Силабус освітнього компонента
Програма навчальної дисципліни

Інформаційна безпека у видавничо-поліграфічній діяльності

Шифр та назва спеціальності
G20 – Видавництво та поліграфія

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Спеціалізація
-

Кафедра
Системного аналізу та інформаційно-аналітичних технологій (322)

Освітня програма
Сучасні технології у видавництві та медіаіндустрії

Тип дисципліни
Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
2

Мова викладання
Українська

Викладачі, розробники

Колбасін Вячеслав Олександрович
viacheslav.kolbasin@khpi.edu.ua
Кандидат технічних наук, доцент, доцент кафедри системного аналізу та інформаційно-аналітичних технологій НТУ "ХПІ"

Досвід роботи – 26 років. Автор понад 40 наукових та навчально-методичних праць. Має професійні сертифікації: AWS Certified Solutions Architect – Associate, AWS Certified Machine Learning – Specialty, Oracle Certified Associate Java SE7, Oracle Certified Professional Java SE7.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

«Інформаційна безпека у видавничо-поліграфічній діяльності» – один з курсів профільної підготовки, що продовжує фундаментальну підготовку магістрів за освітньою програмою – «Сучасні технології у видавництві та медіаіндустрії». Дисципліна навчає комплексу заходів, спрямованих на захист інформації від будь-якого навмисного чи випадкового впливу, який може завдати шкоди її власникам або системам, збереження її конфіденційності, цілісності та доступності

Мета та цілі дисципліни

Дисципліна має метою сформувати систему знань, навичок та компетентностей для забезпечення ефективного захисту інформації та інформаційних систем від загроз, навчити студентів орієнтуватися в

інформаційному просторі, розпізнавати небезпеки та користуватися методами й засобами захисту, а також розуміти принципи конфіденційності, цілісності та доступності інформації.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

Інтегральна компетентність: Здатність розв'язувати складні задачі дослідницького та/або інноваційного характеру у сфері видавництва та поліграфії

Загальні компетентності:

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.

ЗК 2. Здатність генерувати нові ідеї (креативність).

ЗК 4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

ЗК 8. Здатність до абстрактного мислення, аналізу та синтезу..

СК 1. Здатність комплексно оцінювати вплив середовища функціонування технологічних і виробничих процесів для удосконалення параметрів продукції.

СК 2. Здатність критично осмислювати проблеми видавництва і поліграфії та на межі галузей знань, а також перспективних напрямів розвитку галузі.

СК 3. Здатність визначати головні функції і напрямки вдосконалення забезпечення виробництва розробляти заходи оперативного та перспективного управління, прогнозування і планування виробництва.

СК 7. Здатність застосовувати сучасні методи та інструменти для досліджень у сфері видавництва та поліграфії, а також забезпечення якості продукції.

СК 8. Здатність розробляти і реалізовувати наукові та прикладні проєкти у сфері видавництва і поліграфії та з дотичних до неї міждисциплінарних напрямів з урахуванням технічних, економічних, соціальних, правових та екологічних аспектів.

Результати навчання

РН 3. Приймати ефективні рішення з питань видавництва та поліграфії, у тому числі у складних і непередбачуваних умовах; прогнозувати їх розвиток та кон'юнктуру ринку; визначати фактори, що впливають на досягнення поставлених цілей, зокрема, вимоги споживачів; аналізувати і порівнювати альтернативи; оцінювати ризики та імовірні наслідки рішень.

РН 5. Розробляти та виконувати проекти видавничо-поліграфічного виробництв та систем їх інженерно-технічного забезпечення з врахуванням інженерних, правових, економічних, екологічних та соціальних аспектів, здійснювати їх інформаційне та методичне забезпечення.

РН 8 Розробляти і впроваджувати ефективні технології, розробляти інструкції та технологічні регламенти на випуск продукції видавництва та поліграфії.

РН 9. Здійснювати дослідження та/або провадити інноваційну діяльність з метою отримання нових знань та створення нових технологій та продуктів в сфері видавництва і поліграфії та в ширших мультидисциплінарних контекстах

РН 11. Застосовувати сучасні експериментальні та математичні методи, інформаційні технології та спеціалізоване програмне забезпечення для досліджень і розробок у сфері видавництва та поліграфії.

