

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО

на засіданні кафедри
кібербезпеки та
інформаційних технологій
Протокол № 4 від 27.11.2025 р.

ПОГОДЖЕНО

Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО



СТРАТЕГІЯ КІБЕРСТАНДАРТИЗАЦІЇ ЄС ДЛЯ ЕФЕКТИВНОГО
ПОЄДНАННЯ ТА ЦИФРОВОЇ ІНФРАСТРУКТУРИ: ДОСВІД ДЛЯ
УКРАЇНИ

робоча програма навчальної дисципліни (РПНД)

Галузь знань	всі
Спеціальність	всі
Освітній рівень	другий (магістерський)
Освітня програма	всі
Статус дисципліни	вибіркова
Мова викладання, навчання та оцінювання	українська

Розробники:
к.е.н., проф.

Підписано КЕП

Ірина ЗОЛОТАРЬОВА

д.т.н., проф.

Ольга СТАРКОВА

д.т.н., проф.

Підписано КЕП

Сергій СЕМЕНОВ

к.т.н., доц.

Вячеслав ЛИМАРЕНКО

Завідувач кафедри
кібербезпеки та
інформаційних технологій

Ольга СТАРКОВА

Харків 2025

ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій та цифрових екосистем роль кібербезпеки та стандартизації набуває особливого значення для забезпечення стабільного функціонування державних та приватних цифрових інфраструктур. Особливо це актуально у контексті євроінтеграції України, де впровадження стандартів та практик Європейського Союзу (ЄС) сприяє підвищенню рівня кіберзахисту, ефективності управління цифровими процесами та інтеграції українських ІТ-бізнесів у міжнародні цифрові ринки.

Дисципліна «Стратегія кіберстандартизації ЄС для ефективного поєднання та цифрової інфраструктури: досвід для України» (розроблена в рамках міжнародного проєкту 101176904 – EU-cyberconnect-UA – ERASMUS-JMO-2024-MODULE) має практичну спрямованість і орієнтований на формування у здобувачів комплексних компетентностей у сфері кібербезпеки, цифрових технологій та стандартів штучного інтелекту. Він поєднує теоретичні знання з практичними навичками, необхідними для побудови стійкої, безпечної та ефективної цифрової інфраструктури в Україні, орієнтованої на європейські стандарти.

Мета дисципліни полягає у зміцненні професійного та академічного досвіду здобувачів у таких напрямках: розвиток глибоких знань про стандарти кібербезпеки та етичні принципи використання штучного інтелекту (ШІ) у відповідності до європейських нормативів; набуття практичних навичок у впровадженні цифрових рішень та стандартів, що забезпечують ефективне партнерство між Україною та ЄС; аналіз та застосування кращих європейських практик у сфері цифрової трансформації, цифрової економіки та екологічно орієнтованої цифрової інфраструктури.

Завдання дисципліни:

- ознайомити здобувачів із основними стандартами ЄС у сфері кібербезпеки та цифрової інфраструктури;

- розвинути практичні навички застосування європейських стандартів та етичних принципів штучного інтелекту у цифрових системах;

- проаналізувати досвід ЄС щодо цифрової трансформації та адаптувати його до умов України;

- підготувати здобувачів до управління проєктами у сфері цифрових технологій з дотриманням міжнародних стандартів безпеки.

Об'єкт дослідження – цифрові інфраструктури та стандарти кібербезпеки, що застосовуються у Європейському Союзі та їх вплив на розвиток українського ІТ-бізнесу та цифрової економіки.

Предмет дослідження – процеси запровадження та адаптації стандартів ЄС у сфері кібербезпеки, цифрових технологій та етичних принципів штучного інтелекту для забезпечення ефективності та безпеки цифрових послуг в Україні.

