МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО НАУКИ, ВЫСШЕГО ОБРАЗОВАНИЯ И ИННОВАЦИЙ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

МОО ВО Кыргызско-Российский Славянский университет имени первого Президента Российской Федерации Б.Н. Ельцина

Высшая школа Цифровых технологий

Фонд
оценочных средств

по дисциплине «Программирование сетей и инфокоммуникаций вычислительных комплексов»

Уровень высшего образования

МАГИСТРАТУРА

Направление подготовки

09.04.04 - РФ, 710400 - КР Программная инженерия

(код и наименование направления подготовки)

"Основы анализа и разработки приложений с большими объемами распределенных данных"

Квалификация

магистр

Фонд оценочных средств предназначен для контроля знаний обучающихся по направлению подготовки 09.04.04 – РФ, 710400 - КР «Программная инженерия» по дисциплине «Программирование сетей и инфокоммуникаций вычислительных комплексов».

Фонд оценочных средств рассмотрен и утвержден на заседании Высшей школы Цифровых технологий протокол №1 от 02.09.26

Директор Высшей школы Цифровых технологий:

к.т.н., доцент Хмелева И.В.

Руководитель образовательной программы:

д.т.н., профессор Лыченко Н.М.

Исполнители (разработчики):

доцент, к.т.н., Медведев Б.М. (СПбПУ)

СОГЛАСОВАНО:
Зам. директора по учебной работе
Политехнического института КРСУ Комарцов Н.М. _____

Раздел 1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

Формируемая компетенция	Планируемые результаты обучения	Виды оценочных средств
ПК-11. Способен управлять получением, хранением, передачей, обработкой больших данных.	**Знать:** сетевые протоколы и источники угроз безопасности передачи информации; рекомендации ITU серии Y.4000; принципы стандартизации IoT; архитектуры встраиваемых устройств, туманных и облачных вычислений; сценарии применения IoT	**Блок А** — задания репродуктивного уровня: тематический устный опрос, контрольная работа
	Уметь: применять методы обеспечения безопасности передачи информации; проектировать взаимодействие IoT-устройств и сетевых сервисов; разрабатывать и настраивать ПО устройств; использовать протоколы и облачные средства обработки сообщений	**Блок В** — задания реконструктивного уровня: практические работы № 1–5, решение прикладных задач
	Владеть: практическими приёмами программирования IoT-устройств, настройки сетевого обмена, передачи сообщений в облако, прототипирования и тестирования сетевых приложений, проверки безопасности передачи информации	**Блок С** — практико-ориентированные задания, анализ работоспособности и защищённости разработанного приложения

Оценивание достижения компетенции осуществляется последовательно: проверка теоретических знаний, выполнение практических заданий, комплексная оценка приобретённых умений и навыков.

Раздел 2. Технологическая карта дисциплины

Курс 1, семестр 2. Количество ЗЕ — 2. Отчётность — зачёт.

Название модулей дисциплины согласно РПД	Контроль	Форма контроля	Зачётный минимум	Зачётный максимум	График контроля, неделя
Модуль 1. Архитектура и программирование сетевых устройств Интернета вещей	Текущий	Сдача практических работ № 1 и № 2	12	20	26
	Рубежный	Тематический опрос по архитектуре, устройствам и сетевым протоколам IoT	6	10	30
Модуль 2. Облачные сервисы, приложения и безопасность Интернета вещей	Текущий	Сдача практических работ № 3, № 4 и № 5	12	20	34
	Рубежный	Контрольная работа № 1. Облачные IoT-сервисы и безопасность	10	20	37

ВСЕГО за семестр			**40**	**70**	37
Промежуточный контроль		Зачёт	20	30	По расписанию
Семестровый рейтинг по дисциплине			**60**	**100**	

Раздел 3. Типовые контрольные задания и иные материалы, необходимые для оценки планируемых результатов обучения

Блок А — задания репродуктивного уровня

Модуль 1. Архитектура и программирование сетевых устройств Интернета вещей

Вопросы для устного опроса:

1. Дайте определение Интернета вещей (IoT). Каковы его основные характеристики?
2. Какие рекомендации ITU серии Y.4000 регламентируют построение IoT-систем?
3. В чём различия между концепциями IoT, M2M и Industrial IoT?
4. Назовите основные компоненты архитектуры IoT-системы.
5. Какие средства применяются для идентификации устройств и объектов?
6. Сравните технологии RFID и QR-кодов.
7. Какие типы датчиков применяются в системах IoT?
8. Охарактеризуйте особенности встраиваемого программного обеспечения устройств.
9. Сравните технологии Bluetooth, Wi-Fi и ZigBee.
10. В чём состоит назначение туманных вычислений?
11. Перечислите функции узлов туманных вычислений.
12. Какие характеристики следует учитывать при выборе сетевого протокола для IoT?

Модуль 2. Облачные сервисы, приложения и безопасность Интернета вещей

Вопросы для текущего и рубежного контроля:

1. Каковы основные функции облачной платформы Интернета вещей?
2. Какие способы взаимодействия IoT-устройств с облачными сервисами используются?
3. Какие данные составляют телеметрию IoT-устройства?
4. Перечислите этапы регистрации и подключения устройства к облачному сервису.
5. Какие функции выполняют облачные средства обработки сообщений?
6. Охарактеризуйте архитектуру приложения «Умный дом».
7. Какие задачи решают IoT-системы экологического мониторинга?
8. Что такое аутентификация и чем она отличается от авторизации?
9. Какие угрозы характерны для передачи информации устройствами IoT?
10. Какими способами обеспечиваются конфиденциальность и целостность данных?
11. Какие риски возникают при неправильном управлении идентификаторами и ключами доступа?
12. Какие показатели следует учитывать при оценке эффективности внедрения IoT?

Контрольная работа № 1. Облачные сервисы, приложения и безопасность IoT

Вариант 1:

1. Опишите архитектуру облачной системы сбора данных от датчиков температуры.
2. Обоснуйте выбор способа передачи сообщений от устройства.

3. Предложите механизм аутентификации устройства в облачном сервисе.
4. Разработайте схему обработки телеметрии и возврата управляющей команды.
5. Укажите показатели для оценки работоспособности и безопасности решения.

Вариант 2:

1. Разработайте архитектуру системы мониторинга транспортных средств.
2. Предложите структуру сообщений и порядок их передачи.
3. Определите потенциальные угрозы сетевого обмена.
4. Предложите меры защиты каналов передачи информации.
5. Определите показатели надёжности, производительности и стоимости решения.

Блок В — задания реконструктивного уровня

Практическая работа № 1. Встраиваемое программное обеспечение устройств IoT

Задание: разработать или адаптировать программный компонент, обеспечивающий формирование данных IoT-устройства.

Необходимо:

1. Определить тип устройства и состав передаваемых данных.
2. Описать структуру идентификатора устройства.
3. Разработать алгоритм формирования сообщений.
4. Реализовать программный компонент на выбранной платформе.
5. Продемонстрировать формирование корректного сообщения.
6. Подготовить отчёт с описанием алгоритма и результатами тестирования.

Практическая работа № 2. Сетевые протоколы

Задание: организовать сетевое взаимодействие между двумя программными компонентами IoT-системы.

Необходимо выбрать протокол, разработать схему сетевого обмена, организовать передачу тестовых сообщений, выполнить проверку корректности передачи и описать результаты.

Практическая работа № 3. Облачные сервисы Интернета вещей

Задание: реализовать прототип облачной обработки сообщений IoT-устройства.

Необходимо:

1. Выбрать облачную платформу или локальную тестовую среду.
2. Настроить регистрацию устройства.
3. Реализовать передачу телеметрических данных.
4. Организовать обработку полученных сообщений.
5. Реализовать передачу обратной управляющей команды.
6. Проверить работоспособность и оформить отчёт.

Допускается использование эмулятора устройства при отсутствии необходимого оборудования.