РН 12. Відшуковувати необхідні дані в науковій літературі, базах даних та інших джерелах, аналізувати та оцінювати ці дані.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні заняття – 16 год., самостійна робота –72 год.

Передумови вивчення дисципліни (пререквізити)

Для вивчення курсу студенти потребують базових знань з дисциплін: «Програмування», «Об'єктно-орієнтоване програмування», «Організація та проектування баз даних».:

Особливості дисципліни, методи та технології навчання

Лекції проводяться з використанням мультимедійних технологій. Навчальні матеріали доступні студентам через OneDrive кафедри. Вивчення курсу потребує використання програмного забезпечення Microsoft Visual Studio Code, комплекс JS-бібліотек, крім загально вживаних програм і операційних систем.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до теорії захисту інформації. Основні поняття та визначення. Інформаційні загрози. Види захисту інформації. Криптографічний захист інформації. Основні поняття.	2
Тема 2. Елементи криптології. Основні терміни та визначення. Класифікація шифрів. Симетричне шифрування. Асиметричне шифрування. Порівняння, переваги та недоліки кожного класу шифрів.	2
Тема 3. Використання алгоритмів симетричного шифрування. Шифри пересувань та замін. Шифри пересувань. Види пересувань. Шифри заміни. Види замін Особливості застосування. Переваги та недоліки.	2
Тема 4. Використання алгоритмів симетричного шифрування. Шифри гамування. Гамування основні поняття та особливості використання. Застосування псевдо випадковості. Генерація псевдовипадкових послідовностей. Алгоритми генерації. Види генераторів.	2
Тема 5. Вступ до симетричного шифрування. Особливості використання. Узагальнена схема асиметричної криптосистеми. Вступ до теорії чисел. Використання простих чисел. Функція Ейлера. Алгоритми Евкліда. Види асиметричних алгоритмів.	2
Тема 6. Аналіз алгоритмів асиметричного шифрування. RSA, DSA (алгоритм цифрового підпису), Алгоритм Діффі-Хелмана, алгоритм Єль-Гамаля, алгоритм з еліптичною кривою. Переваги та недоліки алгоритмів.	2
Тема 7. Використання хешування для захисту інформації. Основні методи хешування. Поняття хешування. Колізії. Хеш-таблиці. Коефіцієнт заповнення хеш-таблиць. Контрольна сума. Метод контрольних сум. Метод середніх квадратів.	2
Тема 8. Використання хешування для захисту інформації. Розширені методи хешування. Модульне хешування. Метод ділення. Метод перетворення системи числення. Метод згортання. Мультиплікативний метод.	2
Тема 9. Використання хешування для захисту інформації. Створення та використання хеш-таблиць. Схеми побудови хеш-таблиць. Ланцюжок з окремими списками. Адресація хешування відкритого лінійного зонда. Розв'язання колізій за допомогою ланцюгів. Хеш-функції. Рівномірне хешування. Лінійне хешування. Квадратичне хешування. Подвійне хешування.	2

Теми лекцій	Кількість годин
Тема 10. Використання електронного підпису (ЕЦП) для захисту інформації. Основні поняття ЕЦП. Валідації ЕЦП. Удосконалений ЕЦП. Алгоритми створення ЕЦП. RSA, ElGamal. Порівняння. Переваги та недоліки.	2
Тема 11. Використання комбінованих шифрів. Шифри ADFGX і ADFGVX. Блокове шифрування. Шифрування на основі мереж Фейстель. DES (Data Encryption Standard), DES – ECB, DES – CBC, DES – CFB, DES – OFB, AES.	2
Тема 12. Використання алгоритму RSA (Rivest, Shamir, Adleman). Загальна інформація. Особливості використання алгоритму. Шифрування. Дешифрування. Питання практичного використання алгоритму.	2
Тема 13. . Використання алгоритму Діфі-Хелмана. Загальна інформація. Особливості використання алгоритму. Шифрування. Дешифрування. Питання практичного використання алгоритму.	2
Тема 14. . Використання алгоритму Ель-Гамаля. Загальна інформація. Особливості використання алгоритму. Шифрування. Дешифрування. Питання практичного використання алгоритму..	2
Тема 15. Криптоаналіз. Принципи використання. Загальні поняття криптоаналізу Основні алгоритми криптоаналізу. Порівняння. Переваги та недоліки.	2
Тема 16. Криптоаналіз. Додаткові можливості. Додаткові алгоритми криптоаналізу. Порівняння. Переваги та недоліки..	2
Загальна кількість годин	**32**