Дисципліна також спрямована на підготовку фахівців здатних не лише забезпечувати безпеку та ефективність цифрових систем, але й здійснювати

управління проектами та інноваційними процесами у відповідності до міжнародних стандартів. Він формує у здобувачів критичне мислення та аналітичні здібності для оцінки ризиків, прийняття рішень та впровадження стратегій цифрової трансформації у національному та міжнародному контексті.

В результаті освоєння дисципліни здобувачі здобудуть міцну теоретичну та практичну основу для розвитку української цифрової інфраструктури, покращення ІТ-бізнесу, академічної діяльності та участі у проектах європейської інтеграції, що сприятиме посиленню конкурентоспроможності України у глобальному цифровому просторі.

Результати навчання та компетентності, які формує навчальна дисципліна, визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	Компетентності, якими повинен оволодіти здобувач вищої освіти
Проектувати політики інформаційної безпеки для організацій, враховуючи вимоги NIS2, GDPR, AI Act, етичні стандарти та рекомендації щодо критичної інфраструктури	Здатність розробляти та впроваджувати політики безпеки цифрової інфраструктури відповідно до стандартів ЄС
Застосовувати сучасні методології управління ризиками, аналізувати залежності у цифрових екосистемах та формувати стратегії мінімізації ризиків для бізнесу та державного сектору	Здатність проводити комплексну оцінку ризиків цифрових екосистем і пропонувати оптимальні стратегії захисту
Критично оцінювати технології ШІ, аналізувати ризики їх застосування й інтегрувати етичні принципи ЄС у проекти цифрової трансформації	Здатність інтегрувати етичні принципи, штучний інтелект та європейські стандарти у процеси цифрової трансформації
Проектувати та впроваджувати безпечні цифрові продукти відповідно до DevSecOps, Secure by Design та інших інженерних практик ЄС	Здатність застосовувати принципи захищеної розробки для створення складних цифрових сервісів

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Зміст навчальної дисципліни

Змістовий модуль 1. Кібербезпека та стандарти Європейського Союзу.

Тема 1. Стандартизація та кібербезпека для критичної інфраструктури: EU Toolbox.

1.1. Поняття та класифікація критичної інфраструктури (КІ).

1.2. Загрози та виклики для КІ в контексті кібербезпеки.

- 1.3. Підходи ЄС до захисту критичної інфраструктури.
- 1.4. EU Cybersecurity Toolbox: структура та призначення.
- 1.5. EU Toolbox для 5G та цифрових мереж.
- 1.6. Стандартизація кібербезпеки в Європейському Союзі.
- 1.7. Європейська модель кіберстійкості.
- 1.8. Співпраця між державами-членами ЄС.
- 1.9. Український контекст: адаптація до вимог ЄС.

Тема 2. Стандартизація та підключення для критичної інфраструктури: Цифрова економіка – європейський та український досвід. Вплив на розвиток бізнесу в країнах Європи та Україні.

2.1. Стандартизація та нормативні вимоги до критичної інфраструктури (КІ).

2.2. Цифрова економіка Європи.

2.3. Український досвід цифрової трансформації

2.4. Вплив цифрової інфраструктури на бізнес. Виклики та бар'єри.

Тема 3. Стратегія та стандарти ЄС для цифрової інфраструктури та GreenTech.

3.1. Європейські політики у сфері цифрової інфраструктури.

3.2. GreenTech як складова цифрового переходу.

3.3. Стандарти та технічні вимоги.

3.4. Інновації GreenTech.

3.5. Вплив на українську цифрову сферу.

Тема 4. Політика ЄС та регулювання ШІ.

4.1. Підходи ЄС до регулювання штучного інтелекту.

4.2. Інституції та органи нагляду.

4.3. Вимоги до прозорості та безпеки.

4.4. Вплив на бізнес.

4.5. Перспективи імплементації в Україні.

Змістовий модуль 2. Стійка цифрова інфраструктура Європейського Союзу.

Тема 5. Цифрова інфраструктура ЄС: етичні стандарти штучного інтелекту та європейські цінності.

