



Технології та інструменти кібер-фізичних систем

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

Рівень вищої освіти	<i>Другий (магістерський)</i>
Галузь знань	<i>12 Інформаційні технології</i>
Спеціальність	<i>124 Системний аналіз</i>
Освітня програма	<i>Системний аналіз і управління</i>
Статус дисципліни	<i>Вибіркова</i>
Форма навчання	<i>очна(денна)</i>
Рік підготовки, семестр	<i>5 курс, осінній семестр</i>
Обсяг дисципліни	<i>4 кредити (лекції 36 год., практикум 18 год., СРС 66 год.)</i>
Семестровий контроль/ контрольні заходи	<i>Залік</i>
Розклад занять	<i>http://rozklad.kpi.ua/</i>
Мова викладання	<i>Українська</i>
Інформація про керівника курсу / викладачів	<i>Лектор: к.т.н., доц. Голінко Ігор Михайлович, golinko.igor@iit.kpi.ua Практичні / Семінарські: к.т.н., доц. Голінко Ігор Михайлович</i>
Розміщення курсу	<i>Google classroom</i>

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Дисципліна «Технології та інструменти кібер-фізичних систем» є вибірковою дисципліною навчального плану магістрів із спеціальності «Системний аналіз». Дисципліна надає можливість студентам ознайомитися з теорією і практикою розробки багатовимірних систем управління, які базуються на застосуванні технології промислового Інтернету речей (IIoT). Технологія промислового Інтернету речей (IIoT) є відгалуженням від технології Інтернету речей (IoT), яка є однією із найперспективніших технологій останніх років. За допомогою технологій КФС створюються сотні нових продуктів, що призводить до появи нових компаній на ринку. Людство по всьому світу користуються такими продуктами кожен день. У чималій кількості домівок вже встановлені системи "розумного будинку", в які інтегровані десятки датчиків. Переваги технології кібер-фізичних систем (КФС) можна побачити в різних сферах діяльності людини.

Метою дисципліни є формування у студентів компетентностей та підготовка фахівця, здатного вирішувати прикладні задачі із проектування та супроводження функціонування КФС та вибору технології реалізації та адміністрування мережі промислового Інтернету речей.

Предмет дисципліни - методологія діджиталізації фізичних процесів та технічних пристроїв, які оснащені вбудованими технологіями для взаємодії один з одним, або із зовнішнім середовищем, яка розглядає організацію таких КФС як явище, що здатне перебудувати економічні та суспільні процеси і частково виключає участь людини із процесу управління.

Метою кредитного модуля є формування у студентів наступних *компетентностей*:

- здатність до проектування технічних систем, які в Інтернет-середовищі реалізують заданий функціонал управління фізичними процесами;
- здатність виконувати аналіз та синтез багатовимірних систем управління на базі математичної формалізації фізичних процесів.

Програмні результати навчання:

- використання математичних моделей та методів для розподілу функціоналу між комп'ютеризованими пристроями та їх взаємодії із фізичним середовищем;
- вміння перетворювати звичайні технічні пристрої в Інтернет речі, реалізовувати взаємодію Інтернет речей між собою та фізичними процесами.

2. Пререквізити та постреквізити дисципліни

Пререквізити: використовувати базові знання інформаційних систем та технологій, навички конфігурації безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення математичних моделей, алгоритмів та програмного забезпечення для розв'язання задач проектування КФС.

Постреквізити: вміти проектувати, розробляти, налагоджувати та вдосконалювати системне, комунікаційне, математичне та програмно-апаратне забезпечення інформаційних систем та технологій КФС, вміти управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

Дисципліна належить до вибіркових навчальних дисциплін. Під час вивчення дисципліни використовуються знання з попередніх модулів бакалаврської підготовки: програмування та алгоритмічні мови; теорія керування; основи системного аналізу; моделювання складних систем; архітектура обчислювальних систем. Результати вивчення дисципліни застосовуються у подальшій практичній роботі та при підготовці магістерської дисертації.

3. Зміст навчальної дисципліни

Розділ 1. Основи кібер-фізичних систем

Тема 1.1. Використання Інтернету речей.

Тема 1.2. Складові Інтернету майбутнього.

