

МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования

«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт информационных технологий, машиностроения и автотранспорта

ПОДПИСАНО ЭП КУЗГТУ

Институт информационных технологий,
машиностроения и автотранспорта
Директор

Дата: 05.05.2026 Н24:38:03

Д.М. Дубинкин

Фонд оценочных средств дисциплины

Информационная безопасность интернета вещей

Направление подготовки 10.04.01 Информационная безопасность
Направленность (профиль) Организация и технология защиты информации

Присваиваемая квалификация
"Магистр"

Формы обучения
очно-заочная

5.1 Паспорт комплекта оценочных материалов

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Ф о р м а (ы) т е к у щ е г о к о н т р о л я	К о м п е т е н ц и и , ф о р м и р у е м ы е в р е з у л ь т а т е о с в о е н и я д и с ц и п л и н ы (м о д у л я)	И н д и к а т о р (ы) д о с т и ж е н и я к о м п е т е н ц и и	Р е з у л ь т а т ы о б у ч е н и я п о д и с ц и п л и н е (м о д у л ю)	У р о в е н ь

Опрос по контрольным вопросам, подготовка отчетов по практическим и (или) лабораторным работам	ОПК-2	Разрабатывает требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	Знает принципы построения систем на базе IoT-устройств, а также способы их эффективной реализации; существующие технологии в области Интернета вещей; стандарты реализации интерфейсов подключаемых устройств; стандарты информационного взаимодействия систем. Знает типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях; требования НПА и стандартов по разработке моделей угроз информационной безопасности; наиболее распространенные уязвимости IoT-устройств и протоколов передачи данных; средства обеспечения информационной безопасности IoT-систем; принципы построения защищенных телекоммуникационных систем; механизмы реализации атак в сетях Интернета вещей; Умеет проводить анализ защищенности IoT-систем; Разрабатывать модели угроз для систем Интернета Вещей. Умеет проводить первичную настройку и проверку функционирования СССЭ, средств и систем защиты СССЭ от НСД; разбираться в существующих IoT-технологиях и применять их к конкретным сценариям; внедрять типовые решения по информационной безопасности IoT-систем; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с требованиями нормативно правовых актов и нормативных методических документов. Владеет способами конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией; работать с документацией прилагаемой разработчиком устройства; обнаруживать типовые уязвимости IoT систем. Может формировать требования и разрабатывать спецификации для проектируемой системы на базе IoT-устройств; планировать разработку сложных системы на базе IoT-устройств; проводить выбор эффективных способов реализации структур системы на базе IoT-устройств при решении профессиональных задач.	Высокий или средний
--	-------	---	--	---------------------

Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено.
Средний уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено.
Низкий уровень достижения компетенции - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.

5.2. Контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: <https://el.kuzstu.ru/login/index.php>.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1. Оценочные материалы при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам в оформлении отчетов по лабораторным работам.

Опросе обучающихся по контрольным вопросам

Обучающийся отвечает на 2 вопроса.

Например:

Содержание вопроса (задания)	Правильный ответ
Перечислите три основных уровня (сегмента) типовой архитектуры системы Интернета вещей (IoT), которые необходимо учитывать при разработке технического проекта системы обеспечения информационной безопасности.	В о с п р и я т и е , сетевой, прикладной
Как называется специализированный сетевой узел, который в проектах систем защиты IoT-решений выполняет роль посредника между оконечными устройствами (датчиками) и облачной платформой, обеспечивая локальную фильтрацию трафика и трансляцию протоколов?	Шлюз

Критерии оценивания при ответе на вопросы:

- 100 баллов - при правильном и полном ответе на два вопроса;
- 85...99 баллов - при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75...84 баллов - при правильном и неполном ответе на два вопроса;
- 65...74 баллов - правильном и полном ответе только на один из вопросов
- 25...64 - при правильном и неполном ответе только на один из вопросов;
- 0...24 баллов - при отсутствии правильных ответов на вопросы.

