Міністерство освіти і науки України
Національний університет «Чернігівська політехніка»
Навчально-науковий інститут електронних та інформаційних технологій
Кафедра кібербезпеки та математичного моделювання

СИЛАБУС
Стандартизація, сертифікація засобів та комплексів захисту інформації

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Ткач Ю.М.
(підпис) (прізвище та ініціали)

«*26*» серпня 2024 р.

Розробник (-и): Ларченко М.О., доцент, кандидат юридичних наук, доцент _____
(прізвище та ініціали, посада, науковий ступінь і вчене звання) (підпис)

Силабус навчальної дисципліни обговорено на засіданні кафедри кібербезпеки та математичного моделювання

Протокол від «26» серпня 2024 р. № 7

Узгоджено з гарантом освітньої програми: _____ Петренко Т.А.
(підпис) (прізвище та ініціали)

---

1. Загальна інформація про дисципліну.

Тип дисципліни	*Обов'язкова*
Мова викладання	українська
Рік навчання та семестр	2024-2025 навчальний рік, І семестр, ОПП Кібербезпека за спеціальністю 125 Кібербезпека та захист інформації галузь знань 12 Інформаційні технології
Викладач (-і)	Ларченко Марина Олександрівна, доцент кафедри кібербезпеки та математичного моделювання, кандидат юридичних наук.
Профайл викладача (-ів)	https://mmi.stu.cn.ua/personal-kafedry/
Контакти викладача	Т.м. +38067 296 74 99, E-mail: urlinka2006@gmail.com

2. Анотація курсу.

Дисципліна **"Стандартизація, сертифікація засобів та комплексів захисту інформації"** є ключовою частиною програми підготовки магістрів ОП Кібербезпека за спеціальністю 125 Кібербезпека та захист інформації, галузь знань 12 Інформаційні технології. Курс закладає фундаментальні знання про нормативно-правові та технічні аспекти забезпечення інформаційної безпеки. Загальна тематика курсу охоплює: міжнародні та національні стандарти у сфері кібербезпеки (ISO/IEC 27000, NIST, ДСТУ тощо); процедури сертифікації засобів захисту інформації; оцінку відповідності систем безпеки та аналіз ризиків; механізми акредитації органів сертифікації та стандартизації; роль державних і міжнародних регуляторів у сфері інформаційної безпеки.

Підхід до викладання спрямований на глибоке розуміння теоретичних основ та їх практичне застосування. Особлива увага приділяється складним і прикладним аспектам сертифікації та стандартизації, що вимагає від студентів високого рівня аналітичних навичок. Викладання побудоване на аналізі реальних кейсів, вивченні актуальних міжнародних стандартів та обговоренні їх практичного використання в контексті сучасних кіберзагроз.

Курс орієнтований на підготовку спеціалістів, здатних критично оцінювати методи та засоби захисту інформації, брати участь у розробці, впровадженні та сертифікації систем безпеки відповідно до міжнародних стандартів.

3. Мета та цілі курсу.

Мета курсу – формування у студентів системного розуміння принципів стандартизації та сертифікації засобів і комплексів захисту інформації, а також розвиток навичок їх застосування для забезпечення інформаційної безпеки відповідно до міжнародних та національних вимог.

Цілі курсу:

КЗ 3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КЗ 5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

КФ 2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.

КФ 3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

КФ 4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.

КФ 10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

4. Результати навчання:

ПРН 2. Інтегрувати фундаментальні та спеціальні знання для розв’язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.

ПРН 6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.

ПРН 7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.

ПРН 20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.

5. Пререквізити. Дисципліна є складовою частиною Обов'язкових дисциплін циклу професійної підготовки. Вивчення курсу передбачає наявність систематичних та ґрунтовних знань.

