

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

Подразделение: институт информационных
технологий, машиностроения и
автотранспорта

Должность: директор института

Дата: 15.09.2026 16:04:34

Дубинкин Дмитрий Михайлович

Рабочая программа дисциплины

Информационная безопасность интернета вещей

Направление подготовки 10.04.01 Информационная безопасность
Направленность (профиль) 01 Организация и технология защиты информации

Присваиваемая квалификация
"Магистр"

Формы обучения
очно-заочная

Кемерово 2026 г.



1784080404

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:17:22

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 9 от 03.07.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:17:44

Прокопенко Евгения Викторовна

Согласовано учебно-методической комиссией по направлению подготовки (специальности)
10.04.01 Информационная безопасность

Протокол № 9 от 03.07.2026

ПОДПИСАНО ЭП КУЗГТУ

Подразделение: кафедра информационной безопасности

Должность: заведующий кафедрой (к.н.,спд)

Дата: 17.07.2026 10:18:03

Прокопенко Евгения Викторовна



1784080404

1 Перечень планируемых результатов обучения по дисциплине "Информационная безопасность интернета вещей", соотнесенных с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общефессиональных компетенций:

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

Результаты обучения по дисциплине определяются индикаторами достижения компетенций

Индикатор(ы) достижения:

Разрабатывает требования к средствам и методам контроля проектируемой системы (подсистемы либо компонента системы) обеспечения информационной безопасности.

Результаты обучения по дисциплине:

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.

2 Место дисциплины "Информационная безопасность интернета вещей" в структуре ОПОП магистратуры

Для освоения дисциплины необходимы знания умения, навыки и (или) опыт профессиональной деятельности, полученные в рамках изучения следующих дисциплин: .

Дисциплина входит в Блок 1 «Дисциплины (модули)» ОПОП. Цель дисциплины - получение обучающимися знаний, умений, навыков и (или) опыта профессиональной деятельности, необходимых для формирования компетенций, указанных в пункте 1.

3 Объем дисциплины "Информационная безопасность интернета вещей" в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины "Информационная безопасность интернета вещей" составляет 4 зачетных единицы, 144 часа.

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 2/Семестр 3			



1784080404

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Всего часов			144
Контактная работа обучающихся с преподавателем (по видам учебных занятий):			
Аудиторная работа			
Лекции			12
Лабораторные занятия			
Практические занятия			
Внеаудиторная работа			
Индивидуальная работа с преподавателем:			
Консультация и иные виды учебной деятельности			
Самостоятельная работа под руководством преподавателя			50
Самостоятельная работа			46
Форма промежуточной аттестации			экзамен /36

4 Содержание дисциплины "Информационная безопасность интернета вещей", структурированное по разделам (темам)

4.1. Лекционные занятия

Тема занятия	Трудоемкость в часах	
	ОФ	ОЗФ
1. Угрозы безопасности Интернета Вещей Интернет вещей: технологии, рынок, развитие; Анализ угроз безопасности и классификация уязвимостей систем Интернета Вещей; Моделирование угроз для систем Интернета Вещей.	2	2
2. Уязвимости аппаратной части систем Интернета Вещей Аппаратные механизмы обеспечения безопасности систем Интернета Вещей; Уязвимости аппаратной части систем Интернета Вещей.	2	2
3. Уязвимости беспроводных каналов передачи информации систем Интернета Вещей Безопасность беспроводных каналов ближнего радиуса действия; Безопасность беспроводных каналов среднего радиуса действия; Безопасность беспроводных каналов дальнего радиуса действия.	2	2
4. Атаки на экосистемы Интернета вещей Угрозы в мобильных приложениях интернета вещей	2	2
5. Разработка индивидуального проекта на базе технологий Интернета вещей.	4	4
Итого	12	12

4.2. Самостоятельная работа обучающегося и перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Вид СРС	Трудоемкость в часах	
	ОФ	ОЗФ



1784080404

Ознакомление с содержанием основной и дополнительной литературы, методических материалов, конспектов для подготовки к занятиям	14	14
Составление двуязычного глоссария к литературе по тематике научного исследования, предназначенной для внеаудиторного чтения;	26	26
Подготовка к промежуточной аттестации	6	6
Итого	46	46
Самостоятельная работа под руководством преподавателя	50	50
Экзамен	36	36

Самостоятельная работа под руководством преподавателя:

Внеаудиторная самостоятельная работа выполняется обучающимся самостоятельно по индивидуальным заданиям, полученным от педагогического работника, но без его непосредственного участия.

В ходе выполнения самостоятельной работы педагогический работник осуществляет непосредственное руководство процессом выполнения индивидуальной самостоятельной работы в форме текущего контроля успеваемости. Текущий контроль успеваемости обеспечивает оценивание хода самостоятельного освоения дисциплины (практик). Для организации самостоятельной работы обучающегося по индивидуальным заданиям, полученным от педагогического работника, а так же показатели и критерии оценивания, описание шкал оценивания результатов самостоятельной работы, используются оценочные материалы, размещенные в фондах оценочных средств для текущего контроля успеваемости обучающихся.