Практичні заняття

Практичні заняття в рамках дисципліни не передбачені.

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Симетричне шифрування. Використання шифрів перестановки та заміни. Програмна реалізація алгоритмів і методів використання шрифтів з різними видами перестановок та замін.	2	0,1
Тема 2. Симетричне шифрування. Використання шифрів гамування (адитивних шифрів).Застосування генераторів псевдовипадкових послідовностей. Програмна реалізація алгоритмів і методів використання шрифтів гамування та моделювання роботи генераторів псевдовипадкових послідовностей.	2	0,1
Тема 3. Симетричне шифрування. Використання шифрів гамування (адитивних шифрів). Застосування регістру зсуву з лінійним зворотним зв'язком. Програмна реалізація алгоритмів і методів використання шрифтів гамування та моделювання роботи регістру зсуву з лінійним зворотним зв'язком.	2	0,1
Тема 4. Асиметричне шифрування з відкритими ключами. Алгоритм RSA. Аналіз, вивчення особливостей та програмна реалізація алгоритму RSA, як одного методів використання шифрування з відкритим ключем.	2	0,1

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 5. Асиметричне шифрування. Алгоритм на основі завдання про «укладання ранця». Аналіз, вивчення особливостей та програмна реалізація алгоритму на основі завдання про «укладання ранця», як одного методів використання шифрування з відкритим ключем.	2	0,1
Тема 6. Створення та аналіз хеш-функцій. Аналіз, вивчення особливостей та програмна реалізація хеш-функцій.	2	0,1
Тема 7. Хешування. Використання електронного підпису.. Аналіз, вивчення особливостей та програмна реалізація електронного підпису.	2	0,1
Тема 8. Основи криптоаналізу. Огляд, вивчення особливостей та програмна реалізація деяких алгоритмів криптоаналізу.	2	0,1
Загальна кількість годин	16	$\sum_{i=1}^{n} a_i = 0{,}8$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу та підготовка розрахункової робіти.

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Безпека хмарних технологій (Cloud Security). Особливості захисту даних у моделях IaaS, PaaS, SaaS. Ризики спільного використання інфраструктури та методи шифрування у хмарі.	8
Тема 2. Вразливості вебдодатків та класифікація. **OWASP Top 10:** Вивчення найпоширеніших загроз для вебпідрозділів (SQL-ін'єкції, XSS-скриптинг) та методів їх запобігання.	8
Тема 3. Шкідливе програмне забезпечення та аналіз загроз: Класифікація сучасного ПЗ (вимагачі, руткіти, трояни). Принципи роботи антивірусних систем та пісочниць (sandboxing).	8
Тема 4. Сучасні методи автентифікації та керування доступом. Еволюція паролів, багатофакторна автентифікація (MFA), біометрія та безпарольний доступ (FIDO2/WebAuthn).	8
Тема 5. Криптографічні протоколи інтернет-безпеки. Принципи роботи протоколів SSL/TLS, HTTPS, IPsec та SSH. Застосування асиметричного та симетричного шифрування.	8
Тема 6. Резервне копіювання та відновлення даних після збоїв (DRP/BCP). Стратегії створення бекапів (правило 3-2-1), планування безперервності бізнесу та відновлення IT-інфраструктури.	8
Тема 7. Соціальна інженерія та психологічні маніпуляції. Методи протидії фішингу, претекстингу та вішингу. Навчання персоналу (Security Awareness).	8
Тема 8. Законодавство та стандарти в інформаційній безпеці.	8

Огляд міжнародних стандартів (ISO/IEC 27001), європейського регламенту захисту даних (GDPR) та законів України про кібербезпеку.	
Тема 9. Безпека Інтернету речей (IoT) та розумних пристроїв. Уразливості побутової та промислової смарт-електроніки, архітектура захисту IoT-мереж.	8
Загальна кількість годин	**72**

Розрахункове завдання

Теми розрахункової робіти	Вагові коефіцієнти b
Тема 1. Визначення часу виконання програм чи фрагментів коду реалізації алгоритмів симетричного шифрування. Визначення часу виконання програм, що реалізують алгоритми симетричного шифрування-дешифрування, створених у відповідних лабораторних роботах. Побудова порівняльних таблиць та графіків.	0,1
Тема 2. Визначення часу виконання програм чи фрагментів коду реалізації алгоритмів асиметричного шифрування. Визначення часу виконання програм, що реалізують алгоритми асиметричного шифрування-дешифрування, створених у відповідних лабораторних роботах. Побудова порівняльних таблиць та графіків. Порівняння часу виконання шифрування-дешифрування симетричними та асиметричними методами	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Інформаційна безпека. Навчальний посібник. Ч. 2 / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ, 2022. – 196 с. https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053455.pdf
2. Інформаційна безпека: питання правового регулювання: монографія / А.Ю. Нашинець-Наумова. – Київ: Видавничий дім «Гельветика», 2023. – 168 с. https://elibrary.kubg.edu.ua/id/eprint/18860/1/A_Nashinets-Naumova_monografia_1_FPMV.pdf
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк,О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова – К.:Видавництво Ліра-К, 2023. – 412 с https://jurkniga.ua/contents/informatsiyna-bezpeka.pdf?srsltid=AfmBOoqgaDN_FmmBe9whiFCWeTVAC0ZrPIvNrnn3gX3Y6ZIHc_ME382h
4. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2022. — 352 chttps://repository.hneu.edu.ua/bitstream/123456789/3068/1/%D0%9D%D0%B0%D0%B2%D1%87%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA.%20%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.%20%D0%9A%D0%B0%D0%B2%D1%83%D0%BD%20%D0%A1.%D0%92..pdf
5. Літнарович Р.М. Сучасні технології інформаційної безпеки.Частина 1. Навчальний посібник, МЕГУ, Рівне, 2011.-97 с.Litnarovich R. M.Modern technologies of informative safety. Part 1. Train aid. IEGU,Rivne, 2022 https://essuir.sumdu.edu.ua/bitstream-download/123456789/19469/1/%d0%a1%d1%83%d1%87%d0%b0%d1%81%d0%bd%d1%96%20%d1%82%d

0%b5%d1%85%d0%bd%d0%be%d0%bb%d0%be%d0%b3%d1%96%d1%97%20%d1%96%d0%bd%d1%84%d0%be%d1%80%d0%bc%d0%b0%d1%86%d1%96%d0%b9%d0%bd%d0%be%d1%97%20%d0%b1%d0%b5%d0%b7%d0%bf%d0%b5%d0%ba%d0%b8%20%d0%a7%d0%b0%d1%81%d1%82%d0%b8%d0%bd%d0%b0%201.pdf;jsessionid=9CC35996E9D295887CA07B27E8D541F7
6. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2021. – 144 с https://vstup.htek.com.ua/wp-content/uploads/2024/10/34.1-Grebenyuk.pdf
7.. Основи інформаційної безпеки : навч. пос. / Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. – Вінниця : ВНТУ, 2023. – 316 с. https://pdf.lib.vntu.edu.ua/books/IRVC/Dudikevich_2018_316.pdf
8. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки.[Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. ,2018. – 320 с
https://elibrary.kubg.edu.ua/id/eprint/27370/1/V_Buriachok_Posibnik_2019_FITU.pdf
9. Ю. А. Тарнавський; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 2,04 Мбайт). – Київ : КПІ ім. Ігоря Сікорського, 2023. – 162 с. https://www.filestack.com/wp-content/uploads/2024/10/React-Ebook-Filestack.pdf
10. Погребняк А.В. Технології комп'ютерної безпеки. Монографія. МЕГУ, Рівне, 2011.-117 с. Pogrebnyak A.V. Technologies of computer safety. Monograph. IEGU, Rivne, 2011.-117 p
https://essuir.sumdu.edu.ua/bitstream-download/123456789/20273/1/%d0%9a%d0%bd%d0%b8%d0%b3%d0%b0%d0%9f%d0%be%d0%b3%d1%80%d0%b5%d0%b1%d0%bd%d1%8f%d0%ba%20%d0%90.%d0%92..pdf

