принципи інформаційної безпеки за Законом України «Про кібербезпеку» та ISO/IEC 27001:2022.
5. Як можна вирішити проблему недостатньої гармонізації українського законодавства з міжнародними стандартами? Наведіть 2–3 пропозиції.

Тема 2. Національне законодавство у сфері кібербезпеки

6. Які функції виконують СБУ та Держспецзв'язку у сфері кібербезпеки згідно із Законом України «Про основи національної безпеки» (2018)?
7. Охарактеризуйте структуру державних органів України, відповідальних за кібербезпеку.
8. Які проблеми координації між державними органами у сфері кібербезпеки в Україні є найбільш актуальними?
9. Як Закон України «Про основи національної безпеки» (2018) сприяє забезпеченню кібербезпеки?
10. Запропонуйте 2–3 заходи для покращення імплементації законодавства у сфері кібербезпеки в Україні.

Тема 3. Міжнародні стандарти інформаційної безпеки

11. Які ключові положення Будапештської конвенції про кіберзлочинність (2001)?
12. Опишіть основні вимоги стандарту ISO/IEC 27001:2022 до системи управління інформаційною безпекою.
13. Яку роль відіграють ENISA та ITU у формуванні міжнародних стандартів кібербезпеки?

14. Які проблеми виникають під час імплементації міжнародних стандартів інформаційної безпеки в Україні?
15. Проаналізуйте, як NIST Cybersecurity Framework може бути адаптований до українського законодавства.

Тема 4. Правові аспекти захисту персональних даних

16. Які основні вимоги Закону України «Про захист персональних даних» (2010) до обробки персональних даних?
17. Порівняйте ключові положення Закону України «Про захист персональних даних» та GDPR (2016).
18. Які проблеми гармонізації українського законодавства з GDPR є найбільш актуальними?
19. Як хмарні технології впливають на захист персональних даних в Україні? Назвіть 2–3 виклики.
20. Запропонуйте правові заходи для забезпечення захисту персональних даних у воєнний період.

Тема 5. Правове регулювання кіберзлочинності

21. Які види кіберзлочинів регулюються статтями 361–363 Кримінального кодексу України?
22. Опишіть механізми розслідування кіберзлочинів в Україні. Які труднощі виникають?
23. Яку роль відіграє міжнародне співробітництво у боротьбі з кіберзлочинністю?
24. Які проблеми юрисдикції виникають при розслідуванні кіберзлочинів? Наведіть приклад.
25. Проаналізуйте ефективність застосування Кримінального кодексу України у боротьбі з кіберзлочинністю.

Тема 6. Захист критичної інфраструктури

26. Що таке критична інфраструктура за Законом України «Про критичну інфраструктуру і її захист» (2021)?
27. Які основні заходи захисту критичної інфраструктури від кібератак передбачені в Україні?
28. Які міжнародні стандарти застосовуються для захисту критичної інфраструктури? Назвіть 2–3 приклади.
29. Охарактеризуйте проблеми координації між секторами при захисті критичної інфраструктури.
30. Запропонуйте 2–3 заходи для підвищення стійкості критичної інфраструктури до кібератак.

Тема 7. Інформаційна безпека в умовах воєнного стану

31. Які правові аспекти захисту інформації регулюються Законом України «Про правовий режим воєнного стану» (2015)?
32. Як кібератаки впливають на інформаційну безпеку в умовах воєнного стану? Наведіть приклад.
33. Які обмеження на доступ до інформації можуть застосовуватися в умовах воєнного стану?
34. Проаналізуйте роль державних органів у забезпеченні кібербезпеки під час війни.
35. Запропонуйте 2–3 заходи реагування на кібератаки в умовах воєнного стану.

Тема 8. Правові аспекти кібероперацій

36. Що таке кібероперації за Талліннським посібником 2.0 (2017)?
37. Як міжнародне право регулює відповідальність за кібероперації?
38. Які проблеми юрисдикції виникають у кіберпросторі під час кібероперацій?

39. Опишіть роль Талліннського посібника 2.0 у формуванні правового регулювання кібероперацій.
40. Запропонуйте правові механізми для врегулювання відповідальності за кібероперації.

