

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»**

УТВЕРЖДАЮ

Проректор по учебной работе

(подпись) Василенко В.Н.
(Ф.И.О.)

«25» мая 2023 г.

**РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ**

Информационная безопасность интернет вещей
(наименование дисциплины (модуля))

Специальность

10.05.03 – Информационная безопасность автоматизированных систем
(код и наименование направления подготовки)

Специализация

Безопасность открытых информационных систем
(наименование направленности (профиля) подготовки)

Квалификация выпускника

Специалист по защите информации

(Бакалавр/Специалист/Магистр/Исследователь. Преподаватель-исследователь)

Воронеж

1. Цели и задачи дисциплины

Целями и задачами освоения дисциплины «Информационная безопасность интернет вещей» являются в соответствии с типом задач профессиональной деятельности:

- научно-исследовательский: обоснование необходимости защиты информации в автоматизированной системе, моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ПКв-6	способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей	ИД1 ПКв-6 обладает навыками определения всех типов угроз данным для различных информационных автоматизированных систем

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1 ПКв-6 обладает навыками определения всех типов угроз данным для различных информационных автоматизированных систем	Знает: терминологию и определения интернет вещей, процесс получения и обработки показаний цифровых и аналоговых датчиков, управление сенсором и контроллером, проектирование деталей конструкции, виды сборки, модернизация, проектирование печатных плат, компьютерную среду программирования Arduino; основные технологии сбора и обработки данных; основные элементы, используемые при создании IoT-платформ; особенности методов, используемых при обмене данными между «вещью» и IoT-платформой
	Умеет: самостоятельно решать технические задачи в процессе создания IoT-систем (планирование предстоящих действий, самоконтроль, применять полученные знания, приемы и опыт создания систем с использованием специальных элементов, и других объектов и т.д.); создавать реально действующие модели IoT-систем при помощи специальных элементов по разработанной схеме, по собственному замыслу; создавать программы на компьютере для различных IoT-систем
	Владеет: навыками программирования интернет вещей, тестирования готового продукта, разработки технологической карты или инструкции по эксплуатации готового продукта, навыками работы с виджетами, использования сервисов для организации обмена данными

3. Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность интернет вещей» относится к части формируемой участниками образовательных отношений Блока 1 ООП.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин: Система обнаружения компьютерных атак, интеллектуальные системы защиты информации.

Дисциплина является предшествующей для изучения: производственной практики, Аудит информационных технологий и систем обеспечения информационной безопасности, Безопасность облачных и распределенных вычислений.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет _____ 3 _____ зачетных единиц.

Виды учебной работы	Всего академических часов	Распределение трудоемкости по семестрам
		4 семестр
Общая трудоемкость дисциплины (модуля)	108	108
Контактная работа в т. ч. аудиторные занятия:	73,9	73,9
Лекции	36	36
<i>в том числе в форме практической подготовки</i>	–	–
Практические занятия	36	36
<i>в том числе в форме практической подготовки</i>	36	36
Консультации текущие	1	1
Вид аттестации (зачет с оценкой)	0,9	0,9
Самостоятельная работа:	34,1	34,1
Проработка материалов по конспекту лекций	6,4	6,4
Проработка материалов по учебнику для подготовки к практическим занятиям	24	24
Подготовка доклада	3,7	3,7

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Часов по разделу
1	Понятие интернета вещей	Введение. Общие тенденции. Принципы защиты. Слабые места IoT. Сертификация в области IoT.	24
2	Обеспечение информационной безопасности IoT	Основные виды угроз безопасности IoT. Безопасность связи. Усиленная модель доверия для IoT. Защита устройств. Защита программного кода IoT. Эффективная хостовая защита IoT	24
3	Эталонная архитектура интернета вещей	Контроль устройств. Аналитика безопасности как реакция на угрозы за рамками контрмер. Контроль взаимодействий в сети.	34
4	Комплексное обеспечение безопасности IoT	Необходимость обеспечения комплексной безопасности IoT. Принципы обеспечения комплексной информационной безопасности IoT	25
	<i>Консультации текущие</i>		1
	<i>Зачет, экзамен</i>		0,9

