Силабус освітнього компонента

Програма навчальної дисципліни

Комп`ютерні мережі

Шифр та назва спеціальності
К4 – Управління інформаційною безпекою

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Управління інформаційною безпекою

Тип дисципліни
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

Викладачі, розробники

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Комп'ютерні мережі" є обов`язковою навчальною дисципліною. Мережеві технології та інтернет впливають на людей по-різному в різних країнах світу. У майбутньому основні напрямки для розробників нових технологій будуть пов'язані з використанням інтернет в

якості бази для створення нових продуктів і послуг, розроблених спеціально з урахуванням можливостей мережі. Оскільки розробники розширюють межі досяжного, можливості взаємно підключених мереж, що утворюють інтернет, гратимуть дедалі все більше значення в досягненні успіху цих проектів.

Мета та цілі дисципліни

Формування теоретичних знань основних принципів побудови сучасних мереж, до яких відносяться локальні, глобальні та регіональні мережі, за допомогою яких реалізовуються нові підходи управління сучасним інформаційним суспільством, а також формування практичних навичок із побудови та управління корпоративними системами та мережами.

Формат занять

Лекції, лабораторні заняття, індивідуальне завдання, самостійна робота, консультації. Підсумковий контроль – іспит.

Компетентності

ЗК3. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК5. Здатність спілкуватися іноземною мовою.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.
СК3. Проектувати системи управління та захисту інформації на підприємстві установі, організації.
СК5. Здатність узагальнення вітчизняного та закордонного досвіду з питань управління інформаційною безпекою.
СК6. Здатність використовувати іноземну мову для отримання додаткових знань і умінь з питань управління інформаційною безпекою, взаємодіяти з іноземними партнерами.
СК7. Здатність організовувати та проводити аналіз оточення організації установ з метою виявлення та закриття можливих каналів витоку інформації.
СК8. Здатність використовувати механізми забезпечення управління інформаційною безпекою у її визначальних сферах.
СК9. Здатність організації реагування на загрози на об'єктах критичної інфраструктури, установах та підприємствах.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.
СК11. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації.

Результати навчання

РН3. Вміти за допомогою абстрактного мислення, аналізу та синтезу оцінювати результати професійної діяльності та забезпечувати її якість, бути критичним і самокритичним, наполегливим щодо поставлених завдань і взятих зобов'язань.
РН4. Вільно спілкуватися державною мовою.
РН5. Вільно спілкуватися іноземною мовою у межах потреби своєї професійної діяльності.
РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
РН8. Вміти використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій щодо формування системи управління інформаційної безпеки.

РН10. Вміти аналізувати виклики та загрози інформаційної безпеки об'єктів критичної інфраструктури та синтезувати інформацію щодо розроблення та реалізації стратегій та політики безпеки.
РН11. Вміти забезпечувати процеси захисту та функціонування системи управління інформаційною безпекою та захисту інформації на основі практик, навичок та знань, щодо інфраструктури кіберфізичних систем та інформаційних потоків.
РН12. Вміти використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН13. Вміти вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління інформаційної безпеки згідно встановленої політики безпеки в інформаційно-комунікаційних системах.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН16. Вміти реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційно-комунікаційних системах.
РН17. Вміти розв'язувати задачі управління інфораційною безпекою в інформаційно-комунікаційних системах на основі моделей управління безпекою.
РН18. Розуміти основні теоретичні поняття, застосовувати набуті практичні навички дослідження та підготовки документів, їх правильного використання в управлінській діяльності.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно-комунікаційних систем.
РН22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Законодавчі основи процесів інформатизації в Україні, вміння використовувати ОС Linux, знання механізмів роботи з Packet Tracer.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Основні положення теорії взаємодії відкритих систем.	2