6. Обсяг курсу:

Вид заняття	Загальна кількість годин денна/заочна
Лекції	16/6
Лабораторні заняття	16/6
Самостійна робота	88/108
Індивідуальне завдання – розрахунково-графічна робота	
Всього кредитів	4

Лекційні, лабораторні заняття, розрахунково-графічна робота, самостійна робота – з використанням системи дистанційного навчання Moodle, Teams, рекомендованих джерел, відеоматеріалів тощо.

7. Тематика курсу.

Лекції (16/6 годин):

1. **Основи стандартизації та сертифікації у сфері інформаційної безпеки** – 2 години
   Поняття, мета та завдання стандартизації та сертифікації
   Основні міжнародні та національні регулятори (ISO, IEC, NIST, ДСТУ)
2. **Міжнародні стандарти інформаційної безпеки (ISO/IEC 27000, NIST, COBIT, ITIL)** – 2 години
   Загальні принципи та структура стандартів
   Вимоги до управління ризиками інформаційної безпеки
3. **Національні стандарти та нормативна база України** – 2 години
   Законодавство України щодо захисту інформації
   ДСТУ та інші регуляторні вимоги
4. **Процедури сертифікації засобів та комплексів захисту інформації** – 2 години
   Види сертифікації та порядок її проведення
   Органи акредитації та сертифікації
5. **Методології оцінки відповідності та управління ризиками** – 2 години
   Процедури аудиту та тестування безпеки
   Оцінка ефективності захисних заходів
6. **Системи управління інформаційною безпекою (СУІБ)** – 2 години
   Концепція та впровадження систем управління
   Сертифікація СУІБ за стандартами ISO/IEC 27001
7. **Сертифікація криптографічних засобів та механізмів захисту інформації** – 2 години
   Основи криптографічного захисту та вимоги до сертифікації
   Оцінка криптографічних алгоритмів та їх відповідність стандартам
8. **Перспективи розвитку стандартизації та сертифікації в умовах новітніх загроз** – 2 години
   Виклики сучасної кібербезпеки
   Вплив штучного інтелекту та квантових технологій на стандартизацію

Лабораторні (16/6 годин):

1. Лабораторна робота №1: **Огляд міжнародних стандартів з управління інформаційною безпекою**
2. Лабораторна робота №2: **Класифікація засобів захисту інформації за міжнародними стандартами**
3. Лабораторна робота №3: **Аналіз процедур тестування та оцінювання засобів захисту інформації**
4. Лабораторна робота №4: **Оцінка та управління ризиками інформаційної безпеки в рамках сертифікації засобів захисту**
5. Лабораторна робота №5: **Розробка комплексної моделі захисту на основі стандартів сертифікації**
6. Лабораторна робота №6: **Вибір технологій криптографічного захисту та аналіз їх відповідності нормативним вимогам**
7. Лабораторна робота №7: **Аналіз практики сертифікації програмного устаткування для забезпечення інформаційної безпеки**
8. Лабораторна робота №8: **Оцінка відповідності технічних засобів захисту інформації вимогам екологічної безпеки та енергоефективності**

Розрахунково-графічна робота (РГР)

Тема: Розробка системи захисту інформації з урахуванням міжнародних стандартів та оцінка її відповідності.

Самостійна робота (88/108 годин):

1. Вивчення нормативних документів (ISO, NIST, ДСТУ)
2. Аналіз сучасних тенденцій у сертифікації засобів захисту
3. Ознайомлення з методами оцінки відповідності
4. Підготовка до лабораторних занять та виконання тестових завдань
5. Робота з дистанційними навчальними матеріалами (Moodle, Teams)