Тема 9. Правові аспекти використання штучного інтелекту в кібербезпеці

41. Які етичні принципи використання штучного інтелекту в кібербезпеці визначено Рекомендацією ЮНЕСКО (2021)?
42. Опишіть ключові положення EU AI Act (2021) щодо використання ШІ в кібербезпеці.
43. Які етичні виклики виникають при використанні ШІ в кібербезпеці? Наведіть 2–3 приклади.
44. Як відсутність правового регулювання ШІ впливає на кібербезпеку в Україні?
45. Запропонуйте 2–3 правові заходи для регулювання використання ШІ в кібербезпеці.

Тема 10. Відповідальність за порушення у сфері інформаційної безпеки

46. Які види відповідальності (адміністративна, кримінальна, цивільна) передбачені за порушення інформаційної безпеки в Україні?
47. Проаналізуйте статті 361–363 Кримінального кодексу України щодо відповідальності за кіберзлочини.
48. Які проблеми доказування кіберзлочинів є найбільш актуальними в Україні?
49. Як міжнародна відповідальність за кіберзлочини регулюється на глобальному рівні?
50. Запропонуйте 2–3 заходи для підвищення ефективності притягнення до відповідальності за кіберзлочини.

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

1. Кліщенко В.О. Нормативно-правове забезпечення кібербезпеки. Київ: Юрінком Інтер, 2023. – С. 10–30.
2. Совгиря О.В. Правові основи інформаційної безпеки. Київ: Ваіте, 2022. – С. 15–40.
3. Закон України «Про кібербезпеку» від 05.10.2017 № 2163-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
4. Погребняк С.П. Принципи інформаційної безпеки. Журнал східноєвропейського права. – 2022. – № 95. – С. 12–22. URL: https://doi.org/10.5281/zenodo.4701234
5. Хоменко В.М. Законодавство України у сфері кібербезпеки. Право України. – 2022. – № 11. – С. 20–35.
6. Білак М. Нормативно-правова база кібербезпеки. Юридичний вісник. – 2021. – № 7. – С. 10–20.
7. ENISA. EU Cybersecurity Legislation Overview. 2022. – С. 5–15. URL: https://www.enisa.europa.eu/publications
8. ISO/IEC 27001:2022. Information Security Management Systems. – С. 1–10. URL: https://www.iso.org/standard/27001
9. NIST. Cybersecurity Framework. 2021. – С. 10–20. URL: https://www.nist.gov/cyberframework
10. Кравець І.М. Основи інформаційної безпеки: правовий аспект. Право України. – 2021. – № 10. – С. 15–25.
11. Закон України «Про основи національної безпеки» від 19.06.2018 № 2469-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
12. Кліщенко В.О. Національні механізми кібербезпеки. Київ: Юрінком Інтер, 2023. – С. 50–70.
13. Совгиря О.В. Державні органи у сфері кібербезпеки. Київ: Ваіте, 2022. – С. 40–60.
14. Погребняк С.П. Імплементація законодавства у сфері кібербезпеки. Вісник НАПрН України. – 2022. – № 6. – С. 12–22.
15. Хоменко В.М. Роль Держспецзв’язку у кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 100–110.
16. Білак М. Координація державних органів у кібербезпеці. Юридичний вісник. – 2021. – № 8. – С. 10–20.
17. ENISA. National Cybersecurity Strategies. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
18. Council of Europe. Cybersecurity Governance Report. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications
19. NIST. Guidelines on Cybersecurity Governance. 2021. – С. 15–25. URL: https://www.nist.gov/cyberframework