Тема 1.3. Історія виникнення Інтернету речей та поняття кібер-фізичної системи

Тема 1.4. Екосистема Інтернету речей

Тема 1.5. Архітектура та ключові модулі Інтернету речей

Розділ 2. Еталонна модель IoT

Тема 2.1. Стандарти сумісності IoT

Тема 2.2. Еталонна модель IoT від MCE-T

Тема 2.3. Еталонна модель від Всесвітнього форуму IoT

Тема 2.4. Модель NIST Special Publication 800-183

Тема 2.5. Модель Industrial Internet of Things Reference Architecture

Розділ 3. IoT платформи

Тема 3.1. Поняття IoT платформа

Тема 3.2. Платформа Linux Foundation

Тема 3.3. Платформа AggreGate

Тема 3.4. Платформа Everyware Cloud

Розділ 4. Основні види сенсорів Інтернету речей

Тема 4.1. Прості сенсори

Тема 4.2. Інтелектуальні сенсори

Розділ 5. Технології комунікації в IoT мережах

Тема 5.1. Технології та протоколи передачі даних на довгі відстані в IoT мережах

Тема 5.2. Технології та протоколи передачі даних на короткі відстані в IoT мережах

Тема 5.3. Маршрутизатори і шлюзи

Тема 5.4. Протоколи IoT передачі даних від мережевого пристрою в хмару

Розділ 6. Огляд основних технологій кібер-фізичних систем

Тема 6.1. Інтернет речей (IoT, IIoT)

Тема 6.2. Цифрові двійники (Digital Twins)

Тема 6.3. Великі дані (Big Data)

Тема 6.4. Машинне навчання (Machine Learning)

Тема 6.5. Віртуальна реальність

Тема 6.6. Доповнена реальність

Розділ 7. Цифрові двійники для промислового використання

Тема 7.1. Еталонна модель цифрового двійника від Industrial Internet Consortium

Тема 7.2. Зв'язки між цифровими двійниками в кіберсистемах

Тема 7.3. Цифровий двійник в життєвому циклі об'єкту управління

Розділ 8. Системний підхід до розробки математичного забезпечення цифрового двійника

Тема 8.1. Методи та алгоритми фільтрації, що застосовуються на пограничних пристроях КФС

Тема 8.2. Методи та алгоритми аналізу великих даних, що застосовуються у хмарному середовищі КФС

Тема 8.3. Розробка математичної моделі цифрового двійника для рівня бізнес-аналітики об'єкта

Тема 8.4. Розробка математичної моделі цифрового двійника для рівня використання об'єкта

Тема 8.5. Розробка математичної моделі цифрового двійника для рівня функціонування об'єкта

Розділ 9. Безпека кібер-фізичних систем

Тема 9.1. Актуальність питання безпеки кібер-фізичних систем

Тема 9.2. Основні загрози та напрями кібератак

Тема 9.3. Методи та засоби кіберзахисту

4. Навчальні матеріали та ресурси

Базова література

1. Панкратова Н.Д. Системний аналіз: теорія та застосування: підруч. / Н.Д. Панкратова. - Київ: Наук. думка, 2018. - 348 с. ISBN:978-966-00-1643-9
2. Жураковський Б.Ю. Технології інтернету речей. [Електронний ресурс]: навч. посіб. / Б.Ю. Жураковський, І.О. Зенів. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 271 с. [Електронний ресурс]. - Режим доступу: <https://ela.kpi.ua/handle/123456789/42078>.
3. Грудзинський Ю.Є. Технології сучасних кібер-фізичних систем. [Електронний ресурс]: навч. посіб. / Ю.Є. Грудзинський. – Київ : КПІ ім. Ігоря Сікорського, 2020. – 327 с. [Електронний ресурс]. - Режим доступу: <https://ela.kpi.ua/handle/123456789/43394>
4. Пупена О.М. Технології Індустрії 4.0: конспект лекцій / О.М. Пупена, – К.: НУХТ, 2020. – 81 с. [Електронний ресурс]. - Режим доступу: <http://library.nuft.edu.ua/ebook/file/100.106.pdf>

Додаткова література

5. Nataliya Pankratova, Igor Golinko Digital Twin Simulation for Cyber-Physical Systems on Electric Heater Example // System Analysis & Intelligent Computing, 2022. P. 22-77.
6. Голінко І.М. Технічні засоби автоматизації [Електронний ресурс]: навч. посіб. / Укладач: І.М. Голінко. – Київ: КПІ ім. Ігоря Сікорського, 2020. –63 с. [Електронний ресурс]. - Режим доступу: <https://ela.kpi.ua/handle/123456789/41518>
7. Perry Lea Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security. Packt Publishing, 2018. P. 526. ISBN 978-1-78847-059-9.
8. S. Li, L.D. Xu Securing the Internet of Things. Syngress, 2017. p. 154. ISBN 9780128045053.