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак.ч	ПЗ, ак.час	СР, ак.час
1	Понятие интернета вещей	8*	8*	8
2	Обеспечение информационной безопасности IoT	10*	10*	8
3	Эталонная архитектура интернета вещей	8*	8*	10

4	Комплексное обеспечение безопасности IoT	10*	10*	8,1
	Консультации текущие	1		
	Зачет с оценкой	0,9		

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак.ч.
1	Понятие интернета вещей	Введение. Общие тенденции. Принципы защиты. Слабые места IoT. Сертификация в области IoT.	8*
2	Обеспечение информационной безопасности IoT	Основные виды угроз безопасности IoT. Безопасность связи. Усиленная модель доверия для IoT. Защита устройств. Защита программного кода IoT. Эффективная хостовая защита IoT	10*
3	Эталонная архитектура интернета вещей	Контроль устройств. Аналитика безопасности как реакция на угрозы за рамками контрмер. Контроль взаимодействий в сети.	8*
4	Комплексное обеспечение безопасности IoT	Необходимость обеспечения комплексной безопасности IoT. Принципы обеспечения комплексной информационной безопасности IoT	10*

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, ак.ч.
1	Понятие интернета вещей	Создание приложения на платформе «Интернета вещей» для сбора и первичной обработки данных с различного оборудования Создание интерфейсной страницы приложения, обеспечивающую вывод получаемых значений в режиме реального времени Обеспечение передачи данных между конечными устройствами и платформой «Интернета вещей» Мониторинг собираемых данных и передача управляющих команд	8*
2	Обеспечение информационной безопасности IoT	Проверка безопасности связи IoT. Построение усиленной модели доверия для IoT. Обеспечение защиты программного кода IoT. Предложения для эффективной хостовой защита IoT на примерах	8*

3	Эталонная архитектура интернета вещей	Разработка схемы размещения и подключения оборудования гибкой производственной ячейки Адаптация подготовленного ранее приложения на платформе Интернета вещей для выполнения задания и сбора данных с оборудования гибкой производственной ячейки Тестирование и отладка алгоритмов выполнения производственного задания Демонстрация функциональности системы	10*
4	Комплексное обеспечение безопасности IoT	Разработка системы визуализации данных работы мониторинга и определения технико-экономических показателей Разработка технической документации проекта	10*

5.2.3 Лабораторный практикум Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Понятие интернета вещей	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебнику для подготовки к практическим занятиям	3
		Подготовка доклада	3
2	Обеспечение информационной безопасности IoT	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебнику для подготовки к практическим занятиям	3
		Подготовка доклада	3
3	Эталонная архитектура интернета вещей	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебнику для подготовки к практическим занятиям	5
		Подготовка доклада	3
4	Комплексное обеспечение безопасности IoT	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебнику для подготовки к практическим занятиям	3,1
		Подготовка доклада	3

6 Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1. Основная литература

Кирсанов, Э.А. Обработка информации в пространственно-распределенных системах радиомониторинга: статистический и нейросетевой подходы [Электронный ресурс] : учебное пособие / Э.А. Кирсанов, А.А. Сирота. — Электрон. дан. — Москва : Физматлит, 2012. — 344 с.

6.2. Дополнительная литература

1. Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е. Артемьев. - М.: НИЦ ИНФРА-М, 2015. - 200 с

2. Микроконтроллеры для систем автоматики: Учебное пособие / Водовозов А.М. - Вологда:Инфра-Инженерия, 2016. - 164 с

3. Программируемые контроллеры в системах промышленной автоматизации: Учебник / Шишов О.В. - М.: НИЦ ИНФРА-М, 2016. - 365 с.

4. Введение в облачные вычисления и технологии / Губарев В.В., Савульчик С.А. - Новосибир.: НГТУ, 2013. - 48 с

5. Информационная безопасность интернета вещей: методические указания для самостоятельной работы студентов, обучающихся по специальности 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрипников, Е. В. Чернышова; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2021. - 20 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Данылиев, М. М. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс]: методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылиев, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж: ВГУИТ, 2016. – 32 с. Режим доступа в электронной среде:

<http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813>.