5.1. Основи етики європейського цифрового суспільства.

5.2. Етичні вимоги до ШІ.

5.3. Документи ЄС з етики ШІ.

5.4. Роль цифрової інфраструктури у забезпеченні етики.

5.5. Практичні кейси.

Тема 6. Захищені принципи розробки для цифрових послуг.

6.1. Secure by Design / Privacy by Design.

6.2. Стандарти та найкращі практики.

6.3. Архітектурні вимоги.

6.4. Управління вразливостями.

6.5. Приклади застосування в Україні.

Тема 7. Впровадження Закону про штучний інтелект та етичні принципи розробки нових додатків у контексті цифрової трансформації українського бізнесу.

- 7.1. Європейська модель правового регулювання ШІ.
- 7.2. Український шлях до регулювання.
- 7.3. Етичні принципи для бізнесу.
- 7.4. Процес впровадження.
- 7.5. Виклики для українських компаній.

Тема 8. Технологічний суверенітет та інтелектуальна власність Європи.

- 8.1. Поняття технологічного суверенітету.
- 8.2. Європейська стратегія.
- 8.3. Інтелектуальна власність.
- 8.4. Вплив на інновації.
- 8.5. Український контекст.

Змістовий модуль 3. Ефективне поєднання та етика Європейського Союзу.

Тема 9. Цифрова освіта: досвід ЄС-UA.

- 9.1. Європейські освітні ініціативи.
- 9.2. Платформи та інструменти.
- 9.3. Український досвід.
- 9.4. Порівняння ЄС-UA.
- 9.5. Майбутні пріоритети.

Тема 10. Методології управління ризиками для стійких інфраструктур: вплив специфіки цифрових екосистем на прийняття рішень людиною.

- 10.1. Види ризиків.
- 10.2. Стандарти управління ризиками.
- 10.3. Прийняття рішень в умовах невизначеності.
- 10.4. Оцінка стійкості та безперервності.
- 10.5. Вплив цифрових екосистем на ризики.

Тема 11. Управління проєктами. Стандарти безпеки.

- 11.1. Основи управління проєктами.
- 11.2. Інтеграція безпеки в управління.
- 11.3. Стандарти безпеки.
- 11.4. Документація та аудит.
- 11.5. Приклади реалізації.

Тема 12. Безпека хмарної інфраструктури.

- 12.1. Види хмар та їх особливості.
- 12.2. Архітектурні загрози.
- 12.3. Стандарти та вимоги.
- 12.4. Інструменти хмарної безпеки.
- 12.5. Організаційні практики.

Перелік лабораторних занять / завдань за навчальною дисципліною наведено в табл. 2

Таблиця 2

Перелік лабораторних занять / завдань

Назва теми та / або завдання	Зміст
Тема 1. Лабораторна робота 1.	Оцінка кіберризиків для об'єкта критичної інфраструктури за методологією EU Toolbox (аналіз постачальників, технічних ризиків та рівнів загроз)
Тема 2. Лабораторна робота 2.	Порівняльний аналіз стандартів цифрової інфраструктури ЄС та України. Створення таблиці відповідності (mapping table) для NIS2 та українських нормативів
Тема 3. Лабораторна робота 3.	Аналіз екотехнологій (GreenTech) у цифрових системах: оцінка енергоефективності дата-центру або телекомунікаційної мережі за стандартами ЄС
Тема 4. Лабораторна робота 4.	Класифікація систем штучного інтелекту за категоріями ризику відповідно до AI Act на прикладі 5 реальних або уявних систем
Тема 5. Лабораторна робота 5.	Оцінка етичних ризиків ШІ: аналіз кейсу (розпізнавання обличч, оцінка кредитоспроможності, автоматизований відбір персоналу) за критеріями прозорості та недискримінації
Тема 6. Лабораторна робота 6.	Застосування принципів Secure by Design: створення моделі загроз (threat model) для вебдодатку з використанням STRIDE або аналогічної методики
Тема 7. Лабораторна робота 7.	Розробка етичної політики для компанії, що впроваджує ШІ (policy paper): правила використання даних, аудит моделей, відповідальність
Тема 8. Лабораторна робота 8.	Оцінка ризиків залежності від іноземних технологій: аналіз supply-chain у вибраному цифровому продукті (наприклад: хмарний сервіс, обладнання 5G, софт)
Тема 9. Лабораторна робота 9.	Створення цифрового освітнього модуля (mini-course) у Moodle або Google Classroom з дотриманням стандартів DigComp
Тема 10. Лабораторна робота 10.	Оцінка ризиків за методологією ISO 31000 або NIST RMF для обраної IT-системи (з побудовою матриці ризиків)
Тема 11. Лабораторна робота 11.	Створення плану проєкту з інтеграцією вимог інформаційної безпеки: матриця відповідальності (RACI), оцінка ризиків, план аудиту
Тема 12. Лабораторна робота 12.	Аналіз налаштувань хмарної інфраструктури (AWS/Azure/GCP або їх симулятор): виявлення помилок безпеки та формування рекомендацій