8. Система оцінювання та вимоги

Загальна система оцінювання курсу	Оцінювання курсу базується на **накопичувальній системі** та включає: **поточний контроль** (оцінювання лабораторних занять) – 40 балів, **проміжний модульний контроль** – 10 балів, **виконання індивідуального завдання (РГР)** – 10 балів **та підсумковий контроль** – 40 балів. Оцінювання кожного виду діяльності здійснюється окремо відповідно до **досягнення навчальних цілей**.
Вимоги до РГР, КР, КП тощо	**Критерії оцінювання РГР:** 1) відповідність завдання вимогам курсу – **2 балів;** 2) обґрунтування вибору стандартів та методів захисту – **2 балів;** 3) якість аналізу ризиків та оцінка відповідності – **2 балів;** 4) оформлення роботи, відповідність методичним рекомендаціям – **2 балів;** 5) своєчасність здачі роботи – **2 бали.**
Практичні (лабораторні) заняття	Оцінка кожного лабораторного заняття здійснюється за наступними критеріями: 1) виконання практичного завдання – **3 бали;** 2) аналіз отриманих результатів – **1 бал**; 3) належне оформлення звіту – **1 бал.**
Умови допуску до підсумкового контролю	1. Виконання та захист **не менше 50% лабораторних робіт** (щонайменше 4 із 8). 2. Проходження проміжного модульного контролю.

	3. Виконання **розрахунково-графічної роботи** (РГР).

Розподіл балів, які отримують здобувачі вищої освіти

Модуль за тематичним планом дисципліни та форма контролю		**Кількість балів**
Змістовий модуль 1. Основи стандартизації та сертифікації інформаційної безпеки		**30/30**
1	Основи стандартизації та сертифікації у сфері інформаційної безпеки	**5/5**
2	Міжнародні стандарти інформаційної безпеки (ISO/IEC 27000, NIST, COBIT, ITIL)	**5/5**
3	Національні стандарти та нормативна база України	**5/5**
4	Процедури сертифікації засобів та комплексів захисту інформації	**15/15**
Змістовий модуль 2. Оцінка відповідності та перспективи розвитку сертифікації		**30/30**
1	Методології оцінки відповідності та управління ризиками	**5/5**
2	Системи управління інформаційною безпекою (СУІБ)	**15/15**
3	Сертифікація криптографічних засобів та механізмів захисту інформації	**5/5**
4	Перспективи розвитку стандартизації та сертифікації в умовах новітніх загроз	**5/5**
Усього поточний і проміжний модульний контроль		**60/60**
Семестровий контроль (Екзамен)		**40/40**
Разом		**0…100**

Шкала оцінювання результатів навчання

Оцінка в балах	**Оцінка ECTS**	**Оцінка за національною шкалою (диференційований залік)**	
		для екзамену (диференційованого заліку), курсового проєкту (роботи), практики, атестації	для заліку
90 – 100	**A** (*відмінно*)	відмінно	зараховано
82-89	**B** (*дуже добре*)	добре	
75-81	**C** (*добре*)		
66-74	**D** (*задовільно*)	задовільно	
60-65	**E** (*достатньо*)		
0-59	**FX** (*незадовільно*)	незадовільно з можливістю повторного складання	незараховано з можливістю повторного складання

9. Обладнання та програмне забезпечення.

При вивченні курсу використовується наступне **обладнання та програмне забезпечення**:

І. Апартне забезпечення:

Персональні комп'ютери або ноутбуки з можливістю роботи у віртуальному середовищі. Операційні системи: Windows 10/11 Pro, Linux (Ubuntu, Kali Linux, CentOS – для безпекового аналізу), MacOS. Серверне обладнання для моделювання сертифікаційних процесів.

Мережеве обладнання (маршрутизатори, комутатори, мережеві екрани) для аналізу сертифікації апаратних засобів захисту.

Криптографічні пристрої (апаратні токени, смарт-карти, HSM – Hardware Security Module) для лабораторних досліджень криптографічного захисту.

II. Програмне забезпечення:

Для аналізу міжнародних стандартів інформаційної безпеки (ЛР 1, 2): ISO/IEC 27001 Toolkit – для розробки політик інформаційної безпеки, NIST Security Content Automation Protocol (SCAP) Tools – для оцінки відповідності стандартам, COBIT Framework – для аналізу та оцінки управління інформаційними ризиками.