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	http://www.edu.ru/index.php
Научная электронная библиотека	http://www.elibrary.ru/defaulttx.asp?
Федеральная университетская компьютерная сеть России	http://www.runnet.ru/
Информационная система «Единое окно доступа к образовательным ресурсам»	http://www.window.edu.ru/
Электронная библиотека ВГУИТ	http://biblos.vsuet.ru/megapro/web
Сайт Министерства науки и высшего образования РФ	http://minobrnauki.gow.ru
Портал открытого on-line образования	http://npoed.ru
Информационно-коммуникационные технологии в образовании. Система федеральных образовательных порталов	http://www.ict.edu.ru/
Электронная образовательная среда ФГБОУ ВО «ВГУИТ»	http://education.vsuet.ru

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – ОС Windows; Microsoft Office.

7 Материально-техническое обеспечение дисциплины

<p>Аудитории для проведения занятий лекционного типа, лабораторных и практических занятий</p>	<p>Ауд.332, 424, 420 Компьютеры - 12 шт., стенды – 5 шт. Компьютер РЕГАРД – 11 шт., стенды – 3 шт. Компьютеры Core i5-4460 – 10 шт., Core i5-4570 – 1 шт., проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ», средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1», система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ), профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной), портативный обнаружитель закладок Protect1203 (переносной), устройство активной защиты информации «ВЕТО-М», электронный замок Samsung SHS-2920, системный блок Supermicro Amibios 786 Q 2000, коммутатор TP-Link SG1024DE, маршрутизатор MikroTik RB2011iLS-IN,</p>	<p>ОС Astra Linux Альт Образование 8.2 [Лицензия № AAA.0217.00 с 21.12.2017 г. Лицензионный договор № РБТ-14/1623-01-ВУЗ от 18.12.2017 г.] бессрочно, Libre Office 6.1 [Лицензия № AAA.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, wxMaxima [Лицензия № AAA.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, Lazarus [(бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus] бессрочно, SMathStudio [(бесплатное ПО) https://ru.wikipedia.org/wiki/SMath_Studio] бессрочно, Avidemux [(бесплатное ПО) https://ru.wikipedia.org/wiki/Avidemux] бессрочно, Oracle VM Virtual Box [https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, AnyLogic 8.3 [(бесплатное ПО) https://www.anylogic.ru/downloads/personal-learning-edition-download/] бессрочно. ОС Astra Linux Альт Образование 8.2 [Лицензия № AAA.0217.00 с 21.12.2017 г. Лицензионный договор № РБТ-14/1623-01-ВУЗ от 18.12.2017 г.] бессрочно, Libre Office 6.1 [Лицензия № AAA.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, wxMaxima [Лицензия № AAA.0217.00 с 21.12.2017 г.] бессрочно, Lazarus [(бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus] бессрочно, Oracle VM Virtual Box [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, FreePascal [(бесплатное ПО) https://ru.wikipedia.org/wiki/Free_Pascal] бессрочно. Microsoft Windows 7 [Microsoft Open License Microsoft Windows Professional 7 Russian Upgrade Academic OPEN 1 License No Level#47881748 от 24.12.2010г. http://eopen.microsoft.com] бессрочно, Microsoft Office 2007 Standart [Microsoft Open License Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com] бессрочно, Adobe Reader XI [(бесплатное ПО) https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader/volume-distribution.html] бессрочно, Microsoft Visual Studio 2010 [Сублицензионный договор № 17623/VRN3От 07 июля 2010 г. на право использование программы для ЭВМ MSDN AA Developer Electronic Fulfillment, FreePascal[(бесплатноеПО) https://ru.wikipedia.org/wiki/Free_Pascal] бессрочно, ФИКС 2.0.2 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + уста-</p>
---	---	--