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3.

Перелік самостійної роботи

Назва теми та / або завдання	Зміст
Тема 1	Стандартизація та кібербезпека для критичної інфраструктури: EU Toolbox
Тема 2	Стандартизація та підключення для критичної інфраструктури: цифрова економіка – європейський та український досвід
Тема 3	Стратегія та стандарти ЄС для цифрової інфраструктури та GreenTech
Тема 4	Політика ЄС та регулювання штучного інтелекту
Тема 5	Цифрова інфраструктура ЄС: етичні стандарти штучного інтелекту та європейські цінності
Тема 6	Захищені принципи розробки для цифрових послуг
Тема 7	Впровадження Закону про штучний інтелект та етичні принципи розробки нових додатків у контексті цифрової трансформації українського бізнесу
Тема 8	Технологічний суверенітет та інтелектуальна власність Європи
Тема 9	Цифрова освіта: досвід ЄС-UA
Тема 10	Методології управління ризиками для стійких інфраструктур: вплив специфіки цифрових екосистем на прийняття рішень людиною
Тема 11	Управління проектами. Стандарти безпеки
Тема 12	Безпека хмарної інфраструктури

Кількість годин лекційних, лабораторних занять та годин самостійної роботи наведено в робочому плані (технологічній карті) з навчальної дисципліни.

МЕТОДИ НАВЧАННЯ

У процесі викладання навчальної дисципліни для набуття визначених результатів навчання, активізації освітнього процесу передбачено застосування таких методів навчання, як:

Словесні (лекція (Тема 1, 3), проблемна лекція (Тема 2, 4-12).

Наочні (демонстрація (Тема 1-12)).

Практичні (лабораторні роботи (Тема 1-12)).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100 бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, практичних, лабораторних та семінарських занять і має на меті перевірку рівня підготовленості здобувача вищої освіти до виконання конкретної роботи і оцінюється сумою набраних балів:

– для дисциплін з формою семестрового контролю залік: максимальна сума – 100 балів; мінімальна сума – 60 балів.

Семестровий контроль проводиться у формі заліку.

Підсумкова оцінка за навчальною дисципліною визначається:

– для дисциплін з формою семестрового контролю залік – сумуванням всіх балів, отриманих під час поточного контролю.

Під час викладання навчальної дисципліни використовуються наступні контрольні заходи:

Поточний контроль: лабораторні роботи (84 балів), письмові контрольні роботи (16 балів).

Семестровий контроль: залік (за сукупністю всіх балів, отриманих протягом семестру).