9. Микитишин А.Г. Телекомунікаційні системи та мережі: навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк– Тернопіль: Тернопільський нац. техн. ун-т імені Івана Пулюя, 2017. – 384 с.
10. Tripathy B. Internet of Things (IoT): Technologies, Applications, Challenges and Solutions (англ.) / B. Tripathy, J. Anuradha. – Florida: CRC Press, 2017. P. 334
11. Джексон Р.Г. Новейшие датчики / - Москва, Техносфера, 2007. -384 с.
12. Digital Twins for Industrial Applications / An Industrial Internet Consortium White Paper, Version 1.0, 2020. P. 20. [Електронний ресурс]. - Режим доступу: https://www.iiconsortium.org/pdf/IIC_Digital_Twins_Industrial_Apps_White_Paper_2020-02-18.pdf
13. Бідюк П.І. Інформаційна система підтримки прийняття рішень для прогнозування фінансово-економічних процесів на основі структурно-параметричної адаптації моделей // П.І. Бідюк, О.М. Трофимчук, А.В. Федоров / Наукові вісті НТУУ "КПІ", 2011. № 6. с. 42-53.

Навчальний контент

5. Методика опанування навчальної дисципліни (освітнього компонента)

Методи навчання включають.

1. Лекції: мультимедійні презентації з ілюстрацією прикладів на дошці.
2. Комп'ютерний практикум заняття: групові виконання завдань у навчальній лабораторії, консультації.

Перелік тем лекційних занять

№ заняття	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
1.	<p>Лекція 1. Складові майбутнього Інтернету Використання Інтернету речей. Складові Інтернету майбутнього. Інтернет речей. Інтернет людей. Інтернет контенту. Інтернет сервісу. Література: 2, 4, 10. Самостійна робота: вивчення складових Інтернет мережі майбутнього.</p>
2.	<p>Лекція 2. Основи кібер-фізичних систем Історія виникнення Інтернету речей та основні поняття кібер-фізичної системи. Базові визначення в IoT. Інтернет речей в промисловості. Екосистема Інтернету речей. Архітектура Інтернету речей та ключові модулі Інтернету речей (рівень датчиків, мережевий рівень, рівень обробки даних, рівень додатків). Література: 2, 3, 7, 8. Самостійна робота: вивчення основ кібер-фізичних систем.</p>
3.	<p>Лекція 3. Еталонна модель IoT Стандарти сумісності IoT. Еталонна модель IoT від MCE-T. Еталонна модель від Всесвітнього форуму IoT. Модель NIST Special Publication 800-183. Модель Industrial Internet of Things Reference Architecture. Література: 2, 7, 8. Самостійна робота: вивчення еталонної моделі IoT.</p>
4.	<p>Лекція 4. IoT платформи Поняття IoT платформи. Платформа Linux Foundation. Платформа AggreGate. Платформа Evereware Cloud.</p>

№ заняття	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
	Література: 2. Самостійна робота: вивчення IoT платформ, основні поняття про мікросистемні технології.
5.	Лекція 5. Прості та інтелектуальні сенсори Прості сенсори. Активні та пасивні сенсори. Фізичні основи роботи електричних сенсорів. Резистивні сенсори. Ємнісні та імпедансні сенсори. Сенсори лінійного переміщення. Сенсори кутового переміщення. Література: 2, 3, 11. Самостійна робота: вивчення простих та інтелектуальних сенсорів.
6.	Лекція 6. Інтелектуальні сенсори Сенсорно-комп'ютерні системи. Інтелектуальні сенсори. Класифікація інтелектуальних сенсорів. Інтелектуальні акустичні сенсори. Деформаційні інтелектуальні сенсори. Принципи роботи глобальної системи орієнтування. Сенсори GPS. Література: 2, 3, 11. Самостійна робота: вивчення принципів роботи глобальної системи орієнтування і сенсорів GPS.
7.	Лекція 7. Технології передачі даних на довгі відстані в IoT мережах Технології: LoRaWAN, SigFox, Weightless-P. Стандарт NB-IoT. Література: 2, 3. Самостійна робота: вивчення протоколів та інтерфейсів Інтернету речей.
8.	Лекція 8. Технології передачі даних на короткі відстані в IoT мережах Технології: Z-Wave, NFC, RFID, Bluetooth Low Energy, Wi-Fi HaLow. Сенсорні мережі. Література: 2, 3. Самостійна робота: вивчення протоколів та інтерфейсів Інтернету речей.
9.	Лекція 9. Маршрутизатори і шлюзи Функції маршрутизації. Моделі IoT шлюзів від світових брендів. Література: 2, 3. Самостійна робота: засвоєння принципів функціонування IoT шлюзів.
10.	Лекція 10. Протоколи IoT передачі даних від мережевого пристрою в хмару Протокол MQTT. Інші IoT протоколи. Література: 2 - 4. Самостійна робота: вивчення протоколів IoT передачі даних.
11.	Лекція 11. Огляд основних технологій кібер-фізичних систем Інтернет речей (IoT, IIoT). Цифрові двійники (Digital Twins). Великі дані (Big Data). Машинне навчання (Machine Learning). Віртуальна реальність. Доповнена реальність. Література: 2 - 4.

