Силабус освітнього компонента
Програма навчальної дисципліни

Безпека інтернет-речей

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
7

Мова викладання
Українська

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" є обов`язковою навчальною дисципліною. Дисципліна спрямована на вивчення основних концепцій та підходів до розробки та впровадження

надійних, безпечних систем IoT, дослідження моделей та методів забезпечення надійності та забезпечення безпеки та оцінки систем на основі IoT, ознайомлення з процесом тестування та пошуку вразливостей в пристроях IoT.

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 роботи, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

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.
СК1. Здатність використовувати безпекові режими під час виконання службових обов'язків.
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.
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.
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.
РН9. Вміти використовувати безпекові режими під час виконання службових обов'язків.
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 – 32 год., лабораторні роботи – 16 год., самостійна робота –72 год.

Передумови вивчення дисципліни (пререквізити)

Розробка веб-додатків, Основи побудови та захисту мікропроцесорних систем.

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. Тема 1. Історія інтернету речей. Історія розвитку інтернету речей. Перспективи розвитку інтернету речей. Індустрія і виробництво. Споживачі. Роздрібна торгівля, фінанси і маркетинг. Медицина. Транспорт і логістика. Сільське господарство та навколишнє середовище. Енергетика. Розумне місто. Уряд і армія. Архітектура та ресурси сучасних операційних систем.	2
Тема 2. Датчики, кінцеві точки і системи живлення. Злиття датчиків. Пристрої введення. Пристрої виведення. Функціональні приклади (всі разом). Функціональний приклад - TI SensorTag CC2650. Між	2

датчиком і контролером. Джерела енергії та управління живленням. Відтворення електроенергії. Сховище енергії.	
Тема 3. Теорія комунікації та інформації. Теорія комунікації. Радіочастотна енергія і теоретичний діапазон. Радіочастотна інтерференція. Теорія інформації. Межі бітрейта і теорема Шеннона-Хартлі. Частота бітових помилок. Вузькосмуговий і широкосмуговий зв'язок. Радіоспектр. Керуюча структура.	2
Тема 4. Бездротова персональна мережа (WPAN) не на основі IP. Стандарти бездротової персональної локальної мережі. Стандарти 802.15. Bluetooth.IEEE 802.15.4. Zigbee.Z-Wave.	2
Тема 5. WPAN і WLAN на базі IP. Протокол інтернету і протокол управління передачею. Роль протоколу IP в інтернеті речей. WPAN з IP - 6LoWPAN. WPAN з IP - Thread. Архітектура і топологія Thread. Стек протоколу Thread Маршрутизація Thread. Адресація Thread. Виявлення сусіда Протоколи IEEE 802.11.	2
Тема 6. Системи та протоколи телекомунікації (ГВС). Функціональна сумісність пристроїв стільникового зв'язку. Стандарти та модель управління. Технології доступу стільникового зв'язку. Категорії абонентського обладнання 3GPP. Росподіл спектра і смуг частот в 4G LTE. Топологія та архітектура мережі 4G LTE. Стек протоколів мережі E-UTRAN 4G LTE. Географічні області 4G LTE, потоки даних і процедури передачі обслуговування. Структура пакета 4G LTE. Категорії 0, 1, M1 і NB-IoT. 5G LoRa і LoRaWAN. Фізичний рівень LoRa. Рівень MAC LoRaWAN. Топологія LoRaWAN. Короткий опис LoRaWAN. Sigfox. Фізичний рівень Sigfox. Рівень MAC Sigfox. Стек протоколу Sigfox. Топологія Sigfox.	2
Тема 7. Маршрутизатор і шлюзи. Функції маршрутизації. Функції шлюзу. Маршрутизація відмов стійкість і позасмугове управління. VLAN.VPN. Управління швидкістю трафіку і QoS. Функції безпеки. Метрики і аналітика. Обробка на краю. Програмне мережеве взаємодія. Архітектура SDN. Традиційна міжмережева взаємодія. Переваги SDN.	2
Тема 8. IoT-протоколи передачі даних від граничного пристрою в хмару. Протоколи. MQTT. MQTT-SN. Архітектура і топологія MQTT-SN. Обмежений прикладної протокол. Деталі архітектури CoAP. Інші протоколи. STOMP. AMQP. Зведення і порівняння протоколів.	2
Тема 9. Топологія хмарних і туманних обчислень. Модель хмарних сервісів. Публічне, приватна і гібридна хмара. Хмарна архітектура OpenStack. Keystone. Обмеження хмарних архітектур для IoT. Туманні обчислення.	4
Тема 10. Аналіз даних і машинне навчання в хмарних і туманних платформах. Простій аналіз даних в інтернеті речей. Машинне навчання в інтернеті речей. Моделі машинного навчання.	4
Тема 11. Безпека інтернет речей. Загальновживані поняття кібербезпеки пов'язані з атакою. Анатомія кібератак на IoT-пристрої. Фізична і апаратна безпека. Криптографія. Архітектура про програмно-обумовленого периметра. Рекомендації щодо захисту IoT-пристроїв.	4
Тема 12. Консорціуми і спільноти.	4