20. Кравець І.М. Правові аспекти кібербезпеки в Україні. Журнал східноєвропейського права. – 2021. – № 96. – С. 10–20. URL: https://doi.org/10.5281/zenodo.4712345
21. Council of Europe. Budapest Convention on Cybercrime (оновлення 2023). URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
22. Совгиря О.В. Міжнародні стандарти кібербезпеки. Київ: Ваіте, 2022. – С. 60–80.
23. Кліщенко В.О. Конвенція про кіберзлочинність. Право України. – 2021. – № 8. – С. 20–35.
24. Білак М. Імплементація стандартів ISO/IEC 27001. Юридичний вісник. – 2021. – № 9. – С. 10–20.
25. Погребняк С.П. Роль ENISA у кібербезпеці. Вісник НАПрН України. – 2022. – № 7. – С. 15–25.
26. Хоменко В.М. Міжнародні стандарти інформаційної безпеки. Актуальні проблеми державотворення. – 2022. – С. 110–120.
27. ENISA. Cybersecurity Standards Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
28. ITU. Global Cybersecurity Index. 2021. – С. 5–15. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
29. Кравець І.М. Міжнародне співробітництво у сфері кібербезпеки. Право України. – 2021. – № 11. – С. 20–30.
30. NIST. International Cybersecurity Standards. 2021. – С. 10–20. URL: https://www.nist.gov/cyberframework
31. 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
32. General Data Protection Regulation (GDPR) (оновлення 2023). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
33. Совгиря О.В. GDPR та Україна. Київ: Ваіте, 2022. – С. 80–100.
34. Кравець І.М. Захист персональних даних: правові аспекти. Право України. – 2021. – № 9. – С. 15–25.
35. Білак М. Гармонізація з GDPR. Юридичний вісник. – 2021. – № 10. – С. 10–20.
36. Погребняк С.П. Захист даних у воєнний період. Вісник НАПрН України. – 2022. – № 8. – С. 15–25.
37. Хоменко В.М. Судова практика у сфері захисту даних. Актуальні проблеми державотворення. – 2022. – С. 120–130.
38. Council of Europe. Convention 108+ (оновлення 2022). – С. 5–15. URL: https://www.coe.int/en/web/data-protection/convention108+
39. ENISA. Data Protection Guide. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
40. Кліщенко В.О. Захист даних у кіберпросторі. Київ: Юрінком Інтер, 2023. – С. 90–110.
41. Кримінальний кодекс України від 05.04.2001 № 2341-III (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text
42. Совгиря О.В. Кіберзлочинність: правові аспекти. Київ: Ваіте, 2022. – С. 100–120.
43. Кравець І.М. Розслідування кіберзлочинів. Журнал східноєвропейського права. – 2021. – № 97. – С. 10–20. URL: https://doi.org/10.5281/zenodo.4712346
44. Білак М. Міжнародне співробітництво у боротьбі з кіберзлочинністю. Юридичний вісник. – 2021. – № 11. – С. 15–25.
45. Погребняк С.П. Проблеми розслідування кіберзлочинів. Вісник НАПрН України. – 2022. – № 9. – С. 12–22.
46. Хоменко В.М. Правове регулювання кіберзлочинності. Актуальні проблеми державотворення. – 2022. – С. 130–140.
47. UNODC. Comprehensive Study on Cybercrime. 2021. – С. 20–30. URL: https://www.unodc.org/documents/organized-crime/cybercrime/UNODC_Study_on_Cybercrime.pdf
48. ENISA. Cybercrime Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications

49. Кліщенко В.О. Механізми протидії кіберзлочинності. Київ: Юрінком Інтер, 2023. – С. 120–140.
50. Interpol. Global Cybercrime Report. 2022. – С. 5–15. URL: https://www.interpol.int/en/Crimes/Cybercrime
51. Закон України «Про критичну інфраструктуру і її захист» від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
52. Совгиря О.В. Кібербезпека критичної інфраструктури. Київ: Ваіте, 2022. – С. 120–140.
53. Кравець І.М. Захист критичної інфраструктури. Право України. – 2022. – № 10. – С. 15–25.
54. Білак М. Кібератаки на критичну інфраструктуру. Юридичний вісник. – 2022. – № 11. – С. 10–20.
55. Погребняк С.П. Міжнародні стандарти захисту критичної інфраструктури. Вісник НАПрН України. – 2022. – № 10. – С. 15–25.
56. Хоменко В.М. Координація захисту критичної інфраструктури. Актуальні проблеми державотворення. – 2022. – С. 140–150.
57. ENISA. Critical Infrastructure Protection Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
58. NATO. Critical Infrastructure Protection Guidelines. 2022. – С. 5–15. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm
59. Council of Europe. Report on Critical Infrastructure and Cybersecurity. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications
60. Кліщенко В.О. Захист критичної інфраструктури від кіберзагроз. Київ: Юрінком Інтер, 2023. – С. 150–170.
61. Закон України «Про правовий режим воєнного стану» від 12.05.2015 № 389-VIII (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/389-19#Text
62. Совгиря О.В. Кібербезпека в умовах війни. Київ: Ваіте, 2022. – С. 140–160.
63. Кравець І.М. Інформаційна безпека в умовах воєнного стану. Право України. – 2022. – № 12. – С. 15–25.
64. Білак М. Захист інформації в умовах війни. Юридичний вісник. – 2022. – № 12. – С. 10–20.
65. Погребняк С.П. Кібератаки в умовах війни. Вісник НАПрН України. – 2022. – № 11. – С. 15–25.
66. Хоменко В.М. Правові аспекти захисту інформації в умовах війни. Актуальні проблеми державотворення. – 2022. – С. 150–160.
67. NATO. Cybersecurity in Wartime. 2022. – С. 5–15. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm
68. ENISA. Cybersecurity in Armed Conflicts. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
69. Council of Europe. Report on Cybersecurity in Armed Conflicts. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications
70. Кліщенко В.О. Кібербезпека в умовах воєнного стану. Київ: Юрінком Інтер, 2023. – С. 170–190.
71. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (оновлення 2023). URL: https://ccdcoe.org/research/tallinn-manual/
72. Совгиря О.В. Правове регулювання кібероперацій. Київ: Ваіте, 2022. – С. 160–180.
73. Кліщенко В.О. Кібероперації та міжнародне право. Юридичний науковий електронний журнал. – 2022. – № 5. – С. 40–50. URL: https://doi.org/10.32782/2524-0374/2022-5/40
74. Білак М. Відповідальність за кібероперації. Юридичний вісник. – 2022. – № 13. – С. 15–25.
75. Погребняк С.П. Юрисдикція в кіберпросторі. Вісник НАПрН України. – 2022. – № 12. – С. 12–22.
76. Хоменко В.М. Кібервійни та міжнародне право. Актуальні проблеми державотворення. – 2022. – С. 160–170.
77. UN Group of Governmental Experts Report on Cyberspace. 2021. – С. 10–20. URL: https://www.un.org/disarmament/group-of-governmental-experts/

78. Council of Europe. Report on Cyber Operations. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications
79. ENISA. Cyber Operations Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
80. Кравець І.М. Міжнародне право та кібероперації. Право України. – 2021. – № 12. – С. 20–30.
81. Рекомендація ЮНЕСКО з етики штучного інтелекту. 2021. – С. 5–15. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137
82. European Commission. AI Act Proposal. 2021. – С. 10–20. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
83. Совгиря О.В. Правове регулювання ШІ. Київ: Ваіте, 2022. – С. 180–200.
84. Кліщенко В.О. Штучний інтелект у кібербезпеці. Юридичний науковий електронний журнал. – 2022. – № 6. – С. 40–50. URL: https://doi.org/10.32782/2524-0374/2022-6/40
85. Білак М. Етичні аспекти ШІ в кібербезпеці. Юридичний вісник. – 2022. – № 14. – С. 15–25.
86. Погребняк С.П. Правові виклики ШІ. Вісник НАПрН України. – 2022. – № 13. – С. 12–22.
87. Хоменко В.М. Регулювання ШІ в кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 170–180.
88. Council of Europe. Report on Artificial Intelligence and Cybersecurity. 2022. – С. 8–18. URL: https://www.coe.int/en/web/cdcj/publications
89. ENISA. AI and Cybersecurity Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
90. Кравець І.М. Етика ШІ в кібербезпеці. Право України. – 2021. – № 13. – С. 20–30.
91. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X (редакція 2023). URL: https://zakon.rada.gov.ua/laws/show/8073-10#Text
92. Совгиря О.В. Правова відповідальність у кібербезпеці. Київ: Ваіте, 2022. – С. 200–220.
93. Кравець І.М. Відповідальність за кіберзлочини. Право України. – 2022. – № 11. – С. 15–25.
94. Білак М. Доказування кіберзлочинів. Юридичний вісник. – 2022. – № 15. – С. 10–20.
95. Погребняк С.П. Міжнародна відповідальність за кіберзлочини. Вісник НАПрН України. – 2022. – № 14. – С. 12–22.
96. Хоменко В.М. Правові аспекти відповідальності у кібербезпеці. Актуальні проблеми державотворення. – 2022. – С. 180–190.
97. UNODC. Global Report on Cybercrime Trends. 2022. – С. 10–20. URL: https://www.unodc.org/documents/organized-crime/cybercrime/Global_Report_2022.pdf
98. ENISA. Cybercrime Liability Report. 2022. – С. 10–20. URL: https://www.enisa.europa.eu/publications
99. Кліщенко В.О. Відповідальність за порушення кібербезпеки. Київ: Юрінком Інтер, 2023. – С. 190–210.
100. NIST. Cybercrime Accountability Guidelines. 2021. – С. 10–20. URL: https://www.nist.gov/cyberframework