№ заняття	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
	Самостійна робота: вивчення основних технологій кібер-фізичних систем.
12.	<p>Лекція 12. Цифрові двійники промислового застосування</p> <p>Еталонна модель цифрового двійника від Industrial Internet Consortium.</p> <p>Зв'язки між цифровими двійниками в кібер-фізичних системах.</p> <p>Цифровий двійник в життєвому циклі об'єкту управління.</p> <p>Література: 3, 4, 12.</p> <p>Самостійна робота: вивчення основних технологій кібер-фізичних систем.</p>
13.	<p>Лекція 13. Методи та алгоритми фільтрації, що застосовуються на пограничних пристроях КФС</p> <p>Завдання методів фільтрації, які застосовуються на пограничних пристроях.</p> <p>Метод ковзного осереднення, метод експоненційного згладжування, цифрові методи фільтрації.</p> <p>Література: 1, 4, 6.</p> <p>Самостійна робота: вивчення основних методів фільтрації, які застосовуються на пограничних пристроях.</p>
14.	<p>Лекція 14. Методи та алгоритми аналізу великих даних, що застосовуються у хмарному середовищі КФС</p> <p>Основні завдання, що розв'язують алгоритми аналізу великих даних.</p> <p>Математичне забезпечення алгоритмів аналізу великих даних у хмарному середовищі КФС.</p> <p>Література: 1.</p> <p>Самостійна робота: вивчення основних методів аналізу даних у хмарному середовищі</p>
15.	<p>Лекція 15. Розробка математичної моделі цифрового двійника для рівня бізнес-аналітики об'єкта</p> <p>Етапи розробки моделі.</p> <p>Формування функцій прогнозування.</p> <p>Оцінювання якості моделі і прогнозів.</p> <p>Література: 1, 13.</p> <p>Самостійна робота: засвоєння етапів розробки математичної моделі для рівня бізнес-аналітики об'єкта.</p>
16.	<p>Лекція 16. Розробка математичної моделі цифрового двійника для рівня використання об'єкта</p> <p>Етапи розробки моделі.</p> <p>Аналіз невизначеностей математичної моделі.</p> <p>Оцінювання якості моделі.</p> <p>Література: 1, 5.</p> <p>Самостійна робота: засвоєння етапів розробки математичної моделі для рівня використання об'єкта.</p>
17.	<p>Лекція 17. Розробка математичної моделі цифрового двійника для рівня функціонування об'єкта</p> <p>Етапи розробки моделі.</p> <p>Оцінювання якості моделі.</p> <p>Література: 1.</p> <p>Самостійна робота: засвоєння етапів розробки математичної моделі для рівня функціонування об'єкта.</p>
18.	<p>Лекція 18. Безпека кібер-фізичних систем</p> <p>Актуальність питання безпеки кібер-фізичних систем.</p> <p>Основні загрози та напрями кібератак.</p> <p>Методи та засоби кіберзахисту.</p>

№ заняття	Назва теми лекції та перелік основних питань (перелік дидактичних засобів, посилання на літературу та завдання на СРС)
	Література: 3, 4. Самостійна робота: вивчення методів та засоби кіберзахисту.

Комп'ютерний практикум використовуються для отримання та закріплення знань і навичок, висвітлених в лекційній частині курсу та під час самостійного вивчення студентами першоджерел. Основні завдання комп'ютерного практикуму – розробка математичних моделей та алгоритмізація сервісних функцій IoT.