5 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине "Информационная безопасность интернета вещей"

5.1 Паспорт комплекта оценочных материалов

Планируемые результаты обучения по дисциплине (модулю)

Дисциплина направлена на формирование следующих компетенций выпускника:

Форма (ы) текущего контроля	Компетенции, формируемые в результате освоения дисциплины (модуля)	Индикатор (ы) достижения компетенции	Результаты обучения по дисциплине (модулю)	Уровень



1784080404

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
--	-------	---	--	---------------------



1784080404

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



1784080404

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 – 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 – 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



1784080404

Содержание вопроса (задания)		Правильный ответ								
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								
Установите соответствие между типом устройства (левая колонка) и его основной функцией в техническом проекте системы обеспечения информационной безопасности IoT (правая колонка): <table><tr><td>Тип устройств</td><td>Основная защитная функция</td></tr><tr><td>А. Криптографический модуль</td><td>1. Инспекция пакетов и сегментация трафика между IoT-сегментом и внешней сетью</td></tr><tr><td>Б. Межсетевой экран</td><td>2. Безопасное хранение ключей и выполнение доверенных вычислений на устройствах</td></tr><tr><td>В. Система IDS/IPS</td><td>3. Обнаружение аномалий в поведении датчиков и попыток сканирования сети</td></tr></table>		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	A - 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: <table><tr><td>Категория угрозы</td><td>Механизм защиты в проекте</td></tr><tr><td>А) Подмена данных в канале связи</td><td>1) Контроль целостности прошивки</td></tr><tr><td>Б) Несанкционированный запуск вредоносного ПО</td><td>2) Двусторонняя аутентификация и шифрование</td></tr><tr><td>В) Перебор паролей к устройству</td><td>3) Ограничение количества попыток входа и использование сертификатов</td></tr></table>		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	A - 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.								

5.2.3. 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



1784080404

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.



1784080404

6 Учебно-методическое обеспечение

6.1 Основная литература

1. Глушак, Е. В. Введение в Интернет вещей (лабораторные работы): практикум : учебное пособие / Е. В. Глушак, А. В. Куприянов. — Самара : Самарский университет, 2023. — 124 с. — ISBN 978-5-7883-2021-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/406634> (дата обращения: 02.12.2025). — Режим доступа: для авториз. пользователей.
2. Суомалайнен, А. Интернет вещей : видео, аудио, коммутация : практическое пособие : [16+] / А. Суомалайнен. — Москва : ДМК Пресс, 2019. — 120 с. : ил. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=578564> (дата обращения: 12.09.2026). — Библиогр. в кн. — ISBN 978-5-97060-761-9. — Текст : электронный.
3. Шамин, А. А. Интернет вещей для начинающих. Визуальное программирование микроконтроллеров семейства ESP8266 : учебное пособие / А. А. Шамин. — Москва ; Вологда : Инфра-Инженерия, 2023. — 120 с. — ISBN 978-5-9729-1167-7. — Текст : электронный. — URL: <https://znanium.ru/catalog/product/2094388> (дата обращения: 07.09.2026). — Режим доступа: по подписке.
4. Смирнов, В. И. Защита информации : лабораторный практикум : [16+] / В. И. Смирнов. — Йошкар-Ола : Поволжский государственный технологический университет, 2017. — 67 с. : ил. — Режим доступа: по подписке. — URL: <https://biblioclub.ru/index.php?page=book&id=476512> (дата обращения: 09.09.2026). — Библиогр. в кн. — ISBN 978-5-8158-1866-8. — Текст : электронный.
5. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ (МИИТ), 2019. — 144 с. — ISBN 978-5-7876-0326-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/188703> (дата обращения: 02.12.2025). — Режим доступа: для авториз. пользователей.
6. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/182491> (дата обращения: 02.12.2025). — Режим доступа: для авториз. пользователей.

6.2 Дополнительная литература

1. Глушак, Е. В. Введение в Интернет вещей (лабораторные работы): практикум : учебное пособие / Е. В. Глушак, А. В. Куприянов. — Самара : Самарский университет, 2023. — 124 с. — ISBN 978-5-7883-2021-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/406634> (дата обращения: 02.12.2025). — Режим доступа: для авториз. пользователей.
2. Глушак, Е. В. Введение в Интернет вещей (практические работы): практикум : учебное пособие / Е. В. Глушак, А. В. Куприянов. — Самара : Самарский университет, 2023. — 72 с. — ISBN 978-5-7883-2016-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/406637> (дата обращения: 02.12.2025). — Режим доступа: для авториз. пользователей.
3. Зараменских, Е. П. Интернет вещей. Исследования и область применения : монография / Е.П. Зараменских, И.Е. Артемьев. — Москва : ИНФРА-М, 2024. — 188 с. — (Научная мысль). — DOI 10.12737/13342. — ISBN 978-5-16-019914-6. — Текст : электронный. — URL: <https://znanium.ru/catalog/product/2144319> (дата обращения: 07.09.2026). — Режим доступа: по подписке.
4. Никулин, В. В. Безопасность и защита информации. Лабораторный практикум : учебно-методическое пособие / В. В. Никулин. — Брянск : Брянский ГАУ, 2021. — 128 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/304352> (дата обращения: 02.12.2025). — Режим доступа: для авториз. пользователей.
5. Грингард, С. Интернет вещей: будущее уже здесь : пер. с англ. / С. Грингард. — Москва : Издательская группа "Точка", 2017. — 224 с. — (Завтра это будут знать все). — Текст : непосредственный.