		<p>новочный пакет], СТРАЖ NT 3.0 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г.], Панцирь [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г.], Ревизор 1 XP [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], Ревизор 3.0 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], СТРАЖ NT 4.0 [ДОГОВОР № 200016222100015 с ООО «Паскаль»], Secret Net[ДОГОВОР № 200016222100015 с ООО «Паскаль»], GIMP [(бесплатное ПО) https://ru.wikipedia.org/wiki/GIMP] бессрочно, Avidemux [(бесплатное ПО) https://ru.wikipedia.org/wiki/Avidemux] бессрочно, Virtual Dub [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualDub] бессрочно, Oracle VM Virtual Box [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, Netbeans [(бесплатное ПО) https://netbeans.org/] бессрочно, СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013</p>
<p>Аудитории для самостоятельной работы, курсового и дипломного проектирования</p>	<p>Читальные залы библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами; Ауд.424: Комплекты мебели для учебного процесса. Количество ПЭВМ – 12 (рабочая станция CPU Core 2Duo E6300 – 1.86 – 10 шт, Celeron D2.8 – 2 шт.), стенды – 3</p>	

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Оценочные материалы (ОМ) для дисциплины включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины.**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

по дисциплине
«Информационная безопасность интернет вещей»

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ПКв-6	способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей	ИД1 ПКв-6 обладает навыками определения всех типов угроз данным для различных информационных автоматизированных систем

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1 ПКв-6 обладает навыками определения всех типов угроз данным для различных информационных автоматизированных систем	Знает: терминологию и определения интернет вещей, процесс получения и обработки показаний цифровых и аналоговых датчиков, управление сенсором и контроллером, проектирование деталей конструкции, виды сборки, модернизация, проектирование печатных плат, компьютерную среду программирования Arduino; основные технологии сбора и обработки данных; основные элементы, используемые при создании IoT-платформ; особенности методов, используемых при обмене данными между «вещью» и IoT-платформой
	Умеет: самостоятельно решать технические задачи в процессе создания IoT-систем (планирование предстоящих действий, самоконтроль, применять полученные знания, приемы и опыт создания систем с использованием специальных элементов, и других объектов и т.д.); создавать реально действующие модели IoT-систем при помощи специальных элементов по разработанной схеме, по собственному замыслу; создавать программы на компьютере для различных IoT-систем
	Владеет: навыками программирования интернет вещей, тестирования готового продукта, разработки технологическая карта или инструкция по эксплуатации готового продукта, навыками работы с виджетами, использования сервисов для организации обмена данными

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
1	Понятие интернета вещей	ПКв-6	Собеседование на зачете	Контроль преподавателем
			Тестирование	Компьютерное тестирование
			Контрольные вопросы к текущим опросам на практических работах	Контроль преподавателем
			Темы докладов	Контроль преподавателем
2	Обеспечение информационной безопасности IoT	ПКв-6	Собеседование на зачете	Контроль преподавателем
			Тестирование	Компьютерное тестирование

			Контрольные вопросы к текущим опросам на практических работах	Контроль преподавателем
			Темы докладов	Контроль преподавателем
3	Эталонная архитектура интернета вещей	ПКВ-6	Собеседование на зачете	Контроль преподавателем
			Тестирование	Компьютерное тестирование
			Контрольные вопросы к текущим опросам на практических работах	Контроль преподавателем
			Вопросы к коллоквиуму	Контроль преподавателем
4	Комплексное обеспечение безопасности IoT	ПКВ-6	Собеседование на зачете	Контроль преподавателем
			Тестирование	Компьютерное тестирование
			Контрольные вопросы к текущим опросам на практических работах	Контроль преподавателем
			Вопросы к коллоквиуму	Контроль преподавателем

3. Оценочные средства для промежуточной аттестации

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1 Собеседование на зачете

3.1.1. ПКВ-6 способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей

№ задания	Формулировка вопроса
01	Основные понятия в области кибербезопасности Интернета вещей;
02	Риски и уязвимости в сфере кибербезопасности Интернета вещей
03	Критическая информационная инфраструктура
04	Основные протоколы передачи данных
05	Аутентификации в IoT
06	Основные понятия в сфере функциональной безопасности;
07	Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации
08	Основные угрозы IoT
09	Архитектура основных подсистем обеспечения ИБ объектов КИИ
10	Основные определения СМИБ
11	Особенности построения СМИБ для объектов КИИ на промышленных объектах
12	Положения нормативных актов, устанавливающих ответственность за нарушение требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК
13	Цели обеспечения кибербезопасности в «Интернет-вещей» для граждан
14	Основные средства обеспечения кибербезопасности (архитектура, принципы построения)
15	Классификация и примеры продуктов «Интернет-вещей» для граждан, примеры угроз

