Силабус освітнього компонента
Програма навчальної дисципліни

Безпека Інтернет-речей та сервісів

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Загальна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
1

Мова викладання
Українська, англійська

Викладачі, розробники

ПОГАСІЙ Сергій Сергійович
Serhii.Pohasii@khpi.edu.ua
Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 95, з них патентів на корисну модель 2, 6 монографій, з яких 4 колективних монографій, 4 навчальних посібників, з яких 4 з грифом Міністерства освіти і науки України, 65 статті у закордонних виданнях та фахових виданнях України, з них 11 у наукометричній базі Scopus. Гарант освітньо-наукової програми «Кібербезпека» третього (доктор філософії) рівня вищої освіти, провідний лектор з дисциплін: «Аналогові та цифрові електронні пристрої», «Інтернет речей та сервісів», «Безпека хмарних технологій», «Основи побудови та захисту сучасних операційних систем», «Моделювання систем критичної інфраструктури», «Основи побудови та захисту мікропроцесорних систем», «Безпека смарт-технологій та Інтернет-речей», «Інформаційно-комунікаційні системи у сфері національної безпеки» у студентів бакалавріата та магістратури, Розділ «Інформаційна безпека хмарних сервісів», «Сучасні методи захисту соціо-кіберфізичних систем», «Моделювання механізмів кібербезпеки» для аспірантів.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Безпека Інтернет речей та сервісів" є обов`язковою навчальною дисципліною. Вивчення дисципліни сприяє підготовці фахівців, що володіють здатністю проектувати та розробляти розумні пристрої, що є частиною розумних систем чи інтелектуального середовища; формує стійкі знання та навички у студентів з розробки апаратних компонентів інтелектуальних систем IoT. Оволодіння програмою курсу сприяє виконанню студентами завдань з інших дисциплін, які передбачають наукові та практичні дослідження, щодо застосування результатів проектування систем IoT («Інтернет речей»). Засвоєння дисципліни дозволить майбутнім фахівцям забезпечити необхідний рівень володіння інструментами дослідження і проектування засобів Інтернету речей, що дасть можливість більш глибшого розуміння реалізації його основних функцій.

Мета та цілі дисципліни

Формування системи знань студентів в області Інтернет речей та цифрових технологій, та більш широкої категорії, яка називається цифровим перетворенням на базі яких дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких системи на виробництві та в науковій сфері. В дисципліні основний акцент робиться на розумінні фундаментальних концепцій і механізмів які лежать в основі функціонування Інтернет речей.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ–1. Здатність застосовувати знання у практичних ситуаціях.
КЗ–2. Здатність проводити дослідження на відповідному рівні.
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).
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.

РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.

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)

Безпека безперервності бізнес-процесів.

Особливості дисципліни, методи та технології навчання

Лекції проводяться інтерактивно з використанням мультимедійних технологій. Застосовуються активні форми проведення занять: лекція, лекційне опитування, лабораторні заняття, консультація. На заняттях використовується компетентністний підхід до навчання, акцентується увага на застосуванні он-лайн курсу з розгляду сучасних питань у галузі кібербезпеки.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Історія інтернету речей. Історія розвитку інтернету речей. Перспективи розвитку інтернету речей. Архітектура та ресурси сучасних операційних систем.	4
Тема 2. IoT платформи. Платформа Linux Foundation.Пплатформа AggreGate. Платформа Everyware Cloud.	4
Тема 3. Прості та інтелектуальні сенсори. Уточнення поняття "сенсор". Прості сенсори. Активні та пасивні сенсори. Сенсорно-комп'ютерні системи. Інтелектуальні сенсори. Класифікація інтелектуальних сенсорів.	4
Тема 4. Інтелектуальні акустичні сенсори. Електричні сенсори. Фізичні основи роботи акустичних сенсорів. Приймачі акустичних сигналів.Інтелектуальні акустичні сенсори. Тонометри. Гідролокатори. Риборозшукові ехолоти. УЗ-сенсори відстані. Інтелектуальні портативні сенсори для УЗ досліджень. Физичні основи роботи електричних сенсорів. Резистивні сенсорі. Ємнісні та імпедансні сенсори.	4
Тема 5. Технології Інтернет речей. Передача даних в архітектурі IoT: MQTT.	4
Тема 6. Передача та обробка даних Інтернет речей. Принцип роботи IoT. Зчитування інформації за допомогою датчиків. Передача даних від датчиків до хмарних сховищ. Обробка даних отриманих за допомогою датчиків. Передача даних на інтерфейс користувача. Основи HTTP. WEB API. Основи REST. Явне використання HTTP-методів. Відображення URI, аналогічних структурі каталогів. Технології та протоколи передачі даних на довгі відстані в IoT мережах:LoRaWAN, SigFox,. NB-IoT,. Weightless-P. Технології та протоколи передачі даних на короткі відстані в IoT мережах: Z-Wave, NFC, RFID, Bluetooth Low Energy, Wi-Fi HaLow. Протоколи для передачі повідомлень в IoT.	4
Тема 7. Сенсорні мережі. Стандарти. Класифікація. Технології. Конструктивні особливості. Протоколи.	4