Електронні ресурси:

1. **Офіційний вебпортал Верховної Ради України** – База нормативно-правових актів України, включаючи закони про кібербезпеку, захист персональних даних та критичну інфраструктуру. URL: https://zakon.rada.gov.ua/laws
2. **ENISA (European Union Agency for Cybersecurity)** – Звіти, гайди та рекомендації з кібербезпеки, захисту даних і критичної інфраструктури. URL: https://www.enisa.europa.eu/publications
3. **ISO (International Organization for Standardization)** – Стандарти інформаційної безпеки, зокрема ISO/IEC 27001:2022. URL: https://www.iso.org/standard/27001

4. **NIST (National Institute of Standards and Technology)** – Ресурси з кібербезпеки, включаючи Cybersecurity Framework та рекомендації. URL: https://www.nist.gov/cyberframework
5. **Council of Europe** – Документи з кіберзлочинності, захисту даних і кібероперацій, включаючи Будапештську конвенцію та Convention 108+. URL: https://www.coe.int/en/web/cdcj/publications
6. **UNODC (United Nations Office on Drugs and Crime)** – Звіти та дослідження з кіберзлочинності. URL: https://www.unodc.org/documents/organized-crime/cybercrime
7. **Interpol** – Ресурси з міжнародної боротьби з кіберзлочинністю. URL: https://www.interpol.int/en/Crimes/Cybercrime
8. **NATO** – Матеріали з кібербезпеки, захисту критичної інфраструктури та кібероперацій у воєнний час. URL: https://www.nato.int/cps/en/natohq/topics_78132.htm
9. **ITU (International Telecommunication Union)** – Глобальний індекс кібербезпеки та рекомендації з міжнародних стандартів. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
10. **European Commission** – Документи з GDPR та EU AI Act. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
11. **UNESCO** – Рекомендації з етики штучного інтелекту. URL: https://unesdoc.unesco.org/ark:/48223/pf0000381137
12. **CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence)** – Талліннський посібник 2.0 та інші ресурси з кібероперацій. URL: https://ccdcoe.org/research/tallinn-manual/
13. **UN (United Nations)** – Звіти Групи урядових експертів з питань кіберпростору. URL: https://www.un.org/disarmament/group-of-governmental-experts/
14. **Держспецзв'язку (Державна служба спеціального зв'язку та захисту інформації України)** – Інформація про кібербезпеку, захист критичної інфраструктури та національні стандарти. URL: https://cip.gov.ua
15. **Cybersecurity and Infrastructure Security Agency (CISA)** – Рекомендації з захисту критичної інфраструктури та кібербезпеки. URL: https://www.cisa.gov/topics/cybersecurity
16. **Global Forum on Cyber Expertise (GFCE)** – Ресурси з міжнародного співробітництва у сфері кібербезпеки. URL: https://www.thegfce.org/publications
17. **World Economic Forum (WEF)** – Звіти про кібербезпеку та штучний інтелект. URL: https://www.weforum.org/reports
18. **Oxford Cyber Security Research Centre** – Наукові статті та звіти з кібербезпеки та кіберзлочинності. URL: https://www.cs.ox.ac.uk/research/cybersecurity
19. **Journal of Eastern-European Law** – Електронний журнал із статтями про кібербезпеку та правові аспекти. URL: https://eelaw.knu.ua/index.php/journal
20. **Legal Scientific Electronic Journal** – Статті з правового регулювання кібербезпеки та ШІ. URL: https://lsej.org.ua

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	Нормативно-правове забезпечення інформаційної безпеки
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 он-лайн 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 _____