6.3 Методическая литература

1. Методические рекомендации по организации учебной деятельности обучающихся КузГТУ / ФГБОУ ВО «Кузбас. гос. техн. ун-т им. Т. Ф. Горбачева», Каф. приклад. информ. технологий ; сост. Л. И.



1784080404

Михалева. – Кемерово : КузГТУ, 2017. – 32 с. – URL: <http://library.kuzstu.ru/meto.php?n=553> (дата обращения: 02.12.2025). – Текст : электронный.

6.4 Профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система «Университетская библиотека онлайн» <http://biblioclub.ru/>
2. Электронная библиотечная система «Лань» <http://e.lanbook.com>
3. Электронная библиотека КузГТУ <https://library.kuzstu.ru/index.php/punkt-2/podrazdel-21>
4. Электронная библиотека Новосибирского государственного технического университета <https://clck.ru/UoXpv>
5. Образовательная платформа «Юрайт» <https://urait.ru/>
6. Электронная библиотечная система «Znaniium» <https://new.znaniium.com/my/documents>
7. Справочная правовая система «КонсультантПлюс» <http://www.consultant.ru/>
8. Национальная электронная библиотека <https://rusneb.ru/>

6.5 Периодические издания

1. Безопасность информационных технологий: научный журнал <https://eivis.ru/browse/publication/379646>
2. Защита информации. Инсайд: информационно-методический журнал <https://eivis.ru/browse/publication/122426>
3. Информация и безопасность : научный журнал

7 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

ЭИОС КузГТУ:

а) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: <https://elib.kuzstu.ru/>. – Текст: электронный.

б) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: <https://portal.kuzstu.ru/>. – Режим доступа: для авториз. пользователей. – Текст: электронный.

с) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: <https://el.kuzstu.ru/>. – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

8 Методические указания для обучающихся по освоению дисциплины "Информационная безопасность интернета вещей"

Самостоятельная работа обучающегося является частью его учебной деятельности, объемы самостоятельной работы по каждой дисциплине (модулю) практике, государственной итоговой аттестации, устанавливаются в учебном плане.

Самостоятельная работа по дисциплине (модулю), практике организуется следующим образом:

1. До начала освоения дисциплины обучающемуся необходимо ознакомиться с содержанием рабочей программы дисциплины (модуля), программы практики в следующем порядке:

1.1 содержание знаний, умений, навыков и (или) опыта профессиональной деятельности, которые будут сформированы в процессе освоения дисциплины (модуля), практики;

1.2 содержание конспектов лекций, размещенных в электронной информационной среде КузГТУ в порядке освоения дисциплины, указанном в рабочей программе дисциплины (модуля), практики;

1.3 содержание основной и дополнительной литературы.

2. В период освоения дисциплины обучающийся осуществляет самостоятельную работу в следующем порядке:

2.1 выполнение практических и (или) лабораторных работы и (или) отчетов в порядке, установленном в рабочей программе дисциплины (модуля), практики;

2.2 подготовка к опросам и (или) тестированию в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики;

2.3 подготовка к промежуточной аттестации в соответствии с порядком, установленном в рабочей программе дисциплины (модуля), практики.

В случае затруднений, возникших при выполнении самостоятельной работы, обучающемуся



1784080404

необходимо обратиться за консультацией к педагогическому работнику. Периоды проведения консультаций устанавливаются в расписании консультаций.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине "Информационная безопасность интернета вещей", включая перечень программного обеспечения и информационных справочных систем

Для изучения дисциплины может использоваться следующее программное обеспечение:

1. Mozilla Firefox
2. Google Chrome
3. ESET NOD32 Smart Security Business Edition
4. Kaspersky Endpoint Security
5. Браузер Спутник

10 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине "Информационная безопасность интернета вещей"

Специальное помещение № 3217 представляет собой учебную аудиторию для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации

Перечень основного оборудования:

специализированная мебель (столы и стулья);
технические средства обучения, служащие для представления учебной информации большой аудитории (ноутбук, переносной проектор, переносной экран);
наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации;
сетевая рабочая станция;
кафедра напольная 760*600*1250мм.;
проектор Acer X1260;
проекционный экран Projecta;
доска классная;
вешалка (доска для одежды).

Специальное помещение для самостоятельной работы № 1211

Перечень основного оборудования:

специализированная мебель (столы и стулья);
компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ;
проектор, экран настенный моторизованный.

Специальное помещение для самостоятельной работы № 3210

Перечень основного оборудования:

специализированная мебель (столы и стулья);
компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

11 Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных так и современных интерактивных технологий.

В рамках аудиторных занятий применяются следующие интерактивные методы:

- разбор конкретных примеров;
- мультимедийная презентация.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.



1784080404