Хронологічна наслідність важливих подій в історії розвитку комп`ютерних мереж. Хронологічна наслідність важливих подій в історії розвитку комп'ютерних мереж. Загальна структура системи зв'язку. Методи комутації. Протоколи глобальних мереж. Імовірно-тимчасові характеристики технологій ГВП. Стек протоколів мережі x.25. Теоретичні способи зменшення надмірності. Алгоритм стиснення повторюваних даних RLE. Алгоритми стиснення за ключовими словами KWE. Алгоритми кодування змінної довжини. Кодування інформації у локальних мережах.	
Тема 2. Модель OSI. **Модель взаємодії відкритих систем. Багаторівнева система вкладання пакетів. Включення проміжних пристрій мережі. Функції різних рівнів iso/osi. Транспортний рівень. Методи взаємодії в мережіosi/iso . Функції різних рівнів iso/osi . Канальний рівень iso/osi. Фізичний рівень (physical layer - pl). Канальний рівень iso/osi . Апаратура локальних мереж. Основні функції адаптерів. Функції драйвера мережевого адаптера в моделі osi. Протоколи високих рівнів. Протоколи високих рівнів. Транспортні протоколи. Мережеві протоколи. Протоколи стеку apple talk і модель osi/iso . Класи мереж. Стандартні мережеві програмні засоби. Однорангові мережі. Мережі на основі серверу.**	1
Тема 3. Якість обслуговування QoS. **Основні вимоги. Показник якості обслуговування мережі. Основні характеристики виробництва. Показники якості передачі даних. Допускні значення вимог до основних показників якості. Алгоритм розрахунку. Приклад розрахунку.**	1
Тема 4. Методи повторної передачі. **Стек протоколів мережі x.25. Множина протоколів hdlc . Метод з зупинкою та очікуванням . ARQ з паралельним використанням віртуальних каналів. Повторна передача на n кроків назад. Ефективність роботи алгоритму ARQ на N кроків назад. Передача з виборчим повтором. Недоліки методу. Методика оцінки ефективності обміну даними у корпоративній мережі. Оцінки ефективності обміну даними у корпоративній мережі у каналах без пам'яті. Ефективність різних мереж без пам'яті.**	1
Тема 5. Мережа Ethernet. **Мережі ethernet і fast ethernet . Стандарти категорії IEEE 802.X . Типи процедур LLC підрівнів . Адресації пакетів. Структура адреса. Метод доступу CSMA / CD . Виникнення конфлікту. Об'єднання кількох сегментів кабелю. Еволюція локальних мереж . Функціонування комутаторів локальної мережі. Передача кадру з порту на порт комутатора. Методи комутації . Управління потоком у напівдуплексному і дуплексному режимах. Технології комутації і модель osi. Трьохрівнева ієрархічна модель мережі.**	1
Тема 6. Протокол мережевого рівня – IP протокол. **Типи адрес. Формати IP-адреси. IP-адресації версії 4. Формат заголовка IP . Угоди про особливості інтерпретації IP-адрес.**	1