Перелік тем і завдань комп'ютерного практикуму

№ заняття	Назва практичної роботи
1	Алгоритми первинного згладжування даних сенсорів на пограничних пристроях КФС.
2, 3	Алгоритми аналізу даних у сервісному середовищі КФС.
4	Контрольна робота за пройденим матеріалом.
5, 6	Розробка та чисельне дослідження моделі цифрового двійника для рівня бізнес-аналітики об'єкта.
7, 8	Розробка та чисельне дослідження моделі цифрового двійника для рівня використання об'єкта.
9	Залікова атестація, контрольна робота за дисципліною (для підвищення рейтингу).

У порядку чи тематиці занять можуть бути зміни, викликані наперед невизначеними обставинами. Слідкуйте за оголошеннями викладачів курсу.

6. Самостійна робота студента

У відповідності до робочого навчального плану передбачено 66 годин самостійної роботи студентів, з яких 8 годин - на підготовку до заліку і 58 годин на підготовку до аудиторних занять, опрацювання матеріалів лекцій, самостійний розв'язок додаткових задач та ознайомлення із навчальною літературою відповідно до структури дисципліни. Робота направлена на засвоєння та поглиблення вивченого матеріалу та на підготовку до занять та семестрового контролю. Самостійна робота студентів передбачає:

- закріплення знань, отриманих під час вивчення дисципліни;
- здобуття навичок самостійного вивчення матеріалу.

Перед кожним лекційним заняттям, окрім першого, студент переглядає надані матеріали та рекомендовані джерела, що стосуються теми лекції.

Перед кожним практичним заняттям студент ознайомлюється з темою та завданнями, запланованими на заняття, повторює теоретичний матеріал.

Політика та контроль

7. Політика навчальної дисципліни (освітнього компонента)

Правила відвідування занять

Очікується, що студент відвідуватиме кожне аудиторне заняття, робитиме це вчасно, без запізнь. У разі особливих обставин студент, за узгодженням з викладачем, може бути відсутнім на занятті, але це не може бути систематично.

Правила поведінки на заняттях

На заняттях передбачається активність студентів, пов'язана з навчальним процесом, включення в інтерактивні форми та методи навчання.

Під час комп'ютерного практикуму, окрім наявного в лабораторії обладнання, студент може користуватися власним ноутбуком.

Правила виконання і захисту практичних робіт

Навчальна лабораторія обладнана персональними комп'ютерами для виконання практичних завдань. До їх використання допускаються лише студенти, які пройшли відповідний інструктаж з техніки безпеки та правил використання обладнання.

Комп'ютерний практикум виконуються бригадами з кількох студентів, сформованими на всю тривалість навчання дисципліни.

До захисту роботи допускаються студенти, які правильно виконали практичне завдання та мають підтвердження у вигляді завіреного викладачем протоколу. Захист проходить у форматі індивідуального спілкування студента з викладачем по тематиці роботи та виконання практичного завдання.

Правила призначення заохочувальних та штрафних балів

За узгодженням з викладачем студент може зробити доповідь по темі, релевантній дисципліні, виконувати додаткові завдання чи брати участь у модернізації методичного забезпечення дисципліни. Заохоченням до подібної успішної роботи є додаткові рейтингові бали загальним обсягом до 10% від максимального рейтингового балу шкали оцінювання. Кількість та правила нарахування балів узгоджується викладачем у кожному окремому випадку.

Захист практичної роботи проводиться на занятті із комп'ютерного практикуму, на якому видане завдання, або на наступному календарному практичному занятті. У такому випадку студент має можливість отримати максимальний бал, відведений на цю роботу. У разі затримки захисту практичної роботи максимальний бал, який може отримати студент, зменшується на 20% за кожне прострочене календарне заняття.

Політика дедлайнів та перескладань

Студент, який з будь-яких причин не зміг вчасно виконати та захистити практичну роботу, може це зробити на наступних практичних заняттях за умови доступності обладнання та часу у викладачів. Під час виконання та захисту практичних робіт пріоритет надається студентам, які виконують завдання згідно календарного плану. Виконання та/або захист практичної роботи після відведеного на неї строку призводить до зниження максимального балу, який студент може отримати за цей вид роботи.

Допуск до перескладання заходів семестрового контролю та самі перескладання здійснюються згідно правил Університету у терміни, визначені Університетом.

Політика щодо академічної доброчесності

Політика та принципи академічної доброчесності визначені у розділі 3 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

У разі виявлення порушення академічної доброчесності результати роботи студента, які стосуються недоброчесності, анулюються.