16	Принципы проектирования систем безопасности значимых объектов КИИ;
17	Состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ
18	Основные риски и проблемы кибербезопасности «Интернет-вещей» в сфере здравоохранения
19	Основные требования к специалистам в области кибербезопасности «Интернет-вещей», критической информационной инфраструктуры
20	Основные риски и проблемы кибербезопасности для «Умного дома»
21	Состав и классификация систем для «Умного города», критерии оценки безопасности
22	Основных угроз, рисков и проблем, структуры и особенностей построения модели угроз для «Умного дома»
23	Основные риски и проблемы кибербезопасности в Smart Grid
24	Основные риски и проблемы кибербезопасности в Индустриальном Интернете вещей
25	Примеры юридических инцидентов в области регулирования кибербезопасности IoT

3.2 Кейс задания к практическим работам

3.2.1. ПКВ-6 способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей

№ задания	Формулировка вопроса
1.	создать приложение на платформе «Интернета вещей» для сбора и первичной обработке данных с различного оборудования, предусмотренного проектом
2.	создать интерфейсную страницу приложения, обеспечивающую вывод получаемых значений в режиме реального времени
3.	обеспечить передачу данных между конечными устройствами (единиц оборудования) и другими источниками, предусмотренными проектом, и платформой «Интернета вещей»
4.	продемонстрировать в реальном времени мониторинг собираемых данных и передачу управляющих команд, предусмотренных проектом
5.	разработать пользовательский интерфейс на платформе «Интернета вещей» в соответствии с логикой представления данных и управления системой автоматизации, определенных проектом
6.	создать интерфейс (отдельную страницу), обеспечивающую задание (ручной ввод) значений, подлежащих передаче на управляемые устройства, и обеспечить передачу этих данных
7.	разработать систему управления, реализующую заданный алгоритм управления оборудованием, в том числе обеспечивающую синхронизацию между отдельными единицами оборудования, и интерфейс к ней
8.	обеспечить адекватное (в соответствии с проектом) выполнение производственных задач и мониторинг работы оборудования
9.	разработать систему сбора данных заданного производственного процесса, их накопления и обработки в соответствии с указаниями проекта
10.	реализовать на платформе «Интернета вещей» интерфейс для визуализации итоговой и текущей информации в соответствии с логикой представления статистических и мониторинговых данных, представляющих интерес в практике управления гибким производством (определяется проектом)
11.	В процессе выполнения модуля системы мониторинга и управления, созданные в предыдущих модулях должны непрерывно функционировать с целью обеспечения непрерывного потока данных для анализа

3.3. Темы докладов

3.3.1 . ПКВ-6 способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей

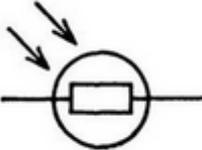
№ задания	Формулировка задания
1.	Определение понятия "Интернет Вещей". Примеры и основные области применения "Интернета Вещей". История появления и развития "Интернета Вещей". Основные факторы, повлиявшие на развитие "Интернета Вещей"
2.	Конечные устройства - контроллеры, датчики, актуаторы. Роль конечных устройств в архитектуре "Интернета Вещей". Примеры и основные области применения датчиков и актуаторов. Подключение датчиков и актуаторов к микроконтроллерам. Разница между микропроцессорами, микроконтроллерами и микрокомпьютерами. Ознакомление с линейкой микропроцессоров Arduino. Ознакомление с линейкой микрокомпьютеров Raspberry Pi
3.	Роль сетевых подключений в "Интернете Вещей". Проводные и беспроводные каналы связи. Протоколы IPv4 и IPv6. Принципы подключения устройств в сеть и способы передачи информации. Сетевые топологии, применяемые для подключения конечных устройств в сеть. Беспроводные сети Wi-Fi. Технологии ZigBee и ее особенности. Технология Bluetooth Low Energy и ее особенности. LPWAN - энергоэффективные сети дальнего радиуса действия.
4.	Примеры собираемых и обрабатываемых данных в IoT-системах. Большие Данные (Big Data). Основные характеристики Больших Данных: объем, скорость, разнородность, достоверность, ценность. Средства и инструменты статической обработки данных. Средства и инструменты потоковой обработки данных. Средства и инструменты хранения данных. Разнородность и семантика данных. Применение средств Семантического Веба для создания единой семантической модели в IoT-системах. Применение средств Машинного Обучения для обработки данных.
5.	Сервисно-ориентированные архитектуры, история развития. Облачные вычисления. Классификация и основные модели облачных вычислений. Роль облачных вычислений в обработке и хранении данных, получаемых от IoT-систем. Примеры облачных платформ и сервисов для обработки и хранения данных, получаемых от IoT-систем.
6.	Принципы проектирования и создания пользовательских приложений и сервисов на основе IoT-систем. Путь от IoT-прототипа до законченного продукта (сервиса). Обзор бизнес-моделей, применяемых для коммерциализации IoT-продуктов. Основные тренды в развитии "Интернета Вещей" в Российской Федерации и мире. Примеры успешного внедрения IoT-систем и сервисов в Российской Федерации