Тема 8. Технології обробки великих даних (Big Data). Принципи роботи з великими даними. Технології і тенденції роботи з Big Data. Обробка і методи аналізу Big Data. Великі дані у промисловості. Алгоритми кластеризації Big Data. Проблеми опрацювання різнотипної інформації.	4
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Packet Tracer — Розгортання та з'єднання пристроїв. Ознайомлення з інструментом Cisco Packet Tracer. Практична робота з підключенням пристроїв IoT, створенням мережевих топологій та налаштуванням взаємодії між елементами системи. **Тема 2. Створення простої домашньої мережі за допомогою Packet Tracer.** Побудова базової моделі «розумного будинку». Налаштування маршрутизаторів, сенсорів і контролерів, перевірка обміну даними між пристроями.	2	0,1
Тема 3. Отримання блимаючого індикатора за допомогою Blockly. Використання візуального програмування для створення простої автоматизації IoT — керування LED-індикатором через Blockly. Знайомство з концепцією подій і логічних умов.	2	0,1
Тема 4. Packet Tracer. Додавання пристроїв IoT у «розумний будинок». Підключення нових IoT-пристроїв (камери, датчики, сигналізації). Налаштування логіки взаємодії між компонентами та симуляція подій у мережі. **Тема 5. Підключення та моніторинг пристроїв IoT.** Практична робота зі створення системи моніторингу IoT-пристроїв. Збір даних, аналіз показників та налаштування оповіщень.	2	0,1
Тема 6. Розумна кімната на базі Raspberry Pi і PL-App. Проєктування системи керування пристроями в межах кімнати з використанням Raspberry Pi. Розробка простих автоматизацій через PL-App.	2	0,1
Тема 7. Основи роботи з Node-RED. Знайомство з платформою Node-RED. Побудова потоків обробки даних IoT, створення логічних зв'язків між сенсорами та діями. **Тема 8. Вивчення протоколів IoT. Протокол MQTT.** Розгортання брокера MQTT, налаштування клієнтів-передплатників та видавців повідомлень. Аналіз особливостей передачі даних і безпеки протоколу.	2	0,1
Тема 9. Використання Web API та Web-сокетів. Робота з API сервісів для керування IoT-пристроями. Використання WebSocket-з'єднань для обміну даними в реальному часі.	2	0,1
Тема 10. Вивчення основ роботи з хмарною платформою IBM Cloud. Реєстрація, налаштування та використання сервісів IBM Cloud для IoT-додатків. Відправлення та зберігання даних із пристроїв.	2	0,1