Практическая работа № 4. Приложения IoT

Задание: разработать архитектуру и минимальный прототип приложения для одного из сценариев: умный дом, умный город, транспорт, телемедицина или мониторинг окружающей среды.

Представить функциональные требования, схему взаимодействия компонентов и результаты проверки прототипа.

Практическая работа № 5. Безопасность IoT

Задание: провести анализ защищённости взаимодействия устройства с сетевым или облачным сервисом.

Необходимо выявить угрозы, предложить меры аутентификации и защиты передачи данных, проверить обработку некорректных сообщений и документировать результаты.

Блок C — задания практико-ориентированного и исследовательского уровня

Комплексное практическое задание

Разработать прототип системы мониторинга на основе IoT, в которой мобильное или встраиваемое устройство передаёт данные в облачный сервис.

Система должна обеспечивать формирование и передачу сообщений, обработку поступающих данных, выполнение заданного действия при наступлении события, а также базовую защиту сетевого взаимодействия.

По результатам работы представить программный код или конфигурацию компонентов, архитектурную схему, протокол испытаний и технический отчёт.

Исследовательское задание

Выполнить сравнительную оценку двух вариантов сетевого взаимодействия IoT-устройств.

Для каждого варианта оценить задержку передачи, устойчивость к ошибкам обмена, сложность интеграции и меры обеспечения безопасности.

Сформулировать обоснованный вывод о предпочтительной архитектуре для заданного прикладного сценария.

Блок D — промежуточный контроль (зачёт)

Вопросы для проверки уровня обученности «ЗНАТЬ»

1. Основные концепции и стандарты IoT.
2. Рекомендации ITU серии Y.4000.
3. Архитектура IoT-систем.
4. Средства идентификации объектов и устройств.
5. Датчики и встраиваемые вычислительные платформы.
6. Технологии беспроводной передачи данных.
7. Архитектура туманных вычислений.
8. Сетевые протоколы IoT.
9. Принципы организации облачных IoT-сервисов.
10. Способы интеграции устройств с облачными платформами.
11. Программные средства обработки IoT-сообщений.

12. Архитектуры прикладных IoT-систем.
13. Применение IoT в задачах городского и экологического мониторинга.
14. Основные угрозы безопасности IoT.
15. Аутентификация и авторизация устройств.
16. Конфиденциальность и целостность передаваемых данных.
17. Управление доступом к облачным сервисам.
18. Принципы обеспечения безопасного хранения информации.
19. Критерии выбора сетевых и облачных технологий.
20. Бизнес-модели и оценка эффективности внедрения IoT.

Задания для проверки уровня обученности «УМЕТЬ» и «ВЛАДЕТЬ»

1. Разработать архитектурную схему взаимодействия IoT-устройства и облачного сервиса.
2. Предложить структуру сообщения для передачи телеметрии.
3. Выбрать сетевой протокол и обосновать его применимость.
4. Составить алгоритм регистрации и аутентификации устройства.
5. Разработать программный прототип обработки входящих сообщений.
6. Предложить комплекс мер защиты данных IoT-приложения.

Пример зачётного билета № 1

Теоретические вопросы:

1. Охарактеризуйте архитектуру туманных вычислений.
2. Какие сетевые технологии используются для обмена данными устройств IoT?
3. Какие методы обеспечивают конфиденциальность передаваемой информации?

Практическое задание:

Разработайте схему системы, в которой датчик температуры передаёт измерения в облачный сервис. Укажите состав компонентов, структуру сообщения, выбранный протокол и меры защиты передаваемых данных.

Пример зачётного билета № 2

Теоретические вопросы:

1. Основные принципы стандартизации IoT.
2. Архитектура облачного сервиса обработки телеметрии.
3. Аутентификация и авторизация в IoT-системах.

Практическое задание:

Разработайте алгоритм регистрации мобильного устройства в облачном сервисе и передачи сообщения о состоянии датчика движения. Предусмотрите обработку ошибок и проверку подлинности устройства.

Пример зачётного билета № 3

Теоретические вопросы:

1. Встраиваемое программное обеспечение устройств IoT.
2. Примеры применения IoT в системах мониторинга.