Норми етичної поведінки

Норми етичної поведінки студентів і працівників визначені у розділі 2 Кодексу честі Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського». Детальніше: <https://kpi.ua/code>.

8. Види контролю та рейтингова система оцінювання результатів навчання (PCO)

Рейтинг студента з дисципліни складається з балів, які він отримує за:

- 1) контрольну роботу (20 балів);
- 2) комп'ютерний практикум (80 балів).

Система рейтингових балів

1. Контрольна робота (максимум 20 балів):

- а. творче розкриття завдання (не менше 90% потрібної інформації) – 18...20 балів;

- b. глибоке розкриття завдання (не менше 75% потрібної інформації), незначні неточності або неповні відповіді – 15...18 балів;
- c. достатнє розкриття завдання (не менше 60% потрібної інформації) або часткова наявність помилкової інформації – 11...15 балів;
- d. відповідь не розкриває завдання або містить помилкову інформацію – 0 балів.

2. Комп'ютерний практикум (максимум 20 бали за кожну роботу).

Максимальна кількість балів за виконання циклу комп'ютерного практикуму дорівнює $20 \times 4 = 80$ балів. Комп'ютерний практикум проводиться в якості захисту практичних робіт. Критерії оцінювання:

- a. 18...20 балів – повна відповідь (не менше 90% потрібної інформації);
- b. 15...18 балів – достатньо повна відповідь (не менше 75% потрібної інформації);
- c. 11...15 балів – неповна відповідь (не менше 60% потрібної інформації);
- d. 0 балів – незадовільна відповідь.

Штрафні та заохочувальні бали:

- якщо завдання практичних робіт здається невчасно (пізніше встановленого строку) без поважної причини, то нараховується 1 штрафний бал (знімається 1 бал від максимальної оцінки);
- за участь у інститутських олімпіадах з дисципліни, модернізації курсу лекційних чи практичних робіт надається від 1 до 5 заохочувальних балів;
- за активність на лекційних заняттях надається від 1 до 5 заохочувальних балів.

Сума штрафних та заохочувальних балів не може перевищувати 5 балів.

Умови позитивного календарного контролю (атестації)

Для отримання «атестовано» з першого календарного контролю (першої атестації) студент повинен мати не менше ніж 15 балів та виконання всіх завдань практичних робіт (на час атестації). Умовою другого календарного контролю – отримання не менше 30 балів, виконання всіх завдань практичних робіт (на час атестації).

Умови атестації

Умовою атестації студента є виконання усіх поточних контрольних заходів та рейтинг більший за 30 балів. На останньому практичному занятті (за розкладом) проводиться семестрова атестація. Студенти, які отримали за рейтингом позитивну оцінку (набрали протягом семестру не менше ніж 60 балів ($RD \geq 60$)), можуть бути атестовані за цими балами без написання контрольної роботи. Студенти, які отримали менше 60 балів, а також ті, хто хоче підвищити оцінку, виконують контрольну роботу і захищають її у вигляді співбесіди. У цьому разі рейтингова оцінка складається з результатів роботи в семестрі (RD) та результатів контрольної роботи. Якщо контрольна робота не може бути позитивно оцінена, то сумарна рейтингова оцінка залишається незмінною.

Максимальна кількість балів за контрольну роботу – 40.

- вичерпна відповідь – 36...40 балів;
- відповідь з незначними помилками – 30...35 балів;
- неповна відповідь та незначні помилки – 24...29 балів;
- грубі помилки – 18...23.
- незадовільна відповідь – 0 балів.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Кількість балів	Оцінка
100-95	Відмінно
94-85	Дуже добре

84-75	Добре
74-65	Задовільно
64-60	Достатньо
Менше 60	Незадовільно
Не виконані умови допуску	Не допущено

9. Додаткова інформація з дисципліни (освітнього компонента)

У рамках опанування дисципліни «Технології кібер-фізичних систем» допускається можливість зарахування сертифікатів проходження дистанційних чи онлайн курсів за відповідною тематикою (за попереднім узгодженням викладачем). Кількість балів визначається після аналізу програми, тривалості та результатів курсу, вказаного у сертифікаті.

Робочу програму навчальної дисципліни (силабус):

Складено доцентом, к.т.н, доцентом, Голінко Ігорем Михайловичем

Ухвалено кафедрою ММСА (протокол № 13 від 05.06.2024)

Погоджено Методичною комісією ІПСА (протокол № 10 від 24.06.2024)