Використання масок в IP адресації. Особливості IPV6. Заголовок IPV6 . Типи адрес в IPV6 . Форми представлення адреси . Модель адресації. Розподіл адресного простору. Протокол ARP . Структура заголовку ARP. Алгоритм використання ARP у ГВС . Маршрутизації в IP-мережах. Таблиці маршрутизації. Протокол DNS . Ієрархія імен в DNS . Типи записів DNS . Основні схеми дозволу DNS-імен.	
Тема 7. Протоколи транспортного рівня. **Транспортний рівень. Transmission Control Protocol. Заголовок TCP. Структура заголовка TCP. TCP порти. Встановлення з'єднання TCP . Протокол UDP . UDP заголовок. Протокол TCP/IP . Функції рівнів. протокол RTP . Заголовок пакета RTP . Мережі на основі RTP. Послідовне включення змішувачів . Протокол RTCP . Пакети звіту RTCP. Формат пакета SDES (опис джерела). Характеристики джерела . Перевірка коректності заголовка RTCP .**	1
Тема 8. Протоколи маршрутизації. **Протоколи маршрутизації. Фіксована маршрутизація. Адаптивна маршрутизація. Показники алгоритмів(метрики). Алгоритми маршрутизації. Динамічна маршрутизація. До маршрутизація. IGP: DISTANCE-VECTOR . IGP: LINK STATE. RIP:Освіта петель. OSPF (OPEN SHORTEST PATH FIRST).**	1
Тема 9. Сучасні мережеві технології. **Компоненти мережі. Подання та топології мереж. Основні типи мереж. Інтернет-підключення. Надійні мережі. Безпека мережі.**	1
Тема 10. Базова конфігурація комутатора та кінцевого пристрою. **Навігація по IOS. Структура команд. Базове налаштування пристроїв. Збереження змін. Порти та адреси. Налаштування IP-адресації.**	1
Тема 11. Протоколи та моделі. **Правила. Протоколи. Набір протоколів. Організації зі стандартизації. Еталонні моделі. Інкапсуляція даних. Доступ до даних.**	1
Тема 12. Фізичний рівень. **Призначення фізичного рівня. Характеристики фізичного рівня. Мідні кабелі. Кабелі UTP. Оптоволоконні кабелі. Бездротове середовище передачі даних.**	1
Тема 13. Транспортний рівень. **Двійкова система числення. Шістнадцяткова система числення. Передача даних. Огляд протоколу TCP. Огляд UDP. Номери портів. Процес обміну даними за протоколом TCP. Надійність та керування потоком. Обмін даними за протоколом UDP. Прикладний рівень, рівень вистави, сеансовий рівень. Однорангові мережі. Протоколи веб-трафіку та електронної пошти. Сервіси IP-адресації. Сервіси обміну файлами.**	1
Тема 14. Принципи забезпечення безпеки мереж. **Загрози та вразливість безпеки. Мережеві атаки. Захист від**	1

мережевих атак. Безпека пристроїв. Пристрої в мережі невеликого розміру. Програми та протоколи в мережі невеликого розміру. Масштабування до більших мереж. Перевірка підключення. Команди хоста та IOS. Методи пошуку та усунення несправностей. Сценарії пошуку та усунення несправностей.	
Тема 15. Базова конфігурація маршрутизатора. Початкове налаштування маршрутизатора. Налаштування інтерфейсів. Налаштування стандартного шлюзу.	1
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Вивчення мережевих інструментів спільної роботи Хмарні сервіси для командної роботи (Google Workspace, Microsoft Teams, Slack). Системи контролю версій (Git, GitHub, GitLab). Спільна робота над документами та кодом. Питання безпеки при використанні хмарних сервісів.	4	1
Тема 2. Вивчення вакансій у сфері інформаційних і мережевих технологій Пошук вакансій на спеціалізованих сайтах (LinkedIn, Indeed, Djinni, Work.ua). Основні вимоги до мережевих спеціалістів (сертифікації, досвід, софт-скіли). Аналіз ринку праці та перспектив кар'єрного росту. Оформлення результатів аналізу.	4	1
Тема 3. Вивчення сервісів конвергентних мереж Поняття конвергентної мережі. Сервіси передачі даних, голосу (VoIP), відео. QoS (якість обслуговування) та її роль. Приклади корпоративних застосувань.	4	1
Тема 4. Packet Tracer. Навігація по IOS Ознайомлення з інтерфейсом Packet Tracer. Основні режими Cisco IOS (User EXEC, Privileged EXEC, Global Configuration). Основні команди перегляду конфігурації (show, ping, traceroute). Використання довідки та автодоповнення команд..	4	1
Тема 5. Packet Tracer. Налаштування початкових параметрів комутатора Підключення до комутатора через консоль. Налаштування імені пристрою та банерного повідомлення. Налаштування паролів доступу. Збереження конфігурації (copy running-config startup-config).	4	1