Тема 11. Вивчення основ роботи з хмарними сервісами для збереження об'єктів. Практичне ознайомлення з хмарними рішеннями для зберігання IoT-даних (наприклад, AWS S3, Azure Blob Storage). Безпечна передача та управління об'єктами у хмарному середовищі.	2	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Архітектура, сенсори та технології Інтернету речей. Дослідити принципи побудови та функціонування систем Інтернету речей (IoT). Розглядаються історія розвитку IoT, основні архітектурні підходи, типи сенсорів (прості, інтелектуальні, акустичні, електричні) та їх роль у формуванні сенсорних мереж. Аналізуються ключові протоколи передачі даних, зокрема MQTT, LoRaWAN, ZigBee, BLE, а також їх застосування у побудові безпечних IoT-систем.	0,1
Тема 2. Обробка даних, IoT-платформи та безпека у хмарних середовищах. У роботі розглядаються питання збору, передавання та обробки даних у системах IoT. Вивчаються принципи функціонування сучасних IoT-платформ (Linux Foundation, AggreGate, Everyware Cloud), особливості протоколів REST і Web API для інтеграції пристроїв, а також методи безпечного зберігання даних у хмарних середовищах. Окрему увагу приділено аналізу технологій Big Data у контексті IoT — їх ролі в аналітиці, прогнозуванні та управлінні процесами.	0,1
Загалом	$\sum_{i=1}^{m} b_i = 0{,}2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Архітектура безпечних IoT-систем. Вивчення рівнів архітектури IoT (пристрої, мережа, хмара, застосунки) та принципів побудови безпечних з'єднань між компонентами.	8
Тема 2. Протоколи безпеки в IoT: TLS, DTLS, CoAP, MQTT-SN. Аналіз особливостей криптографічного захисту та аутентифікації в протоколах обміну даними для IoT.	8
Тема 3. Загрози та вразливості Інтернету речей. Дослідження основних типів атак на IoT-пристрої: DoS, Man-in-the-Middle, ботнети, експлуатація відкритих портів.	7
Тема 4. Безпека пристроїв з обмеженими ресурсами. Методи оптимізації криптографічних алгоритмів для мікроконтролерів та сенсорів.	7

Тема 5. Автентифікація користувачів і пристроїв у IoT-середовищах. Механізми управління ідентичністю, сертифікація та розподіл ключів.	7
Тема 6. Захист конфіденційності користувачів у системах IoT. Аналіз ризиків збору персональних даних і методи мінімізації витоку інформації.	7
Тема 7. IoT у промислових системах (IIoT): безпека SCADA та PLC. Вивчення специфіки промислового Інтернету речей і загроз для критичної інфраструктури.	7
Тема 8. Хмарні сервіси для IoT та їх безпека. Огляд хмарних платформ (AWS IoT, Microsoft Azure IoT, IBM Cloud) та засобів контролю доступу.	7
Тема 9. Етичні аспекти використання Інтернету речей. Розгляд питань приватності, прав користувачів та відповідальності за використання IoT-технологій.	7
Тема 10. Майбутнє IoT: штучний інтелект та автономні системи. Використання машинного навчання для автоматичного виявлення аномалій і кіберзагроз у мережах IoT.	7
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 «Introduction to IoT and Digital Transformation, Exploring IoT with Cisco Packet Tracer (5)»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. David Rose, Enchanted Objects: Design, Human Desire, and the Internet of Things, 2015.
https://responsiveobjects.wordpress.com/wp-content/uploads/2016/01/enchanted-objects_-design-human-desire-and-the-internet-of-things-rose-david.pdf
2. Баранов А.А., Інтернет речей: теоретико-методологічні засади правового регулювання. Том І. Сфери застосування, ризики та бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
https://jurkniga.ua/nternet-rechey-teoretiko-metodologchn-osnovi-pravovogo-regulyuvannya-tom--sferi-zastosuvannya-riziki--barri-problemi-pravovogo-regulyuvannya/
3. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.
https://ru.scribd.com/document/441966460/the-internet-of-things-the-mit-press-essential-knowledge-series-by-samuel-greengard
4. Cuno Pfister, Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud (Make: Projects) 1st Edition, ASIN: B00COVJUGI, 2011, 194 P.

https://www.openhacks.com/uploadsproductos/getting_started_with_the_internet_of_things_pachube_client.pdf
5. Erik Brynjolfsson and Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 1st Edition, ASIN: B00D97HPQI, 2014, 320 P.
http://digamo.free.fr/brynmacafee2.pdf
6. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.
https://www.perlego.com/book/2433384/digital-transformation-survive-and-thrive-in-an-era-of-mass-extinction-pdf
7. 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.
8. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. "Новий Світ-2000", 2023. – 657 с.
https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover.

Додаткова література

9. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P.
https://pdfcoffee.com/machine-learning-the-new-ai-alpaydin-2016pdf-pdf-free.html
10. Nayan B. Ruparelia, Cloud Computing (MIT Press Essential Knowledge series), ASIN: B01FLE5JH8, 2016, 258 P.
https://s3.amazonaws.com/arena-attachments/911381/0ea8a9793158a95d9b91911e49240a43.pdf
11. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
12. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
13. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
14. 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.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/.pdf2.pdf.

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	0,2		

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
K – 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, K, 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**
Ольга КОРОЛЬ