3. Угрозы безопасности при передаче и хранении данных.

Практическое задание:

Предложите архитектуру IoT-системы мониторинга качества атмосферного воздуха. Определите необходимые компоненты, механизм передачи данных, способы проверки корректности и защиты информации.

Раздел 4. Методические материалы, определяющие процедуры оценивания знаний, умений и навыков

Оценивание результатов обучения осуществляется посредством текущего контроля практических работ, рубежного контроля и промежуточной аттестации в форме зачёта.

Шкала оценивания практических работ

- **85–100%** максимального балла — задание выполнено полностью, решение работоспособно, представлено обоснование и результаты проверки.
- **70–84%** — задание выполнено в основном правильно, имеются отдельные несущественные недостатки.
- **60–69%** — реализована основная функциональность, имеются ошибки и неполные результаты.
- **31–59%** — выполнена только часть задания, выявлены существенные недостатки.
- **0–30%** — задание не выполнено или результат не соответствует требованиям.

Шкала оценивания тематического опроса и контрольной работы

Оценка определяется по полноте и корректности ответов, пониманию терминологии, правильности решений, качеству аргументации и способности применять теоретические положения к практическим задачам.

Максимум за тематический опрос первого модуля — 10 баллов; максимум за контрольную работу второго модуля — 20 баллов.

Шкала оценивания зачёта

Промежуточная аттестация предусматривает теоретические вопросы и практическое задание.

Максимум за теоретическую часть — 10 баллов, за практическое задание — 20 баллов. Всего — 30 баллов.

При оценивании учитываются знание основных понятий, правильность решения, способность аргументировать выбранные технологии, соблюдение требований безопасности и качество представления результатов.

Перевод семестрового рейтинга в оценку

Суммарный рейтинг	Результат
85–100 баллов	Отлично / зачтено
70–84 балла	Хорошо / зачтено
60–69 баллов	Удовлетворительно / зачтено

Менее 60 баллов	Неудовлетворительно / не зачтено

Для дисциплины, завершающейся обычным зачётом, итоговый результат фиксируется как «зачтено» или «не зачтено».

Раздел 5. Методические указания для обучающихся по освоению дисциплины и выполнению контрольных заданий

5.1. Общие рекомендации по самостоятельной работе

Самостоятельная работа студентов направлена на закрепление теоретического материала, освоение технологий программирования сетей и устройств Интернета вещей, подготовку к практическим занятиям и промежуточной аттестации.

Рекомендуется изучать материалы лекций, стандарты и техническую документацию, выполнять практические задания, анализировать ошибки программ и сетевого обмена, готовить отчёты.

5.2. Подготовка к практическим занятиям

Перед занятием обучающийся изучает теоретические положения соответствующей темы и знакомится с необходимыми программными средствами.

Практическое задание выполняется индивидуально или в составе учебной группы в соответствии с указаниями преподавателя.

Отчёт должен содержать цель, постановку задачи, краткое описание технологии, алгоритм или схему взаимодействия, результаты выполнения и выводы.

5.3. Подготовка к контрольной работе

Обучающимся следует повторить материал обоих разделов дисциплины, особое внимание уделить архитектуре IoT, сетевым протоколам, облачной интеграции и безопасности.

При решении заданий необходимо обосновывать архитектурные и технологические решения, указывать ограничения выбранных методов и предлагать способы проверки корректности.

5.4. Подготовка к зачёту

Подготовка включает систематизацию теоретического материала, повторение практических работ и анализ выполненных программных решений.

На зачёте обучающийся должен продемонстрировать понимание основных принципов построения IoT-систем, умение применять сетевые технологии, проектировать безопасную передачу данных и анализировать результаты работы программных компонентов.

5.5. Требования к оформлению практических заданий

Результаты представляются в электронном виде. В состав материалов включаются исходный код или конфигурация, пояснительная записка, при необходимости схема сети, журналы проверки и описание полученных результатов.

При использовании облачных сервисов запрещается включать в отчёты действующие пароли, секретные ключи и другие конфиденциальные учётные данные.