3.4. Тестирование

3.4.1 . ПКВ-6 способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей

№ задания	Формулировка задания
1.	Что такое интернет вещей? - сеть где преобладают только машины - гаджеты - функциональная сеть состоящая из физических предметов - умная планета
2.	Из чего состоит веб-сайт? - Из одной или нескольких веб-страниц - Из ссылок - Из серверов - Из сайтов
3.	Что не может находиться на веб-странице? - Музыка - Текст - Картинки

	<ul style="list-style-type: none"> - Видео - Файловая система
4.	<p>Что такое фоторезистор?</p> <ul style="list-style-type: none"> - Изменяет сопротивление в зависимости от освещенности - Используется для вспышки в фотоаппарате - Светится в зависимости от напряжения
5.	 <p>Назовите датчик.</p> <ul style="list-style-type: none"> - Датчик температуры и влажности - Датчик атмосферного давления - Фоторезистор - Датчик линии
6.	 <p>Какая используется линза у датчика PIR?</p> <ul style="list-style-type: none"> - собирающая линза - рассеивающая линза - линза Галилея - линза Кеплера - линза Френеля
7.	 <p>Датчик PIR - это</p> <ul style="list-style-type: none"> - оптический модуль, предназначенный для обнаружения препятствий в виде белых или чёрных линий. - модульный датчик света, который реагирует на видимое световое излучение и изменяет свое сопротивление в зависимости от яркости излучаемого светового потока. - полноценный цифровой термометр, способный измерять температуру в диапазоне от -55°C до +125°C с программируемой точностью 9-12 бит. - модуль используется для обнаружения движения объектов, излучающих инфракрасное излучение, в системах безопасности, автоматических выключателях света
8.	 <p>Это датчик</p> <ul style="list-style-type: none"> - движения - звука - света - газа