Консорціуми з персональним мереж. Bluetooth SIG. Thread Group. Альянс Zigbee Консорціуми за протоколами Open Connectivity Foundation і Allseen Alliance. Консорціуми з глобальних обчислювальних мереж. Weightless SIG . LoRa Alliance. Інженерний рада інтернету. Wi-Fi Alliance Консорціуми з туманним і граничним обчислень. OpenFog. EdgeX Foundry. Спеціалізовані організації Консорціум промислового інтернету. Інститут інженерів з електротехніки та електроніки IoT (IEEE IoT).	
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 інтерфейсом Cisco Packet Tracer. Створення робочого середовища для IoT-пристроїв. Розгортання маршрутизаторів, комутаторів та кінцевих пристроїв. Налаштування базового з'єднання між пристроями. Виявлення можливих уразливостей при неправильній конфігурації.	4	0,1
Тема 2. Створення простої мережі з використанням Packet Tracer. Проєктування локальної мережі з IoT-пристроями. Присвоєння IP-адрес та базова конфігурація TCP/IP. Перевірка зв'язності мережі (ping, traceroute). Використання протоколів DHCP та DNS. Аналіз мережевих ризиків у простих топологіях.	4	0,1
Тема 3. Підключення та моніторинг пристроїв IoT. Підключення датчиків та «розумних» пристроїв до мережі. Використання IoT Monitor у Packet Tracer. Взаємодія між IoT-пристроями (керування через додаток). Моніторинг роботи пристроїв та журнал подій. Виявлення та попередження несанкціонованого доступу.	2	0,1
Тема 4. Розумна кімната на базі Raspberry Pi і PL-App. В Ознайомлення з можливостями Raspberry Pi у IoT. Підключення сенсорів та керованих пристроїв. Програмування логіки роботи розумної кімнати (Python). Використання PL-App для автоматизації процесів. Виявлення ризиків безпеки у смарт-просторах.	2	0,1
Тема 5. Конвергентна мережа і взаємозв'язок речей, питання безпеки та основні стовпи Cisco IoT, технології автоматизації. Архітектура конвергентної мережі IoT. Протоколи обміну даними в IoT (MQTT, CoAP). Основні стовпи Cisco IoT (безпека, масштабованість, аналітика). Приклади атак на конвергентні мережі. Технології автоматизації для управління IoT-пристроями.	2	0,1
Тема 6. Побудова проєкту створення рішення інтернету речей, від планування до прототипування. Аналіз задачі та вимог до IoT-рішення. Вибір архітектури та технологій. Планування структури мережі IoT. Реалізація прототипу в Packet Tracer або на реальних пристроях.	2	0,1

Тестування, виявлення ризиків і пропозиції з удосконалення безпеки.		
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Основи побудови та захисту IoT-мереж. Архітектура інтернету речей: рівні, компоненти, приклади застосування. Типи IoT-пристроїв та їх роль у мережі. Протоколи комунікації в IoT (MQTT, CoAP, HTTP, AMQP). Загрози безпеці в IoT-середовищі: класифікація та приклади. Методи автентифікації та авторизації в IoT. Шифрування і захист передавання даних у IoT-мережах.	0,2
Тема 2. Атаки та захист в системах інтернету речей. Основні кіберзагрози для IoT (DDoS, підміна даних, перехоплення трафіку). Вразливості протоколів IoT та приклади їх використання зловмисниками. Методи моніторингу та виявлення атак на IoT-пристрої. Захист інфраструктури інтернету речей: принципи та інструменти. Рекомендації Cisco IoT Security Framework. Приклади реальних атак на IoT-системи та способи їхнього запобігання.	0,2
Загалом	$\sum_{i=1}^{m} b_i = 0{,}4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Протоколи зв'язку в IoT. Характеристика MQTT, CoAP, AMQP, Zigbee, Z-Wave. Порівняння їх ефективності та безпеки.	11
Тема 2. Моделі загроз для IoT-систем. STRIDE та інші моделі аналізу загроз. Приклади застосування для IoT-рішень.	11
Тема 3. Шифрування та криптографічні методи в IoT. Легкі криптографічні алгоритми для обмежених пристроїв. Використання симетричних і асиметричних методів.	10
Тема 4. Захист IoT-пристроїв на рівні апаратного забезпечення. Безпечне завантаження (Secure Boot). Трастові модулі (TPM) та їх застосування.	10
Тема 5. Аналіз вразливостей IoT-пристроїв. Використання сканерів безпеки (Nmap, Nessus). Методи пентесту IoT.	10
Тема 6. Хмарні сервіси для IoT та їх безпека. AWS IoT, Azure IoT Hub, Google IoT Core. Ризики та засоби захисту даних у хмарних платформах.	10
Тема 7. Стандарти та нормативне регулювання безпеки IoT. ISO/IEC 30141, ETSI EN 303 645. Рекомендації NIST щодо IoT Security.	10
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 Networking with Cisco Packet Tracer»
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. Євсєєв 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
0,6	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:

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

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

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

розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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