Количество баллов	0-64	65-100
Шкала оценивания	Не зачтено	Зачтено

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1. Тема работы.
2. Задачи работы.
3. Краткое описание хода выполнения работы.
4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).
5. Выводы

Критерии оценивания:

- 75 - 100 баллов - при раскрытии всех разделов в полном объеме
- 0 - 74 баллов - при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0-74	75-100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные материалы при промежуточной аттестации

Формами промежуточной аттестации являются экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На зачете обучающийся отвечает на 2 вопроса или проходит тестирование.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85...99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75...84 баллов – при правильном и неполном ответе на два вопроса;
- 65...74 баллов – при правильном и полном ответе только на один из вопросов
- 25...64 – при правильном и неполном ответе только на один из вопросов;
- 0...24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
Шкала оценивания	Не зачтено		Зачтено		

Примерный перечень вопросов на экзамене:

Содержание вопроса (задания)	Правильный ответ
Перечислите три основных уровня (сегмента) типовой архитектуры системы Интернета вещей (IoT), которые необходимо учитывать при разработке технического проекта системы обеспечения информационной безопасности.	В о с п р и я т и е , сетевой, прикладной
Как называется специализированный сетевой узел, который в проектах систем защиты IoT-решений выполняет роль посредника между оконечными устройствами (датчиками) и облачной платформой, обеспечивая локальную фильтрацию трафика и трансляцию протоколов?	Шлюз

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85...94 баллов – при правильном ответе на 16-18 вопросов;
- 75...84 баллов – при правильном ответе на 13-15 вопросов;
- 65...74 баллов – при правильном ответе на 10-12 вопросов
- 25...64 – при правильном ответе только на 1-9 вопрос(ов);
- 0...24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Удовлетворительно	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень тестовых заданий

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;

Содержание вопроса (задания)	Правильный ответ
При разработке технического проекта системы защиты промышленного интернета вещей (IIoT) для изоляции критически важных контроллеров от офисной сети предприятия рекомендуется использовать: 1. Одноранговую сеть (P2P) без маршрутизации. 2. Сегментацию сети с помощью виртуальных локальных сетей (VLAN) и межсетевых экранов. 3. Общую Wi-Fi сеть с открытым доступом для удобства обслуживания. 4. Прямое подключение каждого контроллера к сети Интернет через выделенный IP.	2
Что является обязательным этапом при разработке технического проекта системы обеспечения ИБ для IoT в соответствии с системным подходом? 1. Закупка самого дорогого оборудования на рынке. 2. Моделирование угроз и идентификация уязвимостей компонентов системы. 3. Личное собеседование с каждым пользователем системы. 4. Отказ от использования облачных технологий в пользу бумажных носителей.	2

Содержание вопроса (задания)		Правильный ответ
Установите соответствие между типом устройства (левая колонка) и его основной функцией в техническом проекте системы обеспечения информационной безопасности IoT (правая колонка):		А - 2, Б - 1, В - 3.
Тип устройств	Основная защитная функция	
А. Криптографический модуль	1. Инспекция пакетов и сегментация трафика между IoT-сегментом и внешней сетью	
Б. Межсетевой экран	2. Безопасное хранение ключей и выполнение доверенных вычислений на устройствах	
В. Система IDS/IPS	3. Обнаружение аномалий в поведении датчиков и попыток сканирования сети	
При разработке проекта защиты IoT-системы выберите соответствующий механизм защиты для каждой категории угроз:		А - 2, Б - 1, В - 3.
Категория угрозы	Механизм защиты в проекте	
А) Подмена данных в канале связи	1) Контроль целостности прошивки	
Б) Несанкционированный запуск вредоносного ПО	2) Двусторонняя аутентификация и шифрование	
В) Перебор паролей к устройству	3) Ограничение количества попыток входа и использование сертификатов	
Установите правильную последовательность этапов разработки технического проекта системы обеспечения информационной безопасности (СОИБ) для сети Интернета вещей: 1. 1. Выбор конкретных средств защиты информации и алгоритмов шифрования. 2. 2. Проведение инвентаризации активов и идентификация IoT-устройств. 3. 3. Моделирование угроз и определение векторов атак на компоненты системы. 4. 4. Формирование требований к системе защиты и определение зон доверия. 5. 5. Оценка остаточных рисков и составление спецификации оборудования.		2, 3, 4, 1, 5.
Расположите уровни модели взаимодействия устройств в IoT-системе (от окончного устройства к пользователю) для корректного проектирования мер защиты на каждом этапе: 1. 1. Облачная платформа или центр обработки данных (аналитика и хранение). 2. 2. Полевой уровень (датчики, исполнительные механизмы, контроллеры). 3. 3. Уровень передачи данных (шлюзы, маршрутизаторы, сетевые протоколы). 4. 4. Приложение пользователя (интерфейс мониторинга и управления).		2, 3, 1, 4.

2.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых

электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени, установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответами на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.