Для тестування та оцінки засобів захисту інформації (ЛР 3, 4, 5): OpenSCAP – автоматичний аудит безпеки Nessus, OpenVAS – аналіз вразливостей та тестування безпеки, Metasploit Framework – перевірка захищеності засобів інформаційної безпеки, Wireshark – аналіз мережевого трафіку.

Для дослідження криптографічного захисту (ЛР 6): OpenSSL – генерація сертифікатів та тестування криптографічних алгоритмів, Cryptool 2 – аналіз шифрування та цифрових підписів, VeraCrypt – тестування систем шифрування даних.

Для сертифікації програмного забезпечення (ЛР 7): OWASP ZAP, Burp Suite – тестування безпеки веб-додатків, Checkmarx, SonarQube – аналіз коду на відповідність вимогам безпеки.

Для оцінки відповідності технічних засобів захисту інформації вимогам екологічної безпеки та енергоефективності (ЛР 8): PowerTOP, Joulemeter – аналіз енергоспоживання та ефективності апаратного забезпечення.

Для виконання розрахунково-графічної роботи (РГР): MS Visio, draw.io – моделювання архітектури систем захисту, MATLAB, R – оцінка ризиків та ефективності засобів захисту LaTeX, MS Word – підготовка технічної документації.

Платформи для дистанційного навчання Moodle, Microsoft Teams – розміщення матеріалів, тестування та проведення лекцій, Google Drive/OneDrive – спільна робота з документами.

10. Політики курсу.

У випадку, якщо здобувач протягом семестру не виконав у повному обсязі всіх видів навчальної роботи, має невідпрацьовані лабораторні роботи або не набрав мінімально необхідну кількість балів (25), він не допускається до складання диференційованого заліку під час семестрового контролю, але має право ліквідувати академічну заборгованість у порядку, передбаченому «Положенням про поточне та підсумкове оцінювання знань здобувачів НУ "Чернігівська політехніка"». Повторне складання заліку з метою підвищення позитивної оцінки не дозволяється. У випадку повторного складання заліку всі набрані протягом семестру бали анулюються, а повторний диференційований залік складається у вигляді тестування.

До загальної політики курсу відноситься дотримання принципів відвідування занять у відповідності до затвердженого розкладу, а також вільного відвідування лекційних занять для осіб, які отримали на це дозвіл відповідно до «Порядку надання дозволу на вільне відвідування занять здобувачам вищої освіти НУ «Чернігівська політехніка»». Запорукою успішного вивчення дисципліни є активність та залучення під час проведення лабораторних/практичних та лекційних занять – відповіді на запитання викладача (як один з елементів поточного контролю), задавання питань для уточнення незрозумілих моментів, вирішення практичних завдань. Консультації відбуваються в аудиторіях університету у відповідності до затвердженого розкладу або ж особистих чи групових консультацій (через вбудований форум) на сторінці курсу в системі дистанційного навчання НУ «Чернігівська політехніка».

Політика дедлайнів

Своєчасність здачі лабораторної роботи оцінюється в 0,5 балу за кожну лабораторну роботу. Своєчасність здачі РГР оцінюється в 1 бал. Відповідно, максимальна оцінка за невчасно здані роботи зменшується на зазначену кількість балів. Виключенням може бути наявність поважних причин несвоєчасної здачі зазначених робіт (хвороба, участь в зазначений час в інших видах навчальної, наукової чи організаційної роботи, офіційна робота за фахом тощо).

Політика користування ноутбуками / смартфонами

Прохання до здобувачів тримати смартфони переведеними у беззвучний режим протягом лекційних та практичних занять, так як дзвінки, переписки та спілкування у соціальних мережах відволікають від проведення занять як викладача, так й інших здобувачів. Ноутбуки, планшети та смартфони не можуть використовуватися в аудиторіях під час занять та під час проведення підсумкового контролю (за виключенням проходження тестового контролю в системі Moodle).

