Силабус освітнього компонента
Програма навчальної дисципліни

Безпека смарт-технологій

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
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна, заочна

Семестр
2

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-науової 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 смарт-технологій" є вибірковою навчальною дисципліною. Вивчення дисципліни базується на засвоєнні основ розробки та програмування пристроїв, які працюють з використанням смарт-технологій та технологій Інтернету речей. При цьому пристрої IoT розглядаються як сукупність технічних, інформаційних та програмних засобів, призначених для вирішення широкого кола завдань у різних галузях економіки, освіти, промисловості тощо.

Мета та цілі дисципліни

Формування системи знань студентів в області смарт-технологій та Інтернет речей, та більш широкої категорії, що називається цифровим перетворенням. На базі цих знань дипломований фахівець зможе забезпечувати розробку, застосування і експлуатацію таких систем на виробництві та в науковій сфері. В дисципліні основний акцент направлений на розуміння фундаментальних концепцій і механізмів, які лежать в основі функціонування інтернет-речей.

Формат занять

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

Компетентності

КЗ1. Здатність застосовувати знання у практичних ситуаціях.
КЗ2. Здатність проводити дослідження на відповідному рівні.
КЗ3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
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.
КФ2. 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.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
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.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7. Здатність 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.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно 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.
РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
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 – 16 год., лабораторні роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Веб безпека, Технології програмування, Математичні основи криптології та криптоаналіз, Менеджмент інформаційної безпеки, Моделювання систем критичної інфраструктури.

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. Історія та перспективи Інтернету речей (IoT). Історія розвитку IoT. Основні сфери застосування: промисловість, медицина, транспорт, енергетика, сільське господарство, роздрібна торгівля, розумне місто, уряд і армія. Перспективи розвитку та ринок IoT.	2
Тема 2. Основи смарт-технологій. Визначення та принципи роботи смарт-технологій. Дані, інформація, знання. Приклади практичної реалізації смарт-технологій у різних сферах.	2
Тема 3. Апаратура і сенсорні системи. Датчики, кінцеві точки, пристрої введення/виведення. Джерела живлення та управління енергією. Функціональні приклади (TI SensorTag CC2650 та інші).	2
Тема 4. Теорія комунікацій та протоколи IoT. Теорія комунікації та інформації, межі бітрейту, радіочастотна інтерференція, узкополосна та широкосмугова передача. Протоколи передачі даних: MQTT, CoAP, AMQP, STOMP. Архітектура WPAN, WLAN, Thread, 6LoWPAN.	2
Тема 5. Телекомунікаційні системи та мережеві технології. Стільникові технології 3G/4G/5G, NB-IoT. LoRa, LoRaWAN, Sigfox. Маршрутизатори, шлюзи, VLAN, VPN, QoS, SDN.	2
Тема 6. Архітектура і топологія IoT-систем.	2

Структура IoT-систем, хмарні та туманні обчислення. Публічні, приватні та гібридні хмари, OpenStack, OpenFog, EdgeX Foundry. Комутація між пристроями та мережею.	
Тема 7. Аналіз даних і машинне навчання в IoT. Збір та обробка даних у IoT. Моделі машинного навчання для IoT. Використання аналітики у хмарних і туманних платформах.	2
Тема 8. Безпека та стандарти смарт-технологій. Кібербезпека IoT-пристроїв, фізична та апаратна безпека, криптографія. Архітектура захищеного програмного периметру. Консорціуми та спільноти: Bluetooth SIG, Zigbee Alliance, LoRa Alliance, Open Connectivity Foundation, IEEE IoT, OpenFog та інші.	2
Загальна кількість годин	**16**