9.	<p>За улавливание каких газов, отвечает датчик MQ - 7</p> <ul style="list-style-type: none"> - пропан - бутан - угарный газ - водород
10.	<p>Какой датчик используют в охранных целях?</p> <ul style="list-style-type: none"> - Датчик движения и присутствия - Датчик света - Датчик тока
11.	<p>Какой датчик служит для обнаружения неработающих электроприборов?</p> <ul style="list-style-type: none"> - Датчик тока - Датчик света - Датчик давления
12.	<div style="text-align: center;">  </div> <p>Какой элемент изображен на рисунке?</p> <ul style="list-style-type: none"> - диод - резистор - фоторезистор - терморезистор
13.	<p>Какое устройство считается первым представителем интернета вещей?</p> <ul style="list-style-type: none"> - Автомат по продаже газировки - Домашняя метеостанция - Умный дверной замок
14.	<p>На что способны умные пылесосы?</p> <ul style="list-style-type: none"> - Предоставляют информацию о степени загрязнённости квартиры - Самостоятельно зонировать жильё на комнаты - Не начинают убирать, пока рядом есть домашние животные
15.	<p>А таблетки? Они теперь тоже запрыгивают в рот по расписанию?</p> <ul style="list-style-type: none"> - Нет, но умная упаковка вовремя напомнит принять лекарство - Да. Для велосипедистов предусмотрены умные системы, которые крепятся к шлему и забрасывают таблетку в рот в назначенное время
16.	<p>А как насчёт умной одежды? IoT?</p> <ul style="list-style-type: none"> - Да, настоящий интернет вещей! Главное, чтобы было по размеру - Умной одежды пока не существует
17.	<p>Ваш умный домофон вышел из строя. Чинить или починится сам?</p> <ul style="list-style-type: none"> - Починится: он же умный, должен понимать - Придётся заказывать диагностику и ремонт. Техника хоть и умная, но сама себя не починит - Чинить, но без диагностики: домофон сам подскажет, что сломалось
18.	<p>Игровые консоли подключаются к интернету и обмениваются по нему данными. Их можно причислить к IoT?</p> <ul style="list-style-type: none"> - Безусловно. Автообновления, подключение по Wi-Fi и многое другое: самый настоящий IoT - Ни в коем случае
19.	<p>Спохватиться, нервно всматриваться в счётчик и впопыхах передавать показания. Знакомо? Расслабьтесь, ведь умные счётчики передадут всё за вас. Так ведь?</p>

	<ul style="list-style-type: none"> - Именно! Умные счётчики автоматизировали передачу показаний, так что можно не беспокоиться о пропущенной дате - Не думаю, что такие есть, ведь автоматическая передача может затронуть конфиденциальность
20.	<p>IoT проник буквально в каждую вещь. Наверное, и топоры теперь умные?</p> <ul style="list-style-type: none"> - Конечно. Амплитуду удара и количество поленьев самому, что ли, считать? - Нет

**4. Методические материалы,
определяющие процедуры оценивания знаний, умений, навыков
и (или) опыта деятельности,
характеризующих этапы формирования компетенций**

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания		
				Академическая оценка или баллы	Уровень освоения компетенции	
ПКВ-6 способен определять угрозы безопасности информации, обрабатываемой автоматизированной системой, определять комплекс мер для защиты информации, оценивать возможность внешних и внутренних нарушителей						
ЗНАТЬ: базовые вопросы построения открытых информационных систем	Собеседование на зачете	Уровень владения материалом	60 % и более правильных ответов	Зачтено	Освоена (повышенный, базовый)	
			Менее 59% правильных ответов	Не зачтено	Не освоена (недостаточный)	
	Тест	Результат тестирования	85% и более правильных ответов	Отлично	Освоена (повышенный)	
			75-84% правильных ответов	Хорошо	Освоена (повышенный)	
			65-74% правильных ответов	Удовлетворительно	Освоена (базовый)	
			Менее 64% правильных ответов	Не удовлетворительно	Не освоена (недостаточный)	
	УМЕТЬ: участвовать в разработке компонентов открытых информационных систем	Контрольные вопросы к текущим опросам по практическим работам	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
				студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)
студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки				Удовлетворительно	Освоена (базовый)	

			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ: методикой анализа структуры открытых информационных систем. Терминологией и системным подходом построения защищенных открытых информационных систем	Доклад	Уровень доклада и презентации	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена (повышенный, базовый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена (недостаточный)
ОПК-5.1 - Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем					
ЗНАТЬ: принципы работы сетевых протоколов и технологий передачи данных в открытых информационных системах, основные стандарты построения и взаимодействия открытых систем	Тестирование на зачете	Уровень владения материалом	60 % и более правильных ответов	Зачтено	Освоена (повышенный, базовый)
			Менее 59% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: проектировать взаимодействия многомашиных информационных систем, используя стандартные протоколы эталонной модели, применять на практике стандарты, относящиеся к открытым информационным системам	Контрольные вопросы к текущим опросам по практическим работам	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (повышенный)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (повышенный)
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ: навыками решения формализуемых и трудно формализуемых задач, а также проектирования информационных процессов	Доклад	Уровень доклада и презентации	выставляется студенту при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена (повышенный, базовый)

			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена (недостаточный)
--	--	--	---	------------	----------------------------