Політика заохочень та стягнень

За результатами навчальної, наукової або організаційної діяльності здобувачів вищої освіти за курсом їм можуть нараховуватися додаткові бали – до 10 балів, у залежності від вагомості досягнень. Види позанавчальної діяльності, за якими здобувачі вищої освіти заохочуються додатковою кількістю балів: участь у міжнародних проектах, наукові дослідження, тези, участь у науково-практичних конференціях, винаходи, патенти, авторські свідоцтва за напрямами курсу.

Політика академічної доброчесності

Академічна доброчесність повинна бути забезпечена під час проходження даного курсу, зокрема при виконанні лабораторних, контрольних та розрахунково-графічних робіт (КР/КП) (принципи описані у Кодексі академічної доброчесності НУ «Чернігівська політехніка»). Списування під час проміжного та підсумкового контролів, виконання практичних завдань на замовлення, підказки вважаються проявами академічної недоброчесності. Від усіх слухачів курсу очікується дотримання академічної доброчесності у зазначених вище моментах. До здобувачів вищої освіти, у яких було виявлено порушення академічної доброчесності, застосовуються різноманітні дисциплінарні заходи (включаючи повторне проходження певних етапів).

Правила перезарахування кредитів

Кредити, отримані в інших закладах вищої освіти, а також результати навчання у неформальній та/або інформальній освіті, можуть бути перезараховані викладачем у відповідності до положення «Порядок визначення академічної різниці та перезарахування навчальних дисциплін у НУ «Чернігівська політехніка»». Визнання результатів навчання у неформальній освіті розповсюджується на окремі змістові модулі (теми) навчальної дисципліни.

11. Рекомендована література.

Базові підручники:

1. Салавеліс, Алла Дмитрівна; Павловський, Сергій Миколайович-Стандартизація, метрологія та сертифікація(2023)

2. Стандартизація, сертифікація засобів та комплексів захисту інформації. Методичні вказівки до виконання лабораторних робіт для здобувачів другого (магістерського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» спеціальності 125 Кібербезпека та захист інформації. – Чернігів: НУ «Чернігівська політехніка», 2024 – 94 с. [Електронний ресурс]. Режим доступу: https://ir.stu.cn.ua/jspui/handle/123456789/30068

3. Комплексні системи захисту інформації : конспект лекцій — Ю. І. Хлапонін, А. М. Котенко(2022)

4.Zinaida Zhyvko, Taras Rudyi, Volodymyr Senyk, Liliia Kucharska Legal Basis of Ensuring Cyber Security of Ukraine: Problems and Ways of Eliminating (2020)

5. **Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M.** (2021). *The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda*. The TQM Journal, 33(2), 39-59. https://www.emerald.com/insight/content/doi/10.1108/TQM-09-2020-0202/full/html

6. **Chapple, M., Stewart, J. M., & Gibson, D.** (2021). *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide* (9th ed.). Wiley. https://books.google.com/books/about/ISC_2_CISSP_Certified_Information_System.html?id=kSw0EAAAQBAJ

7. **Peltier, T. R.** (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Auerbach Publications.

8. **Calder, A.** (2019). *ISO/IEC 27001:2013 A Pocket Guide* (2nd ed.). IT Governance Publishing.

9.. **Solms, B. von, & Niekerk, J. van.** (2017). *Information Security Governance*. Springer.

Інтернет-джерела:

1. ISO/IEC 27000 Family of Standards – Офіційний сайт міжнародних стандартів з інформаційної безпеки: https://www.iso.org/isoiec-27001-information-security.html

2. NIST Special Publications on Information Security – База документів NIST щодо стандартів кібербезпеки: https://csrc.nist.gov/publications

3. Єдиний державний реєстр сертифікованих засобів захисту інформації в Україні – Перелік сертифікованих рішень у сфері інформаційної безпеки: https://cip.gov.ua