Лабораторні заняття
Контрольні роботи

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти b	Вагові коефіцієнти a
Тема 1. Архітектура, протоколи та апаратна база IoT. Оцінити знання студентів з апаратної частини IoT, основних протоколів і мережевих технологій, здатність пояснити структуру та взаємодію компонентів IoT-систем.			0,1
Тема 2. Безпека, аналіз даних і хмарні платформи в IoT. Перевірити знання студентів щодо безпеки смарт-технологій, застосування аналітики та машинного навчання в IoT, а також розуміння стандартів і організаційних практик у галузі IoT.			0,1
Тема 1. Packet Tracer – Розгортання та з'єднання пристроїв. Студенти навчаються створювати віртуальні мережі, підключати різні пристрої та перевіряти їхню взаємодію у середовищі Cisco Packet Tracer.	6		0,2
Тема 2. Створення простої мережі з використанням Packet Tracer. Практична робота з побудови базової мережі, налаштування IP-адресації та перевірки зв'язку між пристроями.	6		0,2
Тема 3. Підключення та моніторинг пристроїв IoT. Встановлення і налаштування IoT-пристроїв у Packet Tracer, моніторинг їхніх статусів та взаємодії з мережею.	5		0,1
Тема 4. Розумна кімната на базі Raspberry Pi і PL-App. Розробка практичного IoT-рішення для керування освітленням, температурою та іншими сенсорами кімнати за допомогою Raspberry Pi та PL-App.	5		0,1
Тема 5. Конвергентна мережа і взаємозв'язок речей. Вивчення концепції конвергентних мереж, взаємозв'язку IoT-пристроїв, питань безпеки та основних технологій автоматизації Cisco IoT.	5		0,1
Тема 6. Побудова проекту IoT-рішення. Студенти проходять повний цикл розробки IoT-проекту: планування, вибір обладнання та протоколів, розробка прототипу та тестування готового рішення.	5		0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{m} b_i = 0{,}2$	$\sum_{i=1}^{n} a_i = 0{,}8$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Основи сенсорних технологій та датчиків IoT. Види сенсорів, принципи їх роботи, характеристики та застосування в розумних системах.	8
Тема 2. Енергетична ефективність IoT-пристроїв. Методи економії енергії, джерела живлення, накопичувачі та відновлення енергії.	8
Тема 3. Протоколи бездротового зв'язку IoT. Bluetooth, Zigbee, Z-Wave, LoRa, Sigfox: принципи роботи, порівняння та сфери застосування.	7
Тема 4. Стек протоколів IP для IoT. 6LoWPAN, Thread, MQTT, CoAP: архітектура, топологія, адресація та маршрутизація.	7
Тема 5. Хмарні та туманні обчислення для IoT. Моделі обчислень, архітектура хмарних платформ, публічні та приватні хмари, OpenStack, Edge/Fog Computing.	7
Тема 6. Аналіз даних та машинне навчання в IoT. Методи збору та обробки даних, використання ML-моделей для прогнозування та оптимізації IoT-систем.	7
Тема 7. Основи кібербезпеки IoT. Захист IoT-пристроїв, фізична та апаратна безпека, криптографія, вразливості та методи протидії атакам.	7
Тема 8. Програмування IoT-пристроїв. Основи роботи з Raspberry Pi, Arduino та іншими платформами, використання мов Python, C/C++ для створення IoT-додатків.	7
Тема 9. Автоматизація та інтеграція IoT-систем. Сценарії автоматизації, інтеграція з домашніми та промисловими системами, взаємодія через API та вебсервіси.	7
Тема 10. Стандарти та консорціуми IoT. Bluetooth SIG, Zigbee Alliance, LoRa Alliance, Open Connectivity Foundation, OpenFog, IEEE IoT: стандартизація, сумісність та рекомендації.	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

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Баранов А.А., Інтернет речей: теоретико-методологічні основи правового регулювання. Том І. Сфери застосування, ризики і бар'єри, проблеми правового регулювання, ISBN: 978-966-937-513-1, 2018, 344с.
2. Грінгард С. Інтернет речей. Київ: Книжковий клуб «Клуб сімейного дозвілля», 2018. 176 с. 2. Посібник з Node-Red. [Електронний ресурс]. – Режим доступу : https://github.com/pupenasan/NodeREDGuidUKR.
3. Пархоменко А.В. та ін. Програмно-апаратна платформа для навчання технологіям Інтернету речей: навч. посіб. Запоріжжя: Дике Поле, 2017. 120 с. Електронний ресурс]. – Режим доступу : https://eir.zp.edu.ua/items/920b4a42-219b-4f0d-beed-116ff69abba2
4. Lea P. IoT and Edge Computing for Architects: Implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security, 2nd Edition. Pact Publishing Ltd., 2020. 608 p. [Електронний ресурс]. – Режим доступу : https://www.perlego.com/book/1388466/iot-and-edge-computing-for-architects-implementing-edge-and-iot-systems-from-sensors-to-clouds-with-communication-systems-analytics-and-security-2nd-edition-pdf
5. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
6. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с. [Електронний ресурс]. – Режим доступу : http://kist.ntu.edu.ua/textPhD/tzi.pdf
7. Amazon Web Services (AWS) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/amazon-aws-security/.
8. Microsoft Azure (Azure) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/microsoft-azure-security/.
9. Google Cloud Platform (GCP) [Електронний ресурс]. – Режим доступу : https://www.checkpoint.com/solutions/google-cloud-platform-security/.
10. Kali Linux [Електронний ресурс]. – Режим доступу : https://www.kali.org/.

Додаткова література

11. Serpanos D., Wolf M.C.Internet-of-Things (IoT) Systems. Architectures, Algorithms, Methodologies. Springer, 2018. 95 p. (eBook) [Електронний ресурс]. – Режим доступу : https://doi.org/10.1007/9783-319-69715-4.
12. Khan J.Y., Yuce M.R. Internet of Things (IoT): Systems and Applications 1st Edition. Jenny Stanford Publishing Pte, Ltd., 2019. 340 p. [Електронний ресурс]. – Режим доступу : https://books.google.com.ua/books/about/Internet_of_Things_IoT.html?id=S6S3vAEACAAJ&redir_esc=y
13. Cloud Computing Security [Електронний ресурс]. – Режим доступу : https://www.tutorialspoint.com/cloud_computing/cloud_computing_security.htm.
14. Computer Network Security [Електронний ресурс]. – Режим доступу : https://www.javatpoint.com/computer-network-security.
15. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
16. 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. [Електронний ресурс]. – Режим доступу : https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
17. 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. [Електронний ресурс]. – Режим доступу :

https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.
18. Security of Linux operating system: laboratory workshop / S. Yevseiev, S. Pogasiy, A. Goloskokova, O. Shmatko, M. Melnik (Кібербезпека: безпека операційної системи Linux: лабораторний практикум: навчальний посібник для студентів вищих навчальних закладів англійською мовою / Євсеєв С.П., Погасій С.С., Голоскокова А.О., Шматко О.В., Мельник М.О. – Львів: Видавництво «Новий Світ – 2000», 2021. – 256 с. [Електронний ресурс]. – Режим доступу : 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
0,8	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:

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

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