Більш детальну інформацію щодо системи оцінювання наведено в робочому плані (технологічній карті) навчальної дисципліни.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. European Union Agency for Cybersecurity (ENISA). Cybersecurity of AI and Standardisation. Luxembourg: Publications Office of the European Union, 2023.
2. European Union Agency for Cybersecurity (ENISA). NIS2 Technical Implementation Guidance (ENISA, 2025).
3. European Parliament and Council. Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Official Journal of the European Union, L 333, 27.12.2022.
4. European Union Agency for Cybersecurity (ENISA). A Multilayer Framework for Good Cybersecurity Practices for AI, June 2023.
5. Солодовник Г. В. Методи та системи штучного інтелекту : навчальний посібник. – Харків: ТОВ «ДІСА ПЛЮС», 2021. -177 с. <http://repository.hneu.edu.ua/handle/123456789/34052>
6. Природні та техногенні загрози: підручник / В. В. Тютюнник, О. М. Соболю, О. О. Тютюнник та ін. – Харків, 2023. – 484 с. <http://repository.hneu.edu.ua/handle/123456789/30918>

Додаткова

7. Лисеюк, А., Свінцицька, Т. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. *Право та інновації*, 2024, № 4 (48). [https://doi.org/10.37772/2518-1718-2024-4\(48\)-4](https://doi.org/10.37772/2518-1718-2024-4(48)-4).
8. Федієнко, О.П. Європейський досвід законодавчого забезпечення посилення кіберстійкості. *Інформація і право*, 2024, № 2 (49). [https://doi.org/10.37750/2616-6798.2024.2\(49\).306208](https://doi.org/10.37750/2616-6798.2024.2(49).306208).
9. Грищенко, С.М. Правове регулювання кібербезпеки в умовах цифрової трансформації суспільства. *Інформація і право*, 2025, № 3 (54). [https://doi.org/10.37750/2616-6798.2025.3\(54\).340519](https://doi.org/10.37750/2616-6798.2025.3(54).340519).
10. Василенко, В.М. Національна кібербезпека в умовах диджиталізації суспільства: роль поліції в захисті критичної інфраструктури. *Вісник*

Харківського національного університету внутрішніх справ, 2025, № 2 (109), С. 392–405. <https://doi.org/10.32631/v.2025.2.33>.

11. Вдовенко, С., Даник, Ю., Пермяков, О. Досвід розвитку систем кібербезпеки та кібероборони провідних країн світу. Сучасні інформаційні технології у сфері безпеки та оборони, 2020, № 37 (1), С. 31–48. <https://doi.org/10.33099/2311-7249/2020-37-1-31-48>.

12. Долгова Н. Г. Система підтримки рішень у завданнях проектування кібербезпеки критичної інфраструктури / Н. Г. Долгова, О. О. Шаповалова, Г. В. Солодовник // Кібербезпека: освіта, наука, техніка: електронне фахове наукове видання. – 2025. – №1(29). – С. 348-372. <https://repository.hneu.edu.ua/handle/123456789/37326>.

13. Голубничий Д.Ю. Процес декларування профілів безпеки інформації / О.В. Потій, Д.Ю. Голубничий, М.В. Єсіна та ін. // Радіотехніка. Всеукраїнський міжвідомчий науково-технічний збірник. – Харків, 2024. - № 217. - С. 7 – 22. <http://repository.hneu.edu.ua/handle/123456789/35001>.

14. Leroy I. Critical infrastructure defense: perspectives from the eu and usa cyber experts / I. Leroy, I. Zolotaryova // Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu. – 2023. – № 5. – Р. 165-170. <http://repository.hneu.edu.ua/handle/123456789/30222>.

15. Leroy I. Insights for Economic Security: Recovery Strategies from Cyber-Attacks / I. Leroy, I. Zolotaryova // The 13th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2023, Athens, Greece. – 2023. <http://repository.hneu.edu.ua/handle/123456789/33611>.

Інформаційні ресурси

16. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця навчальної дисципліни «Стратегія кіберстандартизації ЄС для ефективного поєднання та цифрової інфраструктури: досвід для України» <https://pns.hneu.edu.ua/enrol/index.php?id=12627>.