Додаткова література

1. Information Security and Cryptology, 2023
https://www.researchgate.net/publication/241523458_Information_Security_and_Cryptology
2. ReactJS by Example – Building Modern Web Applications with React? 2022 https://bdfc.com.vn/wp-content/uploads/2018/03/ReactJS_by_Example.pdf
13Information Security and Cryptography, 2021 https://tecsec.com/download/188/constructive-key-management/12916/tswl005_info-security-and-cryptograpy.pdf
14. Cryptography and Information Security, 2020 https://www.scribd.com/doc/177537358/Cryptography-and-Information-Security

Інформаційні ресурси

1. Все, що потрібно знати про шифрування

https://safety.rsf.org/ukr/all-you-need-to-know-about-encryption/

2. Інформаційна безпека: що це таке, види та засоби захисту:

https://voll.kiev.ua/uk/blog/informacijna-bezpeka-sho-ce-take-vidi-ta-zasobi-zahistu

3. Криптографічні методи захисту інформації. Контроль цілісності програмних та інформаційних ресурсів:

https://sites.google.com/view/dcptoinformat/%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0-10-11/%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0/%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D0%B9/2-4-

%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%87%D0%BD%D1%96-%D0%BC%D0%B5%D1%82%D0%BE%D0%B4%D0%B8-%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97

4. Інформаційна безпека та види можливих загроз:

https://itbiz.ua/statti-ta-obzori/informacijna-bezpeka-ta-vidi-mozhlivih-zagroz/

5. Сучасні методи гомоморфного шифрування інформаційних ресурсів:

https://ela.kpi.ua/items/3d2d70c9-d6eb-40c6-ab58-1d95fbb06949

6. CSS – ІНФОРМАЦІЙНА БЕЗПЕКА:

https://vstechno.com.ua/?page_id=218

7. АНАЛІЗ СТРУКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ:

https://journals.nupp.edu.ua/sunz/article/view/1412

8. Cryptography Tutorial:

https://www.geeksforgeeks.org/computer-networks/cryptography-tutorial/

9. Cryptography Tutorial:

https://www.tutorialspoint.com/cryptography/index.htm

10. Cryptography and its Types:

https://www.geeksforgeeks.org/computer-networks/cryptography-and-its-types/

11. Cryptography Techniques: Everything You Need to Know:

https://www.theknowledgeacademy.com/blog/cryptography-techniques/

12. Cryptography and network security: The quick and short guide:

https://spectralops.io/blog/cryptography-and-network-security-the-quick-and-short-guide/

13. Principles of encryption:

https://www.open.edu/openlearn/digital-computing/network-security/content-section-4.1

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,8	0	0,2	0

Розрахунок підсумкової оцінки проводиться за формулою:

$$О = П \cdot k_1 + К \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

де: *П* – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
К – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + \ldots + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$К = \frac{К_1 \cdot b_1 + К_2 \cdot b_2 + \ldots + К_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Поточні оцінки за кожну складову (П, *К*, *І*,...) виставляються за 100-бальною шкалою згідно з положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ».

Підсумкова оцінка виставляється відповідно до розрахованої *О* з округленням до найближчого цілого числа в більшу сторону.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту.

Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	26.08.2026	Завідувачка кафедри Тетяна АЛЕКСАНДРОВА
	26.08.2026	Гарант ОП Тетяна АЛЕКСАНДРОВА