Тема 6. Початок роботи консолі за допомогою програми Tera Term Встановлення та налаштування Tera Term. Підключення до обладнання через консольний кабель. Використання різних типів з'єднання (Serial, SSH, Telnet). Виконання базових команд у Tera Term.	3	1
Тема 7. Packet Tracer. Створення основних підключень Типи кабелів (straight-through, crossover, console). Підключення ПК до комутатора. Підключення комутаторів між собою. Тестування зв'язності (ping).	3	1
Тема 8. Створення простої мережі Побудова топології локальної мережі (LAN). Налаштування IP-адрес на ПК. Перевірка зв'язності мережі. Аналіз роботи мережі за допомогою інструментів Packet Tracer.	3	1
Тема 9. Налаштування адреси управління комутатором Призначення IP-адреси на VLAN 1. Налаштування шлюзу за замовчуванням. Перевірка доступності комутатора з ПК. Збереження конфігурації та її відновлення.	3	1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 9$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Базові принципи побудови та функціонування комп'ютерних мереж. Основні положення теорії взаємодії відкритих систем. Модель OSI та TCP/IP: принципи, рівні, функції. Методи комутації та повторної передачі даних. Мережа Ethernet: розвиток стандартів, особливості роботи, протокол CSMA/CD. Протокол IP (IPv4/IPv6): структура, принципи адресації та маршрутизації.	0,5
Тема 2. Сучасні протоколи, технології та безпека комп'ютерних мереж. Протоколи транспортного рівня: TCP, UDP, RTP, їх застосування. Протоколи маршрутизації: RIP, OSPF (порівняльний аналіз). Сучасні мережеві технології: VPN, хмарні сервіси, SDN. Основи мережевої безпеки: типи атак та методи захисту. Базова конфігурація комутаторів та маршрутизаторів (Cisco Packet Tracer).	0,5
Тема 3. Безпека комп'ютерних мереж та методи її забезпечення. Класифікація загроз у локальних та глобальних мережах. Основні принципи побудови захищених мереж. Методи аутентифікації та шифрування даних. Використання VPN для захисту інформаційних	1

каналів. Фаєрволи, IDS/IPS системи та їх роль у безпеці.	
Загалом	$\sum_{i=1}^{m} b_i = 2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу та виконання індивідуального завдання.

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Історія та еволюція комп'ютерних мереж. Розвиток мереж ARPANET, Internet. Стандартизація мережевих технологій (IETF, IEEE, ISO). Перехід від IPv4 до IPv6: причини та перспективи.	8
Тема 2. Фізичні середовища передачі даних. Кабельні технології: коаксіал, «виті пари», оптоволокно. Безпровідні канали: Wi-Fi, Bluetooth, LTE/5G. Характеристики та обмеження середовищ передачі.	8
Тема 3. Топології комп'ютерних мереж. Шина, зірка, кільце, дерево, гібридна топологія. Переваги та недоліки різних топологій. Використання в локальних та глобальних мережах.	7
Тема 4. Служби Інтернету. DNS: структура, принцип роботи. DHCP: автоматичне надання IP-адрес. WWW, FTP, SMTP, POP3, IMAP – принципи роботи сервісів.	7
Тема 5. Основи маршрутизації. Таблиці маршрутизації та їх структура. Статична та динамічна маршрутизація. Приклади налаштування статичних маршрутів.	7
Тема 6. Технології комутації. Комутація каналів vs комутація пакетів. Принцип роботи комутаторів 2-го рівня (L2). VLAN та їх застосування в корпоративних мережах.	7
Тема 7. Протоколи доступу до середовища. CSMA/CD та CSMA/CA. Розподіл каналів у безпровідних мережах. Проблеми колізій та їх уникнення.	7
Тема 8. Хмарні та віртуальні технології в мережах. Хмарні сервіси (IaaS, PaaS, SaaS). Віртуалізація серверів і мереж. SDN (Software Defined Networking) та його роль у сучасних мережах.	7
Тема 9. Безпека комп'ютерних мереж. Класифікація мережевих атак. Основні засоби захисту (фаєрволи, IDS/IPS, VPN). Безпека бездротових мереж (WPA2/WPA3).	7
Тема 10. Моніторинг та адміністрування мереж. SNMP: моніторинг мережевого обладнання. NetFlow та аналіз мережевого трафіку. Інструменти Wireshark, Nmap.	7
Загальна кількість годин	**72**

Тематика індивідуальних завдань

Курсовий проєкт передбачає виконання індивідуального звіту, розкривати обрану тематику, демонструвати вміння аналізувати інформацію та оформлювати текстові документи відповідно до мети навчальної дисципліни. Здобувач обирає конкретну тему в межах загальної тематики за погодженням з викладачем. Обсяг роботи: 30–40 сторінок основного тексту. Звіт має бути оформлений відповідно до вимог, наведених у літературному джерелі [2]. Завдання виконується протягом навчальних тижнів і подається на перевірку до екзамену.

Теми індивідуального завдання

Тема 1. Історія розвитку комп'ютерних мереж.	
Тема 2. Локальні та глобальні мережі: класифікація та особливості.	
Тема 3. Мережеві топології та методи підключення.	
Тема 4. Фізичні середовища передачі даних.	
Тема 5. Моделі взаємодії відкритих систем (OSI та TCP/IP).	
Тема 6. IP-адресація та підмережі.	
Тема 7. Протоколи маршрутизації.	
Тема 8. VLAN та сегментація мережі.	
Тема 9. Безпека комп'ютерних мереж.	
Тема 10. Хмарні сервіси та віртуалізація мереж.	
Тема 11. DHCP та NAT у сучасних мережах.	
Тема 12. Інструменти адміністрування та моніторингу мереж.	
Загальна кількість годин	**72**

Неформальна освіта

Здобувач має можливість перезарахувати окремі теми або курс шляхом: проходження професійних курсів чи тренінгів, онлайн-освіти, професійних стажувань, у сфері, що відповідає навчальним цілям дисципліни.
Для зарахування необхідно надати: сертифікат (електронний або друкований) про проходження курсу/стажування, опис програми тренінгу із зазначенням змісту тем, обсягу та тривалості..

Рекомендовані курси, тренінги, стажування

1. Онлайн-курс CISCO «CCNA1»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf.
2. Система стандартів з організації навчального процесу. ТЕКСТОВІ ДОКУМЕНТИ У СФЕРІ НАВЧАЛЬНОГО ПРОЦЕСУ. Загальні вимоги до виконання. СТЗВО-ХПІ-3.01-2025.

https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2025/06/STZVO-HPI-3.01-2025-2.pdf
3. Волосюк Ю.В. Комп'ютерні мережі: курс лекцій / Ю. В. Волосюк. - Миколаїв: МНАУ, 2019. - 203 с. https://dspace.mnau.edu.ua/jspui/bitstream/123456789/6377/1/Kompiuterni_merezhi_kurs_lektsii.pdf
4. Kurose James F., Ross Keith W. Computer Networking: A Top-Down Approach. 6th Edition / James F. Kurose, Keith W. Ross. - TX: Pearson, 2012. - 864 p. https://broman.dev/download/Computer%20Networking:%20A%20Top-Down%20Approach%206th%20Edition.pdf
5. CCNAv7: Введення в ресурси курсу Networks [Електронний ресурс]. – Режим доступу: https://www.netacad.com/portal/resources/course-resources/ccna-itn.
6. Bonaventure O. Computer Networking: Principls, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p. https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf
7. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. – Львів: «Новий Світ- 2000», 2020 . – 678 с. https://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.

Додаткова література

8. Технологія Ethernet: лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко. - Львів: "Новий Світ - 2000", 2020. - 196 с. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

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
0,3	0,2	0,1	0,4

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
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

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

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

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + ... + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

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

Здобувач вищої освіти 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	30.08.2025		**Завідувач кафедри** Сергій ЄВСЕЄВ
	30.08.2025		**Гарант ОП** Роман